**Міністерство освіти і науки України**

**Луцький національний технічний університет**
(повне найменування закладу вищої освіти)

**Факультет комп'ютерних та інформаційних технологій**
(повне найменування факультету)

**Кафедра комп'ютерної інженерії та безпеки**
(повне найменування кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»

## МОДЕРНІЗАЦІЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІЗ ВПРОВАДЖЕННЯМ СИСТЕМИ МОНІТОРИНГУ ТА ЕЛЕМЕНТІВ ЗАХИСТУ

## MODERNISATION OF NETWORK INFRASTRUCTURE WITH THE IMPLEMENTATION OF A MONITORING SYSTEM AND SECURITY FEATURES

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІмз-21
Боровик Олександр Васильович

(підпис)

Керівник:
к.т.н., доцент
Костючко Сергій Миколайович

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» грудня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *магістр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т.ТЕРЛЕЦЬКИЙ
« 18 » 06 2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

*Боровику Олександру Васильовичу*
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізація мережевої інфраструктури із впровадженням системи моніторингу та елементів захисту*

Керівник роботи *к.т.н., доцент Костючко Сергій Миколайович*

затверджені наказом закладу вищої освіти від «17» червня 2025 року № 290/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 09.12.2025р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
*Вступ*
*Аналітична частина*
*Вибір апаратного та програмного середовища, порівняння існуючого обладнання з новим*
*Створення локально-обчислювальної мережі*
*Висновки*

5. Перелік графічного (ілюстративного) матеріалу:
*Схема та топологія існуючої мережі. Обладнання. Дашборд системи Zabbix. Результати моніторингу мережі. Таблиці порівняльного характеру з існуючим рішенням. Інтерфейс користувача. Архітектура системи моніторингу Zabbix. Топологія та архітекура модернізованої мережі. Лістинг.*

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| *Аналітична частина* | *Костючко С.М., доцент* | | |
| *Вибір апаратного та програмного середовища, порівняння існуючого обладнання з новим* | *Костючко С.М., доцент* | | |
| *Створення локально-обчислювальної мережі* | *Костючко С.М., доцент* | | |
| *Нормоконтроль* | *Багнюк Н.В., доцент* | | |
| *Гарант ОП* | *Гринюк С.В., доцент* | | |
| *Показник запозичень тексту* | ***%*** | | |
| *Академічна доброчесність* | *Міскевич О.І., ст.викладач* | | |

7. Дата видачі завдання 18.06.2025 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | *Огляд літератури із досліджуваної проблеми* | До 01.08.2025 р. | *виконано* |
| 2. | *Аналітична частина* | До 20.08.2025 р. | *виконано* |
| 3. | *Вибір апаратного та програмного середовища, порівняння існуючого обладнання з новим* | До 25.09.2025 р. | *виконано* |
| 4. | *Створення локально обчислювальної мережі* | До 20.10.2025 р. | *виконано* |
| 5. | *Висновки та пропозиції* | До 25.10.2025 р. | *виконано* |
| 6. | *Формування списку використаних джерел* | До 27.10.2025 р. | *виконано* |
| 7. | *Формування додатків* | До 30.10.2025 р. | *виконано* |
| 8. | *Оформлення ілюстративного матеріалу* | До 05.11.2025 р. | *виконано* |
| 9. | *Представлення остаточного варіанту кваліфікаційної роботи керівникові* | До 11.11.2025 р. | *виконано* |
| 10. | *Нормоконтроль* | До 29.11.2025 р. | *виконано* |
| 11. | *Інструментальна перевірка на академічний плагіат* | До 02.12.2025 р. | *виконано* |
| 12. | *Здача кваліфікаційної роботи та всіх супровідних документів на кафедру* | До 09.12.2025 р | *виконано* |

Здобувач вищої освіти _____ Боровик О.В.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Костючко С.М.
(підпис) (прізвище, ініціали)

# АНОТАЦІЯ

Боровик О. В. Модернізація мережевої інфраструктури із впровадженням системи моніторингу та елементів захисту. Рукопис.

Кваліфікаційна робота магістра ОП «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія». Луцький національний технічний університет. Луцьк, 2025.

У роботі розглядаються питання модернізації комп'ютерної мережі з метою підвищення її продуктивності, надійності та рівня безпеки. Об'єктом дослідження є мережеві інфраструктури невеликих організацій, зокрема мережа Поворської сільської ради. Предметом дослідження виступають методи моніторингу, управління та захисту мережевих систем.

Метою роботи є розробка проєктної моделі модернізованої мережі із впровадженням системи моніторингу та засобів захисту інформації, а також оцінка ефективності її впровадження. Для досягнення мети було виконано аналіз існуючої мережевої інфраструктури, визначено проблемні ділянки та вимоги до модернізації, обрано оптимальні програмні та апаратні засоби для моніторингу та захисту мережі.

У роботі застосовано методи системного аналізу, проектування інформаційних систем, моделювання мережевих процесів, а також практичні підходи до впровадження мережевих засобів моніторингу (Zabbix, Nagios) та елементів захисту (фаєрволи, VPN, сегментація мережі, антивірусний захист). Проведено тестування запропонованого проєкту в умовах реальної організації, оцінено ефективність модернізації та її вплив на стабільність та безпеку мережевих процесів.

Ключові слова: комп'ютерна мережа, моніторинг, інформаційна безпека, фаєрвол, VPN, сегментація мережі, модернізація мережевої інфраструктури.

# ABSTRACT

Borovyk O. Modernization of Network Infrastructure with Implementation of Monitoring Systems and Security Elements. Manuscript.

Master's Thesis in the Educational Program «Computer Engeneering», specialty 123 «Computer Engeneering». Lutsk National Technical University. Lutsk, 2025.

The thesis addresses the issues of computer network modernization aimed at improving performance, reliability, and security levels. The object of the study is the network infrastructure of small organizations, in particular the network of Povorska Village Council. The subject of the study is the methods of monitoring, managing, and securing network systems.

The purpose of the work is to develop a project model of a modernized network with the implementation of a monitoring system and security tools, as well as to evaluate the effectiveness of its implementation. To achieve this purpose, an analysis of the existing network infrastructure was carried out, problem areas and modernization requirements were identified, and optimal software and hardware solutions for network monitoring and protection were selected.

The study applies methods of system analysis, information system design, network process modeling, as well as practical approaches for implementing network monitoring tools (Zabbix, Nagios) and security elements (firewalls, VPN, network segmentation, antivirus protection). The proposed project was tested in a real organizational environment, and the effectiveness of the modernization and its impact on network stability and security were assessed.

Keywords: computer network, monitoring, information security, firewall, VPN, network segmentation, network infrastructure modernization.

# ЗМІСТ

# ВСТУП

Сучасні комп'ютерні мережі є невід'ємним елементом інформаційної інфраструктури будь-якої організації. Зі зростанням обсягів оброблюваних даних, підвищенням вимог до надійності та безпеки інформаційних систем постає необхідність модернізації мережевої інфраструктури, упровадження інтелектуальних систем моніторингу та ефективних засобів захисту. Особливо це важливо для невеликих організацій, органів місцевого самоврядування та комунальних установ, які часто мають обмежені фінансові й технічні ресурси, що ускладнює оперативне реагування на технічні збої та кіберзагрози. Модернізація мережевих систем стає ключовим фактором підвищення ефективності роботи персоналу, безперебійного функціонування інформаційних сервісів і захисту конфіденційних даних.

Актуальність теми дослідження. Мережева інфраструктура органів місцевого самоврядування є критичним компонентом організації електронного документообігу, взаємодії з державними інформаційними системами та надання адміністративних послуг громадянам. Традиційні підходи до побудови локальних мереж, засновані на застарілому обладнанні та відсутності централізованого моніторингу, призводять до значних часових витрат на усунення збоїв, знижують продуктивність роботи співробітників і створюють ризики втрати критичної інформації. Створення модернізованої мережевої інфраструктури з використанням сучасних технологій моніторингу та захисту стає необхідністю для ефективної цифровізації діяльності місцевих органів влади.

Сучасний стан проблеми. Питання побудови, оптимізації та захисту комп'ютерних мереж висвітлювалися в працях українських і зарубіжних учених, які досліджували архітектуру мережевих систем, методи маршрутизації, управління трафіком, моніторингу та кібербезпеки, а також розробляли VPN- технології, системи IDS/IPS, фаєрволи й SIEM-рішення. Існуючі комерційні системи моніторингу (PRTG Network Monitor, SolarWinds, Cisco

Prime Infrastructure) мають високу вартість ліцензій і складність налаштування, що обмежує їх застосування в невеликих організаціях. Відкриті рішення (Zabbix, Nagios) потребують значної технічної підготовки персоналу для впровадження та підтримки. Водночас інтеграція систем моніторингу та захисту в умовах обмежених ресурсів місцевих установ опрацьована недостатньо, що визначає доцільність і новизну обраної теми.

Об’єкт дослідження – мережеві інфраструктури невеликих організацій, їх структура, склад обладнання та принципи організації інформаційних потоків.

Предмет дослідження – методи моніторингу, управління та захисту комп’ютерних мереж, а також програмні й апаратні засоби, що забезпечують їхню надійність, безпеку та продуктивність.

Метою кваліфікаційної роботи є розроблення проєктної моделі модернізованої мережі Поворської сільської ради з інтеграцією системи моніторингу та елементів захисту інформації, а також оцінка ефективності її впровадження.

Завдання кваліфікаційної роботи:

– проаналізувати стан існуючої мережевої інфраструктури Поворської сільської ради та визначити її технічні й організаційні особливості;

– виявити проблемні ділянки та сформулювати вимоги до модернізації мережі з урахуванням продуктивності, надійності та безпеки;

– обґрунтувати вибір апаратних і програмних засобів для ефективного моніторингу та захисту мережевих систем;

– розробити проєкт модернізованої мережевої інфраструктури з інтеграцією системи моніторингу та захисту інформації;

– виконати тестування запропонованого проєкту та оцінити його ефективність у реальних умовах функціонування мережі.

Наукова новизна роботи полягає в розробленні концептуальної моделі модернізованої мережі органу місцевого самоврядування, що поєднує технології моніторингу на кшталт Zabbix і PRTG із комплексними засобами безпеки, такими як фаєрволи, VPN та сегментація VLAN, для оптимізації роботи мережі,

централізованого управління, зниження ризику збоїв і спрощення діагностики інцидентів безпеки. Удосконалено методи організації мережевої інфраструктури через впровадження багаторівневого захисту з автоматичною валідацією політик доступу та реального моніторингу стану обладнання.

Практична цінність роботи. Розроблена проєктна модель може бути впроваджена в невеликих організаціях, органах місцевого самоврядування, закладах освіти й комунальних підприємствах для скорочення часу реагування на мережеві інциденти з 8-12 хвилин до 1-2 хвилин, підвищення рівня доступності сервісів з 94,3 % до 99,7 % та забезпечення економії коштів на експлуатацію через зменшення кількості простоїв і оптимізацію використання ресурсів. Архітектура системи допускає адаптацію до специфічних потреб різних установ без значних змін у базовій конфігурації.

Методи дослідження. У процесі виконання роботи використано комплекс методів дослідження, зокрема системний аналіз для оцінки існуючої мережевої інфраструктури, моделювання для прогнозування навантаження та виявлення вузьких місць у мережевих процесах, методи проєктування інформаційних систем для розроблення оптимальної структури мережі.

Інформаційну базу дослідження становлять наукові публікації та монографії в галузі комп’ютерних мереж і кібербезпеки, нормативно-правові акти України, технічна документація обладнання, матеріали офіційних сайтів виробників, статистичні дані з відкритих мережевих ресурсів, а також практичні матеріали, отримані в процесі стажування в Поворській сільській раді.

Апробація результатів. Результати роботи представлені у публікації наукового часопису «Технічні вісті», опублікованого 2025 р., м. Львів [26].

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ, МОНІТОРИНГУ ТА ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

У сучасних умовах ефективна робота будь-якої організації значною мірою залежить від стабільності та безпеки її комп'ютерної мережі. Збільшення обсягів обміну даними, зростання числа користувачів та розвиток інформаційних технологій призводять до виникнення нових загроз та підвищують вимоги до надійності мережевих систем. Тому особлива увага приділяється не лише їх проектуванню та впровадженню, а й постійному моніторингу та забезпеченню інформаційної безпеки.

Теоретичні основи побудови мереж включають в себе знання про класифікацію комп'ютерних мереж за різними критеріями, принципи їх організації, типові архітектури та методи управління інформаційними потоками. Моніторинг мережевої інфраструктури дозволяє своєчасно виявляти проблеми, оцінювати продуктивність систем та запобігати збої. Сучасні підходи до захисту мереж передбачають використання комплексних заходів, що поєднують апаратні та програмні засоби, включаючи фаєрволи, VPN, антивірусний захист, а також організаційні заходи та політики доступу.

Цей розділ присвячено детальному розгляду теоретичних аспектів побудови комп'ютерних мереж, методів їх моніторингу та сучасних підходів до забезпечення безпеки інформації.

## 1.1 Класифікація та принципи проєктування мереж

Комп'ютерні мережі є базовим компонентом сучасних інформаційних систем, оскільки забезпечують обмін даними, спільний доступ до ресурсів і централізоване управління інфраструктурою організації. Розвиток цифрової економіки зумовлює потребу в мережах, які поєднують високу швидкість,

надійність та захищеність передавання інформації, що вимагає коректного вибору їх типу, архітектури та топології на етапі проєктування.

За територіальним охопленням виділяють локальні, міські, глобальні та бездротові мережі. Локальні мережі (LAN) функціонують у межах однієї будівлі або організації, забезпечують високу швидкість обміну даними (до 1 Гбіт/с) і відносно просте адміністрування [24], тому є базовим рішенням для офісів, навчальних закладів та невеликих підприємств. Міські мережі (MAN) об’єднують кілька будівель чи підрозділів у межах населеного пункту і використовуються для побудови корпоративних систем зв’язку або міських сервісів, зокрема в органах місцевого самоврядування. Глобальні мережі (WAN) охоплюють значні відстані, поєднуючи локальні сегменти через маршрутизатори та захищені канали зв’язку (наприклад, VPN-тунелі), а наймасштабнішим прикладом такої мережі є Інтернет. Бездротові локальні мережі (WLAN) забезпечують мобільний доступ користувачів без розгалуженої кабельної інфраструктури, що є важливим для гнучких офісів, мобільних робочих місць та публічних зон доступу.

Додатково мережі класифікують за швидкістю передавання даних, фізичним середовищем і способом комутації [28]. Залежно від пропускної здатності вони поділяються на низько-, середньо- та високошвидкісні, при цьому високошвидкісні рішення застосовуються для обміну великими обсягами інформації між серверами, дата-центрами та хмарними платформами. Як середовище передавання використовують мідний кабель, оптоволокно, радіоканали або супутниковий зв’язок; з них волоконно-оптичні лінії забезпечують найвищу пропускну здатність і мінімальну затримку [29], тому є пріоритетними для магістралей і критичних корпоративних сегментів. За способом комутації сучасні мережі здебільшого орієнтовані на пакетну комутацію в межах стеку TCP/IP, що дає змогу ефективно використовувати ресурси каналів і гнучко маршрутизувати трафік.

Важливою характеристикою мережі є її архітектура, яка визначає розподіл ролей між вузлами та спосіб організації доступу до ресурсів. Класична клієнт-

серверна архітектура передбачає наявність одного або кількох серверів, що обробляють запити клієнтів, керують доступом до баз даних, файлів і прикладних сервісів, а також реалізують політики безпеки; такий підхід став стандартом для систем електронного документообігу, бухгалтерських комплексів і внутрішніх порталів. Однорангова (peer-to-peer) архітектура базується на рівноправній взаємодії вузлів, де кожен комп'ютер може одночасно виступати клієнтом і сервером, що спрощує розгортання невеликих мереж, але обмежує масштабованість і рівень захисту. Хмарна архітектура використовує віртуалізовані ресурси дата-центрів і надає доступ до обчислювальних потужностей, сховищ даних та програмних сервісів через Інтернет [5], спрощуючи адміністрування й дозволяючи гнучко масштабувати ресурси без значних капітальних витрат.

Топологія мережі описує фізичну структуру з'єднань між вузлами та має суттєвий вплив на надійність, масштабованість і простоту обслуговування. Топологія «шина» є однією з найпростіших, проте сильно залежить від працездатності спільного сегмента кабелю, через що її застосування обмежується невеликими системами. Топологія «зірка» сьогодні домінує в локальних мережах, оскільки забезпечує централізоване керування, зручну діагностику несправностей та можливість простого розширення шляхом підключення нових вузлів до комутатора, хоча й створює єдину точку відмови в разі виходу з ладу центрального пристрою. Топологія «кільце» забезпечує впорядковану передачу кадрів і відсутність колізій, але вихід з ладу окремого вузла або ділянки лінії може призвести до зупинки роботи всієї мережі. Топологія «дерево» поєднує властивості шини та зірки, формуючи ієрархічну структуру з декількома рівнями підмереж. У великих корпоративних системах часто використовуються гібридні топології, які комбінують різні варіанти з'єднань для досягнення балансу між продуктивністю, відмовостійкістю та гнучкістю розширення.

Проєктування комп'ютерних мереж базується на таких принципах, як масштабованість, надійність, продуктивність, безпека та економічність.

Масштабованість означає можливість розширення мережі без кардинальної зміни її архітектури, а надійність вимагає побудови відмовостійкої інфраструктури з резервуванням критичних пристроїв і каналів зв'язку. Висока продуктивність досягається раціональним вибором технологій передавання даних, топології та конфігурації обладнання. Безпека передбачає впровадження механізмів автентифікації, авторизації, шифрування трафіку та контролю доступу на різних рівнях, а економічність полягає в оптимальному співвідношенні вартості рішень та якості наданих сервісів.

Сучасні підходи до побудови мережевої інфраструктури передбачають:

– використання SDN (Software Defined Networking) [7] для централізованого управління потоками даних і розподілу навантаження;

– застосування віртуалізації мережевих функцій (NFV) з метою зменшення залежності від спеціалізованого апаратного забезпечення;

– перехід на протокол IPv6, який надає розширений адресний простір і додаткові механізми захисту;

– впровадження систем моніторингу та керування (NMS) для контролю продуктивності й оперативного виявлення інцидентів безпеки;

– інтеграцію з хмарними платформами для забезпечення віддаленого доступу до корпоративних ресурсів і підвищення мобільності користувачів.

Комп'ютерні мережі відіграють ключову роль у різних сферах діяльності. У бізнесі вони забезпечують побудову корпоративних VPN, інтеграцію географічно розподілених офісів і захищений обмін даними між підрозділами. У сфері державного управління мережеві інфраструктури є основою для систем електронного документообігу та сервісів «електронного уряду», що реалізуються в концепції Smart City. В освітніх і наукових установах мережі дають можливість організувати дистанційне навчання, доступ до електронних бібліотек і наукових ресурсів. У медичній галузі вони забезпечують роботу телемедичних сервісів і захист персональних даних пацієнтів, а у фінансовому секторі – функціонування транзакційних систем з високим рівнем криптографічного захисту. На рисунку 1.1 узагальнено взаємозв'язок між

основними типами мереж, архітектурами, топологіями та принципами їх проєктування, що формують основу сучасної інформаційної інфраструктури організації.


Рисунок 1.1 – Класифікація та принципи проектування мереж

Таким чином, правильне класифікування комп'ютерних мереж, обґрунтований вибір архітектури та топології, а також урахування сучасних принципів і технологій проєктування є ключовими передумовами створення ефективної, надійної та безпечної мережевої інфраструктури. Для невеликих організацій і органів місцевого самоврядування це дозволяє поєднати обмежені фінансові ресурси з високими вимогами до безперебійності роботи та захисту інформаційних ресурсів.

## 1.2 Інструменти та методи моніторингу мережевої інфраструктури

Моніторинг мережевої інфраструктури є ключовим елементом ефективного управління інформаційними системами, оскільки дозволяє забезпечити безперебійну роботу мережі, оптимізувати її продуктивність та своєчасно виявляти загрози. У сучасних умовах зростання обсягів трафіку та збільшення кількості кіберзагроз саме моніторинг стає основою якості сервісів і захисту інформаційних ресурсів організації.

Узагальнену схему моніторингу мережевої інфраструктури наведено на рисунку 1.2, де показано взаємодію між об’єктами спостереження, засобами збору даних, системою аналітики та механізмом сповіщення адміністраторів.


Рисунок 1.2 – Моніторинг мережевої інфраструктури

Залежно від рівня контролю та цілей адміністрування розрізняють кілька основних методів моніторингу мережевої інфраструктури. Пасивний моніторинг передбачає спостереження за роботою мережі без прямого втручання в її функціонування і зазвичай базується на зборі статистики трафіку, журналів подій та показників продуктивності [8]. Цей підхід дозволяє своєчасно виявляти перевантаження, помилки в конфігурації пристроїв, тенденції до зниження

швидкодії каналів зв’язку та формувати аналітичні звіти, що слугують основою для планування технічних робіт і модернізації обладнання.

На відміну від пасивного спостереження, активний моніторинг базується на створенні тестових запитів (наприклад, ICMP або SNMP) [15], які надсилаються до мережевих вузлів для визначення їхньої доступності, затримки передачі пакетів та загальної якості каналів зв'язку. Такі методи забезпечують швидке виявлення непрацюючих пристроїв і дають змогу оцінювати поточний стан мережі в реальному часі, що є критично важливим для оперативної діагностики проблем і підтримки високого рівня сервісу.

Особливе місце займає моніторинг у режимі реального часу, який використовує спеціальні програмні агенти для безперервного збирання даних про роботу серверів, комутаторів, маршрутизаторів і точок доступу [18]. Завдяки автоматичним сповіщенням адміністратор негайно отримує повідомлення про аварійні ситуації чи відмови обладнання, що дає змогу мінімізувати час простою системи та швидко реагувати на інциденти до того, як вони вплинуть на користувачів.

Сучасним підходом є поведінковий аналіз трафіку (UBA/NBA), який базується на виявленні аномалій у роботі мережі за допомогою алгоритмів машинного навчання [14]. Такі системи здатні фіксувати нетипову активність користувачів чи пристроїв, виявляти потенційні загрози ще до того, як вони вплинуть на інфраструктуру, і попереджати адміністраторів про можливі інциденти безпеки або технічні збої.

У практиці адміністрування мережевих систем використовуються як відкриті, так і комерційні рішення для моніторингу. Nagios забезпечує базовий контроль доступності серверів і служб, має широкий набір плагінів і є зручним для невеликих організацій з обмеженими ресурсами [17]. Zabbix дозволяє збирати метрики в реальному часі, будувати графіки навантаження, автоматично сповіщати про критичні події та підтримує велику кількість протоколів моніторингу [22], що робить його популярним у середовищі підприємств різного масштабу. Комерційне рішення PRTG Network Monitor має інтуїтивно

зрозумілий інтерфейс, наочні дашборди та надає детальний аналіз пропускної здатності каналів зв’язку, що спрощує впровадження та налаштування системи навіть для адміністраторів з невеликим досвідом. Для великих підприємств і розгалужених мереж доцільним є використання таких рішень, як SolarWinds Network Performance Monitor або Cisco Prime Infrastructure, які дозволяють централізовано керувати сотнями пристроїв, відстежувати топологію мережі в динаміці та інтегрувати дані з системами безпеки.

Окремо слід відзначити інструмент Wireshark, який призначений для глибокого аналізу пакетів трафіку та дає змогу виявляти помилки в налаштуваннях протоколів, діагностувати проблеми з затримками або втратою даних, а також фіксувати підозрілу активність у мережі, що може свідчити про наявність кіберзагроз.

Більшість систем моніторингу працюють на основі стандартних мережевих протоколів. SNMP (Simple Network Management Protocol) використовується для збирання інформації про стан пристроїв, такої як завантаження процесора, використання пам’яті, обсяг трафіку на інтерфейсах і статус портів комутаторів. ICMP (Internet Control Message Protocol) застосовується для перевірки доступності мережевих вузлів за допомогою утиліт ping і traceroute, що дозволяє швидко виявляти проблеми з каналами зв’язку або маршрутизацією. Для детального аналізу структури трафіку використовуються протоколи NetFlow (Cisco) або sFlow (стандарт для різних виробників), які дозволяють визначати джерела перевантажень каналів, контролювати ефективність використання мережевих ресурсів і формувати статистичні звіти про потоки даних. Додатково протокол Syslog забезпечує централізований збір системних журналів подій з різноманітного обладнання (маршрутизатори, комутатори, сервери) та їх подальший аналіз для виявлення проблем безпеки, технічних збоїв або порушень політик доступу.

Регулярне використання систем моніторингу дозволяє не лише своєчасно виявляти неполадки, але й підвищує загальний рівень інформаційної безпеки організації. Моніторинг допомагає оптимізувати використання наявних ресурсів,

планувати модернізацію інфраструктури на основі реальних даних про завантаження каналів і серверів, прогнозувати зростання навантаження на мережу та уникати несанкціонованих втручань у роботу системи шляхом фіксації аномальної активності.

Сучасний розвиток технологій привів до появи нових напрямів моніторингу, що підвищують рівень автоматизації та інтелектуальності систем спостереження за мережевою інфраструктурою. Активно розвивається автоматизація процесів з використанням штучного інтелекту та машинного навчання (AI/ML), що дає змогу аналізувати великі масиви історичних даних, виявляти складні закономірності в роботі мережі та прогнозувати можливі збої ще до того, як вони призведуть до відмови обладнання чи зниження продуктивності. Популярності набувають хмарні сервіси моніторингу (Datadog, Azure Monitor, New Relic), які дозволяють контролювати розподілену інфраструктуру без розгортання локальних серверів збору даних, що спрощує масштабування системи та знижує витрати на обслуговування.

Важливим напрямом є інтеграція систем моніторингу із SIEM- платформами (Security Information and Event Management), такими як Splunk, IBM QRadar або ArcSight [10], які об’єднують контроль продуктивності мережевих компонентів з аналізом подій безпеки та автоматичним кореляційним аналізом інцидентів, що дозволяє виявляти складні багатоетапні атаки. З поширенням контейнерних технологій (Docker, Kubernetes) виникла потреба у спеціалізованих інструментах моніторингу, таких як Prometheus і Grafana, які забезпечують збір метрик із мікросервісних архітектур, автоматичне виявлення нових контейнерів і візуалізацію стану розподілених додатків у реальному часі. Окремо варто виділити прогнозний моніторинг, який аналізує історичні дані про роботу обладнання та визначає ймовірність відмови того чи іншого вузла ще до її виникнення, що дає змогу проводити планове обслуговування та заміну компонентів до того, як вони призведуть до збоїв у роботі мережі.

Разом із очевидними перевагами впровадження систем моніторингу існують і певні проблеми, які необхідно враховувати на етапі проєктування та

налаштування. Головними з них є складність керування великими розподіленими мережами, де кількість пристроїв може сягати тисяч одиниць, що вимагає потужних серверів збору даних і кваліфікованого персоналу для аналізу звітів. Висока вартість ліцензійних комерційних продуктів також може стати перешкодою для невеликих організацій з обмеженими бюджетами, тому у таких випадках доцільно розглядати відкриті рішення на кшталт Zabbix або Nagios. Проблеми сумісності між обладнанням різних виробників також створюють труднощі при інтеграції систем моніторингу, оскільки не всі пристрої підтримують стандартні протоколи або мають обмежений функціонал SNMP.

Важливим залишається і питання кібербезпеки самої системи моніторингу, адже у разі компрометації програмного комплексу або сервера збору даних зловмисник може отримати доступ до критичної інформації про архітектуру мережі, конфігурацію пристроїв і вразливості інфраструктури. Саме тому належне налаштування прав доступу, сегментація мережі для ізоляції моніторингових серверів і контроль привілеїв користувачів є обов’язковими умовами безпечного та ефективного впровадження систем моніторингу.

Вибір системи моніторингу мережевої інфраструктури є стратегічно важливим завданням, від якого залежить надійність, ефективність і безпека функціонування всієї інформаційно-технічної системи організації. Під час оцінювання доцільності впровадження тієї чи іншої платформи слід ураховувати масштаб підприємства (кількість мережевих вузлів, географічну розподіленість), тип обладнання (наявність підтримки SNMP, можливість встановлення програмних агентів), рівень автоматизації (інтеграція з системами нотифікації, підтримка автоматичних дій у відповідь на інциденти), вимоги до безпеки й бюджетні обмеження.

Основними критеріями вибору системи моніторингу є масштабованість, тобто здатність розширюватися без кардинальних змін архітектури при збільшенні кількості об’єктів спостереження; сумісність із обладнанням різних виробників, яка гарантує можливість інтеграції мережевих пристроїв, серверів і робочих станцій без додаткових витрат; наявність модулів віддаленого доступу

та мобільних сповіщень, які дозволяють адміністраторам оперативно реагувати на інциденти навіть поза офісом. Важливою є також можливість інтеграції з SIEM-рішеннями, що поєднують функції моніторингу продуктивності та безпеки, а також підтримка засобів візуалізації даних, які полегшують аналіз зібраної інформації та дозволяють формувати звіти для керівництва.

На практиці моніторинг реалізується через безперервне спостереження за станом серверів, комутаторів, маршрутизаторів і каналів зв'язку, що дає змогу своєчасно виявляти перевантаження мережевих сегментів, збої в роботі обладнання або підозрілу активність, яка може свідчити про спроби атак. Крім того, системи моніторингу дозволяють проводити глибоку аналітику використання ресурсів, виявляти вузькі місця в інфраструктурі та оптимізувати розподіл навантаження між каналами зв'язку. Наприклад, у мережах місцевого самоврядування моніторинг забезпечує контроль роботи поштових серверів, внутрішніх вебпорталів, систем електронного документообігу та відеоспостереження, що є критично важливим для безперебійної взаємодії з громадянами та державними установами.

Окремо слід відзначити роль прогнозного моніторингу, який аналізує історичні дані про навантаження мережі, температуру обладнання, кількість помилок і відмов для передбачення можливих проблем у майбутньому. Такий підхід дозволяє планувати модернізацію системи на основі реальних показників, а не лише реагувати на вже існуючі проблеми, що значно підвищує рівень надійності інфраструктури.

Таким чином, сучасний моніторинг мережевої інфраструктури є не лише технічним інструментом для збору метрик, а й аналітичною системою, яка допомагає ухвалювати обґрунтовані управлінські рішення, оптимізувати експлуатаційні витрати та забезпечувати високий рівень стабільності й безпеки інформаційних ресурсів організації. Впровадження комплексного моніторингу створює основу для побудови інтелектуальної мережевої інфраструктури, здатної самостійно реагувати на зміни навантаження, виявляти аномалії та підтримувати безперебійну роботу критичних сервісів.

## 1.3 Сучасні загрози та підходи до захисту інформації

У сучасних умовах інформатизації суспільства питання захисту інформації набуває особливої актуальності. Збільшення обсягів даних, що передаються через мережі, зростання кількості підключених пристроїв, розвиток хмарних сервісів і віддаленого доступу призводять до підвищення ризику несанкціонованого втручання, втрати або спотворення інформації. Тому побудова ефективної системи інформаційної безпеки є ключовим завданням будь-якої організації, що використовує комп'ютерні мережі для обробки та зберігання конфіденційних даних.

Інформаційна безпека базується на концепції CIA triad (Confidentiality, Integrity, Availability), що передбачає збереження конфіденційності (захист даних від несанкціонованого розголошення), цілісності (гарантування того, що інформація не змінювалася без дозволу) та доступності (забезпечення постійного доступу до ресурсів для легітимних користувачів). Однак сучасні моделі безпеки доповнюються також принципами автентичності, яка передбачає перевірку справжності користувача або пристрою, що намагається отримати доступ до системи, та відмовостійкості, тобто здатності системи функціонувати навіть після часткових збоїв або атак.

Під час проєктування захисту інформаційних систем необхідно враховувати багаторівневу структуру загроз, що охоплює технічний рівень (вразливості програмного та апаратного забезпечення), програмний рівень (зловмисне програмне забезпечення), людський фактор (соціальна інженерія, фішинг) та організаційний аспект (відсутність політик безпеки, недостатнє навчання персоналу). Саме їх взаємодія визначає загальний рівень ризику для мережевої інфраструктури.

Сучасні кіберзагрози можна класифікувати за джерелом походження, способом реалізації та рівнем потенційного впливу на функціонування системи. Програмно-технічні загрози включають віруси, трояни, програми-вимагачі

(ransomware) та експлойти, які використовують вразливості у програмному забезпеченні для проникнення в систему або блокування роботи користувачів. Відомими прикладами таких атак є WannaCry та NotPetya [6], які паралізували роботу тисяч організацій по всьому світу, завдали мільярдних збитків і продемонстрували вразливість глобальної цифрової інфраструктури.

Мережеві загрози спрямовані на порушення роботи каналів зв'язку та отримання несанкціонованого доступу до даних під час їх передачі. До них належать фішинг (обман користувачів через підроблені вебсайти або електронні листи), атаки типу «людина посередині» (MITM), DDoS-атаки, що перевантажують сервери величезною кількістю запитів і виводять їх з ладу [3], а також підміна IP-адрес і перехоплення пакетів трафіку. Ці види загроз часто використовують недоліки в налаштуваннях мережевого обладнання або незахищеність протоколів передавання даних. За статистичними даними глобальних досліджень [16], кількість DDoS-атак продовжує зростати, що підтверджує актуальність впровадження спеціалізованих засобів захисту та систем раннього виявлення загроз.

Внутрішні загрози становлять значну частину інцидентів безпеки і пов'язані з діями співробітників, які навмисно або випадково призводять до витоку інформації, порушення політики безпеки або пошкодження даних. За статистикою, людський фактор залишається однією з основних причин успішних атак, оскільки зловмисники активно використовують соціальну інженерію для отримання облікових даних або обходу технічних засобів захисту

Загрози на рівні інтернету речей (IoT) та мобільних пристроїв стають дедалі актуальнішими з огляду на масове підключення смарт-пристроїв без належного шифрування, регулярних оновлень прошивки або механізмів автентифікації, що робить їх легкою мішенню для ботнетів і віддаленого захоплення. Окремий напрям становлять кіберзагрози державного рівня, які включають кібершпигунство, атаки на критичну інфраструктуру (енергетику, транспорт, телекомунікації) [9], дезінформаційні кампанії та ураження промислових систем керування SCADA. Такі загрози характеризуються високою

складністю, професійним виконанням і можуть мати серйозні наслідки для національної безпеки.

Комплексний захист інформації передбачає реалізацію трьох взаємопов'язаних рівнів, кожен із яких відіграє критично важливу роль у забезпеченні стійкості системи. На технічному рівні застосовуються програмно-апаратні засоби безпеки, серед яких міжмережеві екрани (firewall), що фільтрують вхідний і вихідний трафік за заданими правилами [21], системи виявлення та запобігання вторгненням (IDS/IPS), які в реальному часі аналізують мережеву активність на наявність підозрілих патернів [2], антивірусний захист на всіх кінцевих точках, VPN-тунелі для забезпечення конфіденційності даних під час передачі через відкриті мережі, а також засоби контролю трафіку через протоколи SNMP та NetFlow. Важливим є впровадження систем автоматизованого резервного копіювання, сегментації мережі за допомогою VLAN для ізоляції критичних ресурсів і застосування криптографічного шифрування даних як при передачі, так і при зберіганні.

Організаційний рівень захисту включає розроблення політики безпеки, яка визначає правила використання інформаційних ресурсів організації, порядок доступу до конфіденційних даних і відповідальність співробітників за порушення встановлених норм. Обмеження прав доступу за принципом найменших привілеїв (Principle of Least Privilege) забезпечує те, що кожен користувач має доступ лише до тих ресурсів, які необхідні для виконання його робочих обов'язків. Створення планів реагування на інциденти безпеки (Incident Response Plan) дозволяє чітко регламентувати дії персоналу в разі виявлення атак або збоїв, що мінімізує час відновлення системи. Навчання персоналу з основ кібергігієни, розпізнавання фішингових листів і правил безпечної роботи з корпоративними ресурсами знижує ризик людського чинника, який, за оцінками експертів, становить до 70 % усіх успішних інцидентів у сфері безпеки

Нормативно-правовий рівень захисту базується на міжнародних стандартах, таких як ISO/IEC 27001 (управління інформаційною безпекою), ISO/IEC 27005 (управління ризиками), рекомендаціях інституту NIST (зокрема,

фреймворку кібербезпеки NIST Cybersecurity Framework), а також законодавстві України, де ключовими нормативними актами є закони «Про кібербезпеку», «Про захист інформації в інформаційно-комунікаційних системах» і «Про захист персональних даних». Їх дотримання є обов'язковою умовою для державних органів, фінансових установ і підприємств, які працюють з персональними або службовими даними, а також для організацій, що прагнуть отримати міжнародну сертифікацію або співпрацювати з європейськими партнерами.

Сучасний етап розвитку кіберзахисту характеризується переходом до архітектури Zero Trust, яка базується на принципі «ніколи не довіряй, завжди перевіряй» (Never Trust, Always Verify). Ця модель передбачає, що жоден користувач або пристрій не вважається надійним за замовчуванням, навіть якщо він знаходиться всередині корпоративної мережі, а кожен запит на доступ до ресурсів проходить ретельну автентифікацію та авторизацію. Крім того, активно впроваджуються технології аналітики на основі штучного інтелекту та машинного навчання (AI/ML), які дозволяють виявляти аномалії у поведінці користувачів, розпізнавати нові, раніше невідомі типи атак (zero-day exploits) і попереджати інциденти ще до їх реалізації шляхом прогнозного аналізу.

Значну увагу в сучасній практиці приділяють Cloud Security – захисту хмарних середовищ і сервісів, які використовуються для зберігання великих обсягів даних, розміщення додатків і організації віддаленої роботи. Для цього розробляються спеціалізовані CASB-рішення (Cloud Access Security Broker), що контролюють доступ до хмарних ресурсів і забезпечують шифрування даних. Окремим напрямом розвитку є захист IoT-пристроїв, що передбачає створення стандартизованих протоколів безпеки для «розумних» сенсорів, контролерів і систем автоматизації, які нерідко мають обмежені обчислювальні ресурси та не підтримують традиційні засоби захисту.

У системах моніторингу кібербезпеки зростає роль SIEM-платформ (Security Information and Event Management), які поєднують збір і централізоване зберігання журналів подій з усіх компонентів інфраструктури, автоматичний аналіз великих обсягів даних, кореляцію інцидентів для виявлення складних

багатоетапних атак і автоматичне реагування на загрози згідно з попередньо визначеними сценаріями. Найвідомішими представниками цього класу рішень є Splunk, IBM QRadar, ArcSight і Microsoft Sentinel. Вони дають змогу централізовано контролювати безпеку всієї організації, формувати комплексні звіти для керівництва та органів аудиту, а також забезпечувати швидке реагування на інциденти.

Узагальнену модель багаторівневого захисту інформаційних ресурсів, що інтегрує технічні, організаційні та нормативно-правові компоненти, наведено на рисунку 1.3. На схемі показано взаємодію між підсистемами запобігання (превентивні заходи, що знижують імовірність реалізації загроз), моніторингу (безперервне спостереження за станом системи та виявлення інцидентів), реагування (оперативні дії у відповідь на виявлені атаки або збої) та відновлення (процедури повернення системи до нормального стану після інциденту).

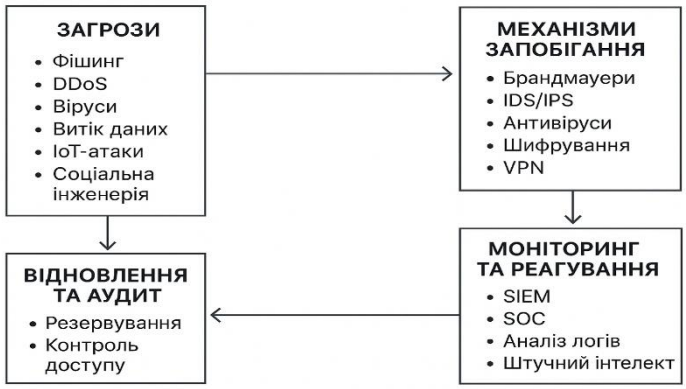


Рисунок 1.3 – Сучасні загрози та підходи до захисту інформації

Таким чином, сучасні загрози інформаційній безпеці характеризуються високою динамічністю, складністю виявлення та різноманітністю форм прояву, що зумовлює необхідність застосування гнучких і багаторівневих підходів до їх нейтралізації. Побудова ефективної системи кіберзахисту вимагає інтеграції технічних рішень (міжмережеві екрани, системи виявлення вторгнень, антивірусні програми, засоби шифрування), організаційних заходів (політики безпеки, навчання персоналу, контроль доступу) і нормативно-правового

регулювання (дотримання стандартів ISO, виконання вимог законодавства). Особливу роль відіграє людський фактор, адже саме користувачі найчастіше стають мішенню фішингових атак, соціальної інженерії та інших методів маніпуляції. Лише системний підхід, орієнтований на постійний моніторинг стану безпеки, регулярне навчання співробітників і адаптацію захисту до нових викликів, може гарантувати належний рівень захисту інформаційних ресурсів організації в умовах безперервної еволюції кіберзагроз.

# РОЗДІЛ 2
# АНАЛІЗ ТА ВИМОГИ ДО МОДЕРНІЗАЦІЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Ефективне функціонування органів місцевого самоврядування в умовах цифрової трансформації суспільства неможливе без сучасної та надійної мережевої інфраструктури. Саме комп'ютерні мережі забезпечують своєчасний обмін інформацією, доступ до державних електронних сервісів, організацію документообігу та комунікацію як всередині установи, так і з зовнішніми організаціями.

Однак наявна мережа Поворської сільської ради має низку обмежень, пов'язаних із застарілим обладнанням, недостатньою пропускною здатністю, відсутністю централізованого моніторингу та ефективних засобів захисту інформації. Це створює ризики втрати даних, збоїв у роботі сервісів та ускладнює реалізацію стратегічних завдань цифровізації громади.

У цьому розділі здійснено детальний аналіз поточного стану мережевої інфраструктури, визначено основні проблеми та обмеження її функціонування, а також сформульовано ключові вимоги до модернізації. Особлива увага приділятиметься питанням масштабованості, безпеки, енергоефективності та інтеграції сучасних технологій моніторингу й адміністрування.

Таким чином, результати аналізу дозволять розробити практичні рекомендації щодо вдосконалення мережевої інфраструктури Поворської сільської ради з урахуванням сучасних тенденцій та потреб громади.

## 2.1 Характеристика існуючої мережі та її проблеми

Мережева інфраструктура Поворської сільської ради є невід'ємною частиною організаційної діяльності установи, адже забезпечує обмін інформацією між працівниками, підтримку внутрішніх сервісів та доступ до мережі Інтернет. На сучасному етапі вона представлена базовим комплексом

обладнання та програмного забезпечення, побудованого за принципом локальної обчислювальної мережі (LAN). Локальна мережа об’єднує робочі місця співробітників апарату ради, декілька багатофункціональних пристроїв, сервери та персональні комп’ютери. Крім того, функціонує бездротова мережа Wi-Fi, яка використовується як співробітниками, так і відвідувачами для підключення до інтернету.

Узагальнену структуру існуючої мережі Поворської сільської ради подано на рисунку 2.1, де показано взаємодію між основними компонентами інфраструктури.

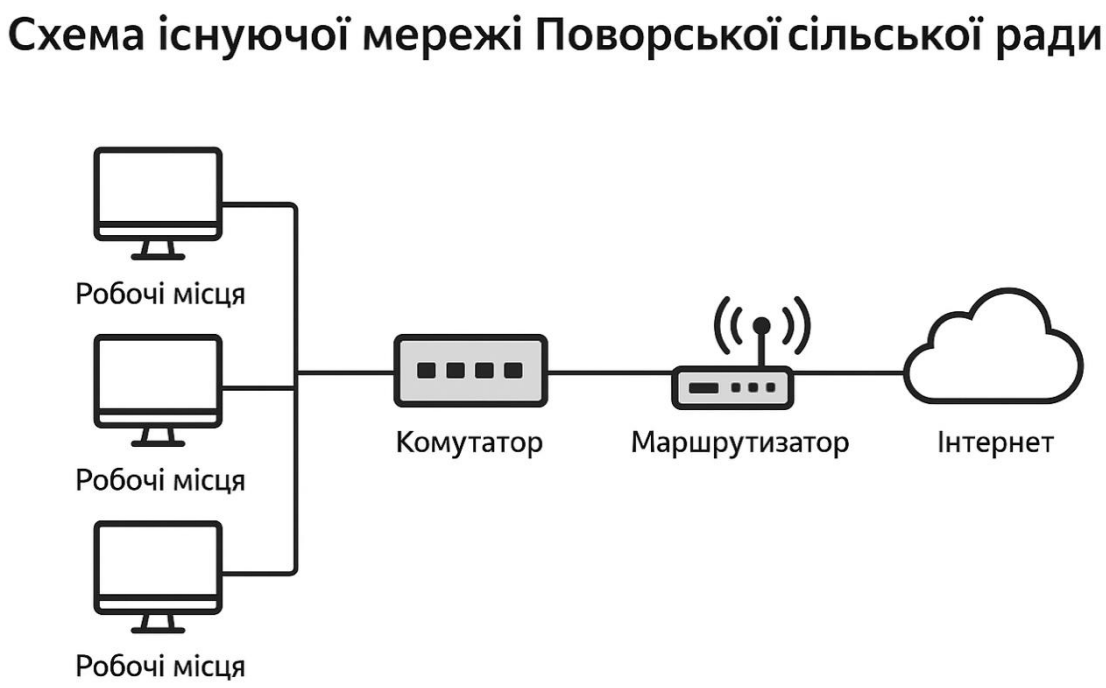


Рисунок 2.1 – Схема існуючої мережі Поворської сільської ради

Попри загальну працездатність, мережа Поворської сільської ради має низку критичних недоліків, які негативно впливають на ефективність роботи персоналу, стабільність зв’язку та безпеку переданої інформації. У ході обстеження виявлено, що більшість компонентів інфраструктури не відповідають сучасним вимогам до швидкодії, надійності й кіберзахисту.

Основним обмежувальним фактором є застаріле мережеве обладнання, що функціонує на базі побутових маршрутизаторів TP-Link TL-WR841N та комутаторів D-Link DES-1008A, які морально і технічно застаріли. Топологію існуючої мережі наведено на рисунку 2.2, де видно, що ці пристрої не підтримують гігабітні інтерфейси, обмежені за кількістю портів і не забезпечують сучасні стандарти безпеки, такі як WPA3, VLAN або VPN.

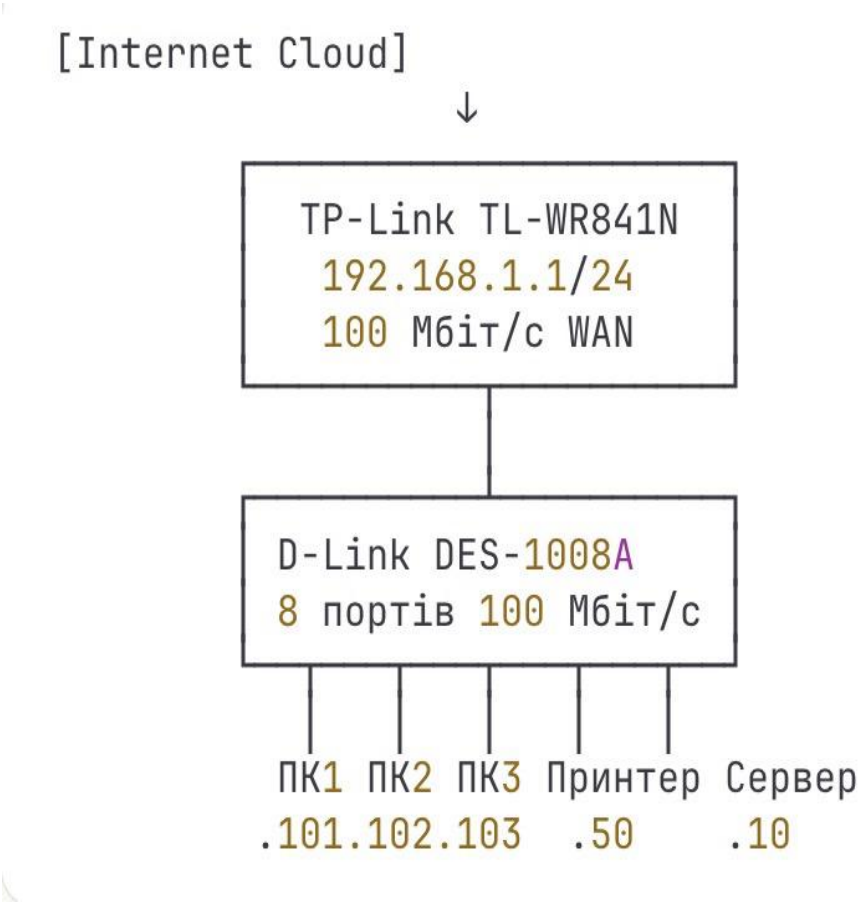


Рисунок 2.2 – Топологія існуючої мережі Поворської сільської ради

Максимальна пропускна здатність портів обладнання становить лише 100 Мбіт/с, що створює затримки при обробці трафіку, особливо під час активного використання хмарних сервісів і внутрішніх баз даних. Детальну інвентаризацію наявного обладнання представлено в таблиці 2.1, де чітко видно технічні обмеження кожного компонента.

Таблиця 2.1 – Поточна конфігурація мережевого обладнання

| № | Пристрій | Модель | IP-адреса | Порти | Швидкість | Стан |
|---|---|---|---|---|---|---|
| 1 | Маршрутизатор | TP-Link TL-WR841N | 192.168.1.1 | 4×LAN, 1×WAN | 100 Мбіт/с | Застаріле |
| 2 | Комутатор | D-Link DES-1008A | - | 8×RJ-45 | 100 Мбіт/с | Застаріле |
| 3 | Сервер | Dell PowerEdge T40 | 192.168.1.10 | 1×Gigabit* | 100 Мбіт/с* | Обмежений |
| 4 | Робочі станції | Lenovo ThinkCentre | 192.168.1.101-115 | 1×Fast Ethernet | 100 Мбіт/с | Працездатні |
| 5 | МФУ | HP LaserJet Pro | 192.168.1.50 | 1×Fast Ethernet | 100 Мбіт/с | Працездатний |

Як видно з таблиці 2.1, основним обмеженням є використання обладнання стандарту Fast Ethernet з пропускною здатністю 100 Мбіт/с, що не відповідає сучасним вимогам до швидкості передачі даних у локальних мережах установ, які працюють із великими обсягами документів і баз даних.

У рамках модернізації мережевої інфраструктури передбачається заміна застарілого обладнання на сучасні пристрої корпоративного класу. На рисунку 2.3 показано маршрутизатор MikroTik hEX S, який планується використати в модернізованій інфраструктурі замість існуючого TP- Link TL- WR841N. Цей пристрій підтримує гігабітні інтерфейси, апаратне шифрування IPSec, VPN-з’єднання і має вбудований міжмережевий екран із гнучкими можливостями налаштування політик безпеки.

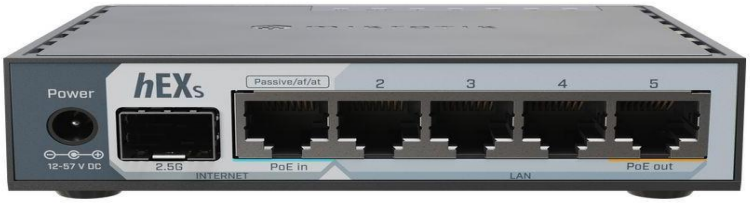

Рисунок 2.3 – Маршрутизатор MikroTik hEX S, використаний у модернізованій мережевій інфраструктурі

Для організації корпоративної бездротової мережі замість застарілих точок доступу стандарту 802.11n планується впровадження Ubiquiti UniFi 6 Lite, що підтримує стандарт Wi-Fi 6 і забезпечує значно вищу швидкість передачі даних, кращу продуктивність у середовищах із великою кількістю підключених пристроїв і підтримує сучасні алгоритми шифрування WPA3. На рисунку 2.4 зображено цю точку доступу, яка забезпечить стабільне покриття бездротовою мережею всієї площі установи.

Рисунок 2.4 – Точка доступу Ubiquiti UniFi 6 Lite (Wi-Fi 6) для організації корпоративної бездротової мережі

Центральним елементом інфраструктури залишиться сервер Dell PowerEdge T40, показаний на рисунку 2.5, який використовується для розміщення внутрішніх сервісів, зберігання даних і системи резервного копіювання. Цей сервер має достатню потужність процесора Intel Xeon,

підтримує RAID-масиви для забезпечення відмовостійкості даних і оснащений гігабітними мережевими інтерфейсами, однак його потенціал повністю не реалізується через обмеження застарілого комутатора.


Рисунок 2.5 – Сервер Dell PowerEdge T40, використаний для розміщення сервісів та резервування даних

Критичною проблемою існуючої мережі є відсутність централізованого моніторингу обладнання та мережевого трафіку. Адміністратор не має можливості контролювати стан портів, завантаженість каналів або вчасно виявляти збої, що ускладнює технічне обслуговування і призводить до того, що несправності усуваються лише після скарг користувачів. Для вирішення цієї проблеми в модернізованій інфраструктурі планується впровадження системи моніторингу Zabbix, інтерфейс якої показано на рисунку 2.6. Ця система забезпечує збір даних про стан обладнання в реальному часі, автоматичне сповіщення про збої та можливість прогнозування відмов на основі історичних даних.

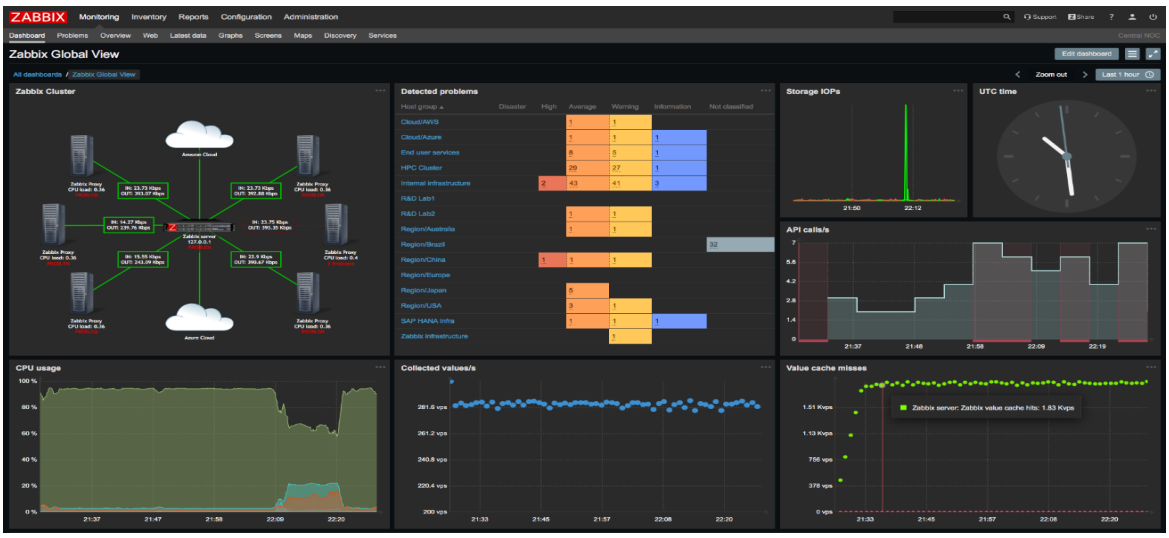


Рисунок 2.6 – Приклад дашборду системи моніторингу Zabbix для контролю роботи мережевої інфраструктури

Ще однією серйозною проблемою є недостатня пропускна здатність каналів локальної мережі, яка побудована на основі кабелю категорії Cat5, що фізично обмежує швидкість передавання до 100 Мбіт/с. При цьому реальні потреби установи перевищують цей рівень у 2-3 рази через збільшення кількості користувачів, інтеграцію з державними інформаційними системами та використання електронного документообігу. Як наслідок, під час пікових навантажень виникають затримки, спостерігаються розриви з'єднання з віддаленими серверами та хмарними сервісами, що знижує загальну продуктивність роботи співробітників.

Серйозною вразливістю є низький рівень кіберзахисту наявної інфраструктури. Єдиним засобом безпеки є базові функції маршрутизатора без окремого міжмережевого екрану або аналітичних систем виявлення вторгнень (IDS/IPS). Мережа не сегментована – внутрішній трафік співробітників, сервери та Wi-Fi користувачів передаються в одному логічному просторі, що створює ризик швидкого поширення шкідливого програмного забезпечення у разі інфікування одного з пристроїв. Відсутнє автоматизоване резервне копіювання критичних даних, немає чітких політик обмеження доступу до ресурсів і журналювання дій користувачів, що робить систему вразливою до

несанкціонованого втручання, витоку інформації або випадкового пошкодження даних.

Існуюча топологія побудована без урахування перспективи розширення мережі. Більшість комутаторів повністю зайняті, резервні порти відсутні, а система адресації IPv4 не оптимізована для можливого підключення нових робочих станцій, серверів або мережевих сервісів. Це унеможливлює швидке масштабування інфраструктури без заміни ключових вузлів мережі, що призводить до додаткових витрат і простоїв у роботі установи.

Точки доступу Wi-Fi підтримують лише застарілий стандарт 802.11n, працюють на перевантаженому діапазоні 2,4 ГГц і використовують алгоритм шифрування WPA2-PSK, який уже не вважається достатньо безпечним за сучасними стандартами. Не передбачено розмежування трафіку співробітників і відвідувачів через окремі VLAN або гостьові мережі, через що існує ризик перехоплення конфіденційних даних або несанкціонованого підключення до внутрішніх ресурсів. Також відсутні механізми фільтрації підключень за MAC- адресами і журналювання сесій користувачів для аудиту безпеки.

Мережа побудована за принципом одного маршрутизатора і комутатора без дублювання критичних компонентів. У разі відмови будь-якого з них зв’язок в установі повністю припиняється, що є критичним для органу місцевого самоврядування, оскільки унеможливлює доступ до баз даних, електронних сервісів і систем документообігу. Відсутність резервних каналів Інтернет-підключення також створює ризик повного відключення від зовнішніх мереж у разі проблем з єдиним провайдером.

Останньою проблемою є недостатня технічна підтримка мережевої інфраструктури. Відсутня окрема IT-служба або відповідальний інженер з належною кваліфікацією. Обслуговування мережі здійснюється епізодично сторонніми спеціалістами без належного документування змін у конфігурації обладнання, що ускладнює модернізацію, створює ризики втрати налаштувань і порушення стабільності під час оновлень програмного забезпечення або додавання нових компонентів.

Для підтвердження виявлених проблем було проведено детальний аналіз продуктивності існуючої мережі з використанням спеціалізованих утиліт моніторингу і тестування швидкості передачі даних. Результати цього аналізу узагальнено в таблиці 2.2, де показано порівняння виміряних параметрів із рекомендованими нормами для мереж сучасних установ.

Таблиця 2.2 – Показники продуктивності існуючої мережі

| Параметр | Виміряне значення | Норма | Відхилення |
|---|---|---|---|
| Пропускна здатність LAN (робоча станція сервер) | 85-94 Мбіт/с | ≥ 900 Мбіт/с | -90 % |
| Затримка (ping) до локального сервера | 3-5 мс | < 2 мс | +150 % |
| Затримка до зовнішніх ресурсів (8.8.8.8) | 18-25 мс | < 20 мс | Прийнятно |
| Втрати пакетів під навантаженням | 1,2-2,8 % | < 0,1 % | +2700 % |
| Час відновлення після збою маршрутизатора | 8-12 хв | < 2 хв | +500 % |
| Доступність сервісів (uptime за місяць) | 94,3 % | ≥ 99,5 % | -5,2 % |

Аналіз даних таблиці 2.2 показує, що найбільш критичними проблемами є недостатня пропускна здатність з відхиленням -90 % від норми, високі втрати пакетів під навантаженням, що перевищують норму в 27 разів, а також тривалий час відновлення після збоїв через відсутність резервування критичних компонентів. Показник доступності сервісів на рівні 94,3 % також не відповідає мінімальним вимогам для інфраструктури державних установ, де очікується безперервність функціонування на рівні не менше 99,5 %. Ці показники чітко підтверджують необхідність комплексної модернізації мережевої інфраструктури з заміною застарілого обладнання, впровадженням систем моніторингу і підвищенням рівня безпеки.

Таким чином, сучасний стан мережевої інфраструктури Поворської сільської ради не відповідає реальним потребам установи та вимогам до ефективності роботи органів місцевого самоврядування. Основними проблемами

залишаються низька швидкодія каналів передачі даних, відсутність системного моніторингу стану обладнання, використання застарілих пристроїв без підтримки сучасних стандартів безпеки та слабкий рівень захисту інформації від кіберзагроз. Подальше функціонування без модернізації може призвести до втрати критично важливих даних, порушення доступу до державних інформаційних систем, зниження ефективності роботи працівників і створення серйозних ризиків для інформаційної безпеки установи. Для підвищення надійності, продуктивності та ефективності функціонування мережі необхідно провести комплексну модернізацію, яка включатиме оновлення обладнання до сучасних стандартів, впровадження централізованої системи моніторингу, підвищення рівня кіберзахисту через сегментацію мережі та міжмережеві екрани, а також організацію резервування критичних компонентів для забезпечення безперервності роботи.

## 2.2 Вимоги до продуктивності, надійності й безпеки

Мережева інфраструктура органу місцевого самоврядування має бути побудована відповідно до сучасних стандартів продуктивності, надійності та безпеки, оскільки від її стабільної роботи безпосередньо залежить якість електронного документообігу, швидкість взаємодії між підрозділами, ефективність управлінських процесів і рівень захисту інформаційних ресурсів.

Продуктивність визначається здатністю мережі передавати дані з необхідною швидкістю без втрат і затримок навіть при збільшенні кількості користувачів або підключених сервісів. Для мережі Поворської сільської ради це означає підтримку гігабітних інтерфейсів на рівні 1 Гбіт/с для комутаторів і маршрутизаторів, а також широкосмугового інтернет-каналу не менше 100 Мбіт/с із можливістю подальшого розширення. Особливу увагу слід приділити параметрам затримки та втраті пакетів, які мають бути мінімальними, що є критично важливим для використання систем відеоконференцій, віддаленого адміністрування, синхронізації баз даних і роботи з хмарними

сервісами. Висока продуктивність також досягається за рахунок підтримки технологій QoS (Quality of Service), що дозволяє пріоритезувати трафік службових систем над другорядним, а також VLAN для розподілу навантаження між сегментами мережі.

Надійність мережевої інфраструктури полягає у її здатності працювати безперервно та відновлюватися після відмов з мінімальними втратами. Це передбачає реалізацію резервування критичних елементів, таких як маршрутизатори, комутатори та сервери, використання двох незалежних інтернет-провайдерів, а також наявність джерел безперебійного живлення для забезпечення роботи під час відключень електроенергії. Високий рівень надійності також забезпечується впровадженням систем централізованого моніторингу, які в реальному часі відстежують працездатність вузлів і дозволяють оперативно реагувати на проблеми. У поєднанні з регулярним резервним копіюванням даних на окремий сервер або у хмарне сховище це дає змогу гарантувати збереження інформації навіть у разі відмови обладнання.

Безпека мережі визначається комплексом технічних, програмних і організаційних заходів, спрямованих на запобігання несанкціонованому доступу, викраденню або спотворенню даних. У сучасних умовах необхідно реалізувати багаторівневий захист периметра мережі, який включає встановлення міжмережевого екрана нового покоління, систем виявлення та запобігання вторгненням, антивірусного захисту на робочих станціях і сервері. Для мінімізації внутрішніх ризиків мережу потрібно сегментувати на VLAN- зони, які окремо об’єднують сервери, робочі станції, Wi-Fi користувачів і відвідувачів. Для бездротового доступу рекомендується застосування стандарту WPA3 і автентифікації через централізований сервер на базі протоколу RADIUS.

Окрім технічних засобів, безпека значною мірою залежить від рівня підготовки персоналу. Необхідно проводити регулярні тренінги з кібергігієни, розробити політику паролів, систему контролю доступу за ролями та забезпечити ведення журналів подій для аудиту дій користувачів. Порівняльну характеристику основних вимог до мережевої інфраструктури наведено в

таблиці 2.3, де систематизовано ключові вимоги за трьома категоріями. Такі як продуктивність, надійність і безпека.

Таблиця 2.3 – Вимоги до продуктивності, надійності й безпеки мережевої інфраструктури

| Категорія | Вимога |
|---|---|
| Продуктивність | Висока пропускна здатність каналів передачі даних |
| Продуктивність | Можливість масштабування під збільшення кількості користувачів і сервісів |
| Продуктивність | Низька затримка при передачі даних у внутрішній мережі та при доступі до Інтернету |
| Надійність | Резервування критично важливого обладнання (маршрутизаторів, комутаторів, серверів) |
| Надійність | Мінімізація часу простою системи у випадку аварії |
| Надійність | Наявність систем резервного копіювання даних |
| Безпека | Використання сучасних методів шифрування та автентифікації |
| Безпека | Захист від DDoS-атак та несанкціонованого доступу |
| Безпека | Впровадження системи моніторингу подій безпеки та журналювання |

Як видно з таблиці 2.3, основними пріоритетами модернізованої мережевої інфраструктури є підвищення рівня безпеки, забезпечення стабільної продуктивності та зменшення ризику простоїв у роботі системи.

Таким чином, модернізована мережева інфраструктура повинна забезпечувати достатню продуктивність для підтримки сучасних сервісів, гарантувати безперервність роботи навіть у разі відмов окремих компонентів, а також мати комплексний захист від кіберзагроз. Лише поєднання цих трьох складових дозволить створити ефективну та стійку інформаційно-комунікаційну систему Поворської сільської ради. Крім того, така інфраструктура сприяє оптимальному використанню ресурсів і зменшенню витрат на обслуговування мережі, а впровадження сучасних технологій моніторингу та автоматичного сповіщення дозволяє оперативно реагувати на збої та потенційні загрози,

забезпечуючи високий рівень цифрової трансформації органу місцевого самоврядування.

### 2.3 Обґрунтування вибору засобів моніторингу та захисту

У процесі модернізації мережевої інфраструктури Поворської сільської ради одним із ключових завдань є впровадження надійних інструментів моніторингу та кіберзахисту. Це необхідно для забезпечення стабільного функціонування інформаційних сервісів, контролю стану мережевого обладнання, а також своєчасного виявлення та усунення загроз інформаційній безпеці. Вибір програмних засобів має враховувати реальні умови роботи установи, зокрема обмежені фінансові ресурси, потребу в безперервності сервісів і простоту адміністрування без залучення великої кількості технічного персоналу.

Для ефективного моніторингу мережевої інфраструктури доцільно обрати рішення, які забезпечують комплексне спостереження за станом мережі, серверів і робочих станцій. Найоптимальнішими за співвідношенням функціональності, вартості та гнучкості налаштування є системи з відкритим кодом та комерційні рішення, що мають доведену ефективність у невеликих організаціях. Серед таких систем варто виділити Zabbix, який забезпечує централізований моніторинг серверів, комутаторів, маршрутизаторів і мережевих сервісів у режимі реального часу. Його перевагами є безкоштовність, підтримка візуалізації даних, масштабованість і можливість інтеграції з системами сповіщень, що особливо важливо для невеликих органів влади з обмеженим IT-бюджетом.

Альтернативним варіантом є PRTG Network Monitor, комерційне рішення з зручним інтерфейсом, автоматичним виявленням пристроїв у мережі та наочними графічними звітами [23]. Його доцільно використовувати у випадках, коли потрібна швидка інтеграція без складного налаштування, однак платна ліцензія може бути обмежувальним фактором. Для діагностики складних мережевих інцидентів також корисним є застосування Wireshark, аналізатора

трафіку, який дозволяє досліджувати пакети даних, виявляти проблеми з передачею або некоректну роботу протоколів.

Застосування зазначених систем дозволяє підвищити прозорість роботи мережі, забезпечити аналітику навантаження та скоротити час реагування на інциденти. Враховуючи бюджетні обмеження, оптимальним вибором для Поворської сільської ради є Zabbix [25], оскільки він поєднує глибокий функціонал, відкриту ліцензію та можливість розширення без додаткових витрат. Система дозволяє відстежувати роботу критичних сервісів, контролювати навантаження на сервери, реєструвати історію подій і формувати детальні звіти для прийняття управлінських рішень.

Для реалізації комплексного підходу до безпеки пропонується впровадження кількох взаємопов'язаних компонентів, які формують багаторівневий захист мережевої інфраструктури. Ключовим елементом периметрового захисту є міжмережевий екран на базі MikroTik RouterOS, який забезпечує фільтрацію трафіку, блокування підозрілих підключень та запобігання мережевим атакам. MikroTik RouterOS надає широкі можливості для налаштування політик доступу, глибокого аналізу трафіку та інтеграції з системами моніторингу [12], що дозволяє створити єдиний контур безпеки та контролю.

Для захисту робочих станцій і серверів від шкідливого програмного забезпечення рекомендовано впровадити антивірусне та антималварне програмне забезпечення корпоративного рівня, зокрема ESET Endpoint Security або Avast Business Security [19]. Ці рішення забезпечують регулярне оновлення баз загроз, централізоване керування через вебконсоль і мінімальне навантаження на систему, що важливо для підтримання продуктивності робочих станцій. Окрім цього, для безпечного віддаленого підключення співробітників до внутрішніх ресурсів необхідно використовувати VPN-технології [27], які дозволяють шифрувати трафік і захищати дані від перехоплення під час передачі через публічні мережі.

Важливою складовою системи безпеки є впровадження резервного копіювання критичних даних. Застосування програм Veeam Backup & Replication або Acronis Cyber Protect [11] дає змогу зберігати архівні копії інформації на окремому сервері або у хмарному сховищі, що гарантує можливість швидкого відновлення даних після інцидентів, включаючи апаратні відмови або кібератаки. Також необхідною є сегментація мережі через створення окремих віртуальних локальних мереж (VLAN), що дозволяє ізолювати службові дані від гостьових підключень і мінімізувати ризик несанкціонованого доступу.

Порівняльну характеристику основних засобів моніторингу та захисту інформаційних систем наведено в таблиці 2.4, де систематизовано ключові параметри кожного рішення. Як видно з таблиці 2.4, найбільш збалансованими за співвідношенням «функціональність-вартість» є рішення Zabbix для моніторингу та MikroTik RouterOS для захисту, які забезпечують комплексний моніторинг і базовий рівень захисту мережевої інфраструктури без значних фінансових витрат.

Таблиця 2.4 – Порівняння засобів моніторингу та захисту інформаційних систем

| Засіб | Призначення | Переваги | Недоліки |
|---|---|---|---|
| Zabbix | Централізований моніторинг мережі та серверів | Безкоштовний, масштабований, гнучкі налаштування | Складність налаштування, потребує ресурсів сервера |
| PRTG Network Monitor | Моніторинг мережі з графічними звітами та дашбордами | Зручний інтерфейс, наочні графіки, легкість у використанні | Платна ліцензія для великих мереж, обмеження у free-версії |
| Nagios | Контроль доступності сервісів і обладнання | Стабільність, великий набір плагінів, відкритий код | Складний інтерфейс, потребує досвіду адміністрування |
| ESET | Антивірусний захист кінцевих пристроїв | Надійний захист, регулярні оновлення баз | Платна корпоративна версія, навантаження на систему |
| Avast Business | Хмарний антивірус та кіберзахист малого бізнесу | Легкий у розгортанні, оптимальний для малого бізнесу | Менш потужний захист у порівнянні з ESET |

Детальні порівняльні технічні характеристики основного мережевого обладнання наведено в додатку А, що дозволяє глибше оцінити технічні можливості кожного компонента системи. З огляду на технічні вимоги, обмежений бюджет і необхідність централізованого управління, оптимальною є комбінація відкритого моніторингу Zabbix із апаратним міжмережевим екраном на базі MikroTik RouterOS та корпоративним антивірусом ESET. Така конфігурація забезпечує комплексне відстеження роботи мережевих вузлів і серверів, виявлення перевантажень і можливих аномалій у трафіку, багаторівневий кіберзахист від вірусів, фішингових атак і несанкціонованого доступу, а також безпечний віддалений доступ співробітників через VPN.

Інтеграція цих засобів створює єдиний моніторингово-захисний контур, що дозволяє не лише реагувати на інциденти, а й прогнозувати ризики на основі аналітики мережевих подій. Це відповідає принципам проактивного управління інформаційною безпекою, коли система не просто фіксує помилки, а запобігає їхньому виникненню. Запропоновану архітектуру системи моніторингу на базі Zabbix представлено на рисунку 2.7, де показано централізований збір даних з мережевого обладнання через протокол SNMP та з кінцевих пристроїв через Zabbix Agent.

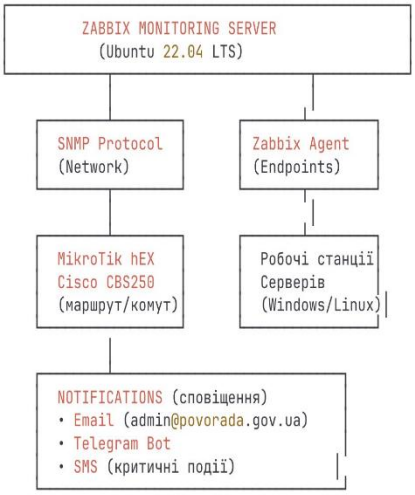


Рисунок 2.7 – Архітектура системи моніторингу на базі Zabbix

Запропонована архітектура передбачає централізований збір даних з мережевого обладнання через SNMP та з кінцевих пристроїв через Zabbix Agent. При виявленні відхилень від порогових значень, таких як завантаження процесора понад 80 %, використання оперативної пам’яті понад 90 % або втрата пакетів понад 1 %, система автоматично надсилає сповіщення адміністратору через електронну пошту або месенджер Telegram. Це дозволяє оперативно реагувати на проблеми ще до того, як вони вплинуть на роботу користувачів.

Таким чином, обрані засоби моніторингу та захисту повністю відповідають сучасним стандартам побудови безпечних інформаційно-комунікаційних систем, а також можливостям місцевого бюджету. Їх впровадження забезпечить стабільність, безперервність і безпеку функціонування інформаційної інфраструктури Поворської сільської ради. Крім того, інтеграція систем моніторингу та захисту дозволяє реалізувати проактивний підхід до управління мережею, коли потенційні загрози та проблеми виявляються на ранніх етапах і усуваються до того, як вони вплинуть на роботу користувачів. Такий підхід сприяє зниженню ризиків простою, підвищенню ефективності управлінських процесів та гарантуванню високого рівня безпеки інформації в Поворській сільській раді, що відповідає вимогам цифрової трансформації органів місцевого самоврядування.

# РОЗДІЛ 3
# ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ МОДЕРНІЗОВАНОЇ МЕРЕЖІ

Сучасні вимоги до ефективності діяльності органів місцевого самоврядування потребують створення надійної, безпечної та масштабованої мережевої інфраструктури, яка забезпечує безперервний обмін інформацією, підтримку електронного документообігу та доступ до державних інформаційних ресурсів. Модернізація мережі Поворської сільської ради спрямована на усунення виявлених проблем, підвищення продуктивності, розширення функціональних можливостей і забезпечення належного рівня кіберзахисту.

Успішна модернізація мережевої архітектури вимагає системного підходу, який охоплює детальний аналіз існуючої інфраструктури, обґрунтований вибір технічних засобів, проєктування оптимальної топології мережі, створення ефективної системи моніторингу та інтеграцію сучасних засобів захисту інформації. Кожен із цих етапів має бути узгодженим із загальною стратегією цифрової трансформації установи та враховувати специфіку роботи органу місцевого самоврядування.

Особлива увага при проєктуванні приділяється забезпеченню безперебійності роботи інформаційних сервісів, оскільки навіть короткочасні збої можуть призвести до порушення надання адміністративних послуг громадянам. Це досягається шляхом резервування критично важливих ресурсів, використання відмовостійких архітектурних рішень і впровадження сучасних протоколів безпеки, що гарантують захист від несанкціонованого доступу та кіберзагроз.

Важливим аспектом модернізації є забезпечення гнучкості системи, тобто можливості її подальшого розширення без необхідності кардинальної зміни базової архітектури. Це передбачає вибір масштабованих технологічних рішень, які дозволяють підключати нові робочі місця, сервери та мережеві сегменти без суттєвого збільшення витрат на обладнання та адміністрування. Водночас

система має підтримувати сучасні стандарти передавання даних, шифрування трафіку та централізованого управління мережевими ресурсами.

Таким чином, головною метою даного розділу є розроблення комплексного проєкту модернізованої мережевої інфраструктури для Поворської сільської ради, яка відповідатиме актуальним вимогам до продуктивності, надійності, безпеки та гнучкості системи управління інформаційними ресурсами, а також забезпечить стабільну основу для впровадження нових цифрових сервісів у майбутньому.

### 3.1 Розробка проєктної моделі мережі

Проєктна модель мережевої інфраструктури Поворської сільської ради базується на аналізі виявлених проблем існуючої системи та визначених вимогах до модернізації. Основною метою є створення надійної, масштабованої та захищеної архітектури, яка забезпечить стабільну роботу інформаційних сервісів, ефективний моніторинг мережевих ресурсів і багаторівневий захист від кіберзагроз. Проєктна модель модернізованої мережевої інфраструктури представлена на рисунку 3.1.

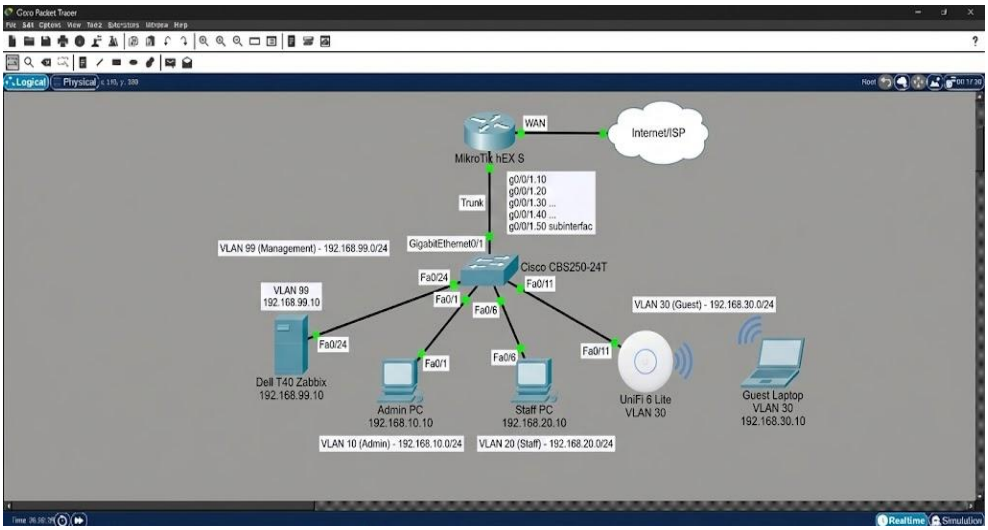


Рисунок 3.1 – Створення та початкове проєктування мережевої топології в Cisco Packet Tracer

Центральним елементом модернізованої мережі є маршрутизатор MikroTik hEX S, який виконує функції мережевого шлюзу, міжмережевого екрану та контролера VLAN-сегментації. Цей пристрій забезпечує високу продуктивність обробки трафіку, підтримку сучасних протоколів безпеки та гнучкість налаштувань через операційну систему MikroTik RouterOS. Маршрутизатор підтримує апаратне прискорення IPSec, що дозволяє організовувати захищені VPN-тунелі без суттєвого зниження швидкості передачі даних. Крім того, RouterOS надає широкі можливості для налаштування політик фільтрації трафіку, контролю пропускної здатності через механізми QoS та централізованого управління мережевими правилами.

Для забезпечення розподілу трафіку між робочими станціями та сегментації мережі використовується керований комутатор MikroTik CRS326-24G-2SRM, який підтримує технологію VLAN, пріоритезацію трафіку через QoS і віддалений моніторинг через протокол SNMP. Цей комутатор має двадцять чотири гігабітні порти Ethernet та два порти SFP для підключення оптоволоконних ліній зв’язку у випадку майбутнього розширення інфраструктури. Застосування керованого комутатора дозволяє створити логічно ізольовані мережеві сегменти для різних груп користувачів, що підвищує безпеку та спрощує адміністрування системи.

Серверна частина інфраструктури базується на сервері Dell PowerEdge T40, який оснащений процесором Intel Xeon E-2224G, оперативною пам’яттю обсягом шістнадцять гігабайт і підтримує технологію програмного або апаратного RAID для забезпечення відмовостійності дисків. На цьому сервері розгортаються ключові служби, включаючи систему моніторингу, сервіси резервного копіювання, а також локальні вебпортали та бази даних. Використання серверного обладнання корпоративного класу гарантує стабільність роботи критичних сервісів навіть у періоди високого навантаження.

Для забезпечення бездротового доступу впроваджено точки доступу Ubiquiti UniFi 6 Lite, які підтримують стандарт Wi-Fi 6 і забезпечують високу швидкість передачі даних, сучасні алгоритми шифрування WPA3 та можливість

централізованого управління через контролер UniFi. Ці точки доступу дозволяють створити окремі бездротові мережі для співробітників і відвідувачів із різними рівнями доступу до внутрішніх ресурсів, що підвищує загальний рівень безпеки мережевої інфраструктури. Окрім цього, передбачено використання джерел безперебійного живлення для критичних компонентів мережі, таких як маршрутизатор, комутатор і сервер, що дозволяє уникнути втрати даних і збоїв у роботі сервісів під час короткочасних відключень електроенергії.

Архітектура мережі передбачає чітку ієрархію компонентів, де основними рівнями є рівень доступу для підключення кінцевих пристроїв, рівень розподілу для управління трафіком між сегментами та ядерний рівень для забезпечення зв'язку з зовнішніми мережами. Така структура дозволяє ефективно масштабувати систему, додавати нові вузли без зміни базової конфігурації та забезпечує простоту діагностики і усунення неполадок. Топологія побудована за принципом зірки з центральним комутатором, що спрощує фізичне розгортання кабельної інфраструктури та дозволяє контролювати кожен порт окремо.

Ключовим елементом проєктної моделі є впровадження технології віртуальних локальних мереж, яка дозволяє логічно розділити фізичну мережу на окремі ізольовані сегменти відповідно до функціональних потреб організації. Топологія модернізованої мережі з сегментацією VLAN представлена на рисунку 3.2.

Створено три основні сегменти:

– VLAN 10 призначений для адміністративних робочих станцій, де зберігаються конфіденційні дані і забезпечується найвищий рівень контролю доступу;

– VLAN 20 використовується для службових комп'ютерів співробітників, які мають обмежений доступ до внутрішніх ресурсів відповідно до своїх посадових обов'язків;

– VLAN 30 виділений для гостьової бездротової мережі Wi-Fi, де відвідувачі мають доступ лише до Інтернету без можливості взаємодії з внутрішніми сервісами установи.

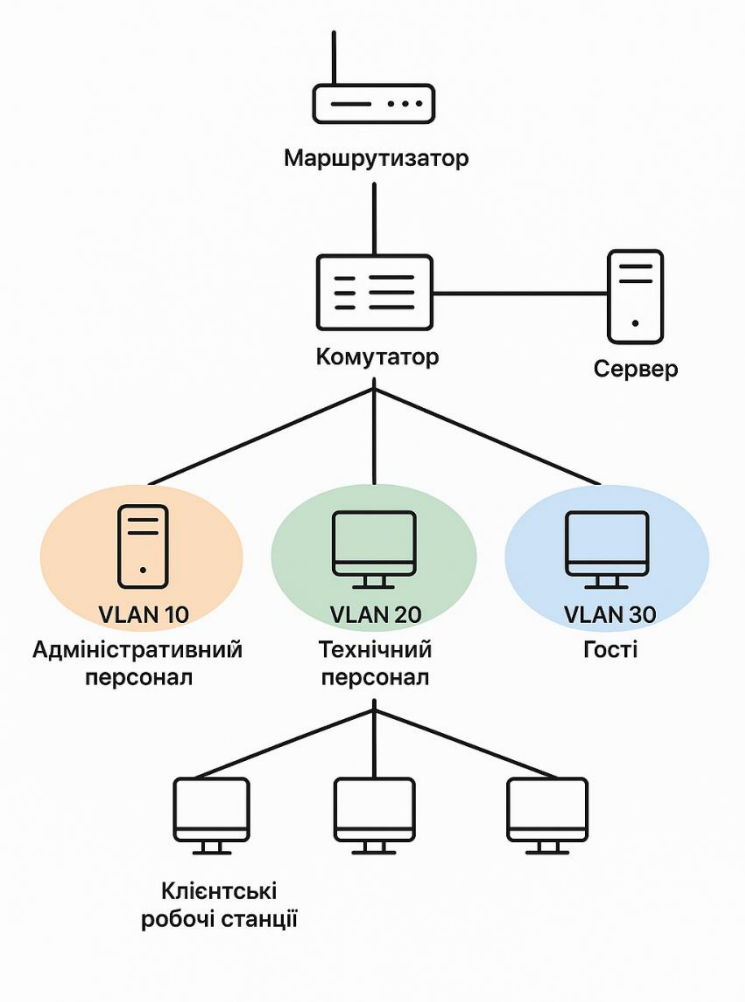


Рисунок 3.2 – Проєктна схема локальної мережі Поворської сільської ради

Кожен VLAN має власний діапазон IP-адрес, окремий шлюз і налаштування DHCP-сервера, що забезпечує автоматичне призначення мережевих параметрів пристроям при підключенні. Для гостьової мережі VLAN 30 додатково налаштовано використання зовнішніх DNS-серверів Google DNS із адресою 8.8.8.8, що дозволяє уникнути перевантаження внутрішніх служб і забезпечує стабільну роботу навіть при великій кількості одночасних підключень.

Проєктування та тестування мережевої конфігурації здійснювалося з використанням спеціалізованих емуляторів мережевого обладнання GNS3 та EVE-NG, які дозволяють створювати віртуальні середовища для моделювання роботи реальних пристроїв. Це дало можливість перевірити правильність налаштувань VLAN, протестувати політики міжмережевого екрану, оцінити ефективність механізмів QoS і переконатися у стабільності VPN-з'єднань ще до фізичного розгортання обладнання. Використання віртуального середовища значно скоротило час налаштування та зменшило ризик помилок конфігурації на етапі впровадження.

До складу проєктної моделі входять також механізми забезпечення відмовостійкості, зокрема технологія агрегації каналів LACP, яка дозволяє об'єднувати кілька фізичних з'єднань у один логічний канал із підвищеною пропускною здатністю та автоматичним переключенням у разі відмови одного з портів. Для серверів передбачено застосування дискових масивів RAID 1 або RAID 5, які забезпечують збереження даних навіть у випадку виходу з ладу одного з жорстких дисків. Крім того, впроваджено систему регулярного резервного копіювання критичних даних з використанням програмних рішень Veeam Backup або Acronis, що гарантує можливість швидкого відновлення інформації після інцидентів різного характеру.

Мережева адресація побудована на базі приватного діапазону IP-адрес класу C із підмережею 192.168.x.x/24, що забезпечує достатній запас адрес для поточних і майбутніх потреб організації. Для кожного сегменту виділено окремий діапазон адрес, а статичні IP-адреси призначаються критичним пристроям, таким як сервери, принтери та точки доступу, що спрощує адміністрування та моніторинг мережі. Динамічне призначення адрес здійснюється через централізований DHCP-сервер на базі маршрутизатора MikroTik із налаштуванням окремих пулів для кожного VLAN.

Організація VPN-доступу базується на використанні протоколів IPsec, OpenVPN і L2TP, які забезпечують шифрування трафіку під час віддаленого підключення співробітників до внутрішніх ресурсів установи. Міжмережевий

екран на базі MikroTik RouterOS налаштовано відповідно до принципів мінімальних привілеїв [20], коли за замовчуванням весь вхідний трафік блокується, а дозволяються лише необхідні служби та порти. Додатково впроваджено механізми захисту від DDoS-атак, фільтрацію пакетів із підозрілими характеристиками та ведення централізованих журналів подій через протокол Syslog для подальшого аналізу в системі моніторингу Zabbix.

Налаштування мережі здійснено з дотриманням міжнародних стандартів і рекомендацій, зокрема IEEE для мережевих протоколів і ISO/IEC 27001 для забезпечення інформаційної безпеки. Детальна схема підключення комутатора MikroTik CRS326-24G-2SRM із розподілом портів за VLAN представлена на рисунку 3.3, де показано логічну структуру підключення робочих станцій, серверів, принтерів і точок доступу до відповідних мережевих сегментів.

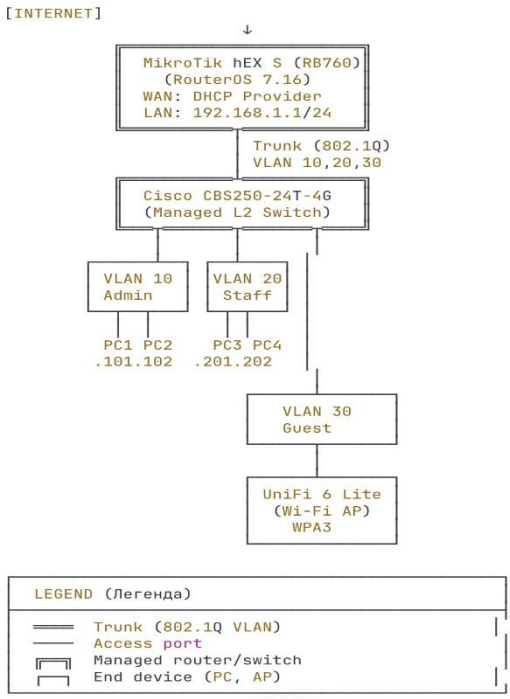


Рисунок 3.3 – Логічна топологія модернізованої мережі

Таблиця 3.1 містить детальний опис конфігурації IP-адресації для кожного VLAN, включаючи діапазони адрес, шлюзи, пули DHCP і DNS-сервери. Ця таблиця є основою для подальшого налаштування мережевого обладнання та документування інфраструктури.

Таблиця 3.1 – Детальна схема IP-адресації модернізованої мережі

| VLAN | Назва | Підмережа | Gateway | DHCP Pool | DNS | Призначення |
|---|---|---|---|---|---|---|
| - | WAN | DHCP | Provider | - | 8.8.8.8 | Інтернет-канал |
| 10 | Admin | 192.168.10.0/24 | .1 | .100-.199 | 192.168.10.1 | Адмін персонал (5 ПК) |
| 20 | Staff | 192.168.20.0/24 | .1 | .100-.199 | 192.168.20.1 | Співробітники (10 ПК) |
| 30 | Guest | 192.168.30.0/24 | .1 | .100-.250 | 8.8.8.8 | Гості Wi-Fi (ізольовано) |
| 99 | Management | 192.168.99.0/24 | .1 | .10-.50 | 192.168.99.1 | Управління обладнанням |

Відповідність між VLAN, IP-адресами та MAC-адресами обладнання систематизована у таблиці 3.2, що спрощує процес усунення неполадок у мережі.

Таблиця 3.2 – Статичні адреси критичних пристроїв

| Пристрій | VLAN | IP-адреса | MAC-адреса | Коментар |
|---|---|---|---|---|
| MikroTik hEX S (ether2) | 10 | 192.168.10.1 | - | Gateway VLAN 10 |
| MikroTik hEX S (vlan20) | 20 | 192.168.20.1 | - | Gateway VLAN 20 |
| MikroTik hEX S (vlan30) | 30 | 192.168.30.1 | - | Gateway VLAN 30 |
| Сервер Dell T40 | 10 | 192.168.10.10 | 00:1A:2B:3C:4D:5E | Файл-сервер |
| Принтер HP | 20 | 192.168.20.50 | 00:11:22:33:44:55 | Мережевий принтер |

| | | | | |
|---|---|---|---|---|
| Cisco CBS250 (management) | 99 | 192.168.99.2 | - | Управління комутатором |
| Zabbix Server | 99 | 192.168.99.10 | - | Моніторинг |

Таким чином, розроблена проєктна модель мережевої інфраструктури Поворської сільської ради враховує всі виявлені проблеми існуючої системи та забезпечує реалізацію сучасних вимог до продуктивності, надійності, масштабованості та безпеки. Впровадження технологій сегментації мережі, централізованого моніторингу, багаторівневого захисту та резервування критичних ресурсів дозволить суттєво підвищити ефективність роботи установи, забезпечити безперебійність надання адміністративних послуг і створити надійну основу для подальшої цифрової трансформації громади. Час на налаштування модернізованої мережі оцінюється у півтора-два робочі дні, а термін повного впровадження всіх компонентів системи становить приблизно тридцять п’ять-сорок днів з урахуванням постачання обладнання, фізичного монтажу, налаштування та тестування.

На рисунку 3.4 показано інтерфейс WinBox із налаштованими VLAN- інтерфейсами для сегментації мережі. Як видно зі скриншоту, створено чотири основні VLAN: VLAN 10 для адміністративного персоналу, VLAN 20 для співробітників, VLAN 30 для гостьової мережі Wi-Fi та VLAN 99 для управління обладнанням. Кожен VLAN має налаштовані L2 MTU та L3 MTU параметри, що забезпечує оптимальну продуктивність передачі даних.

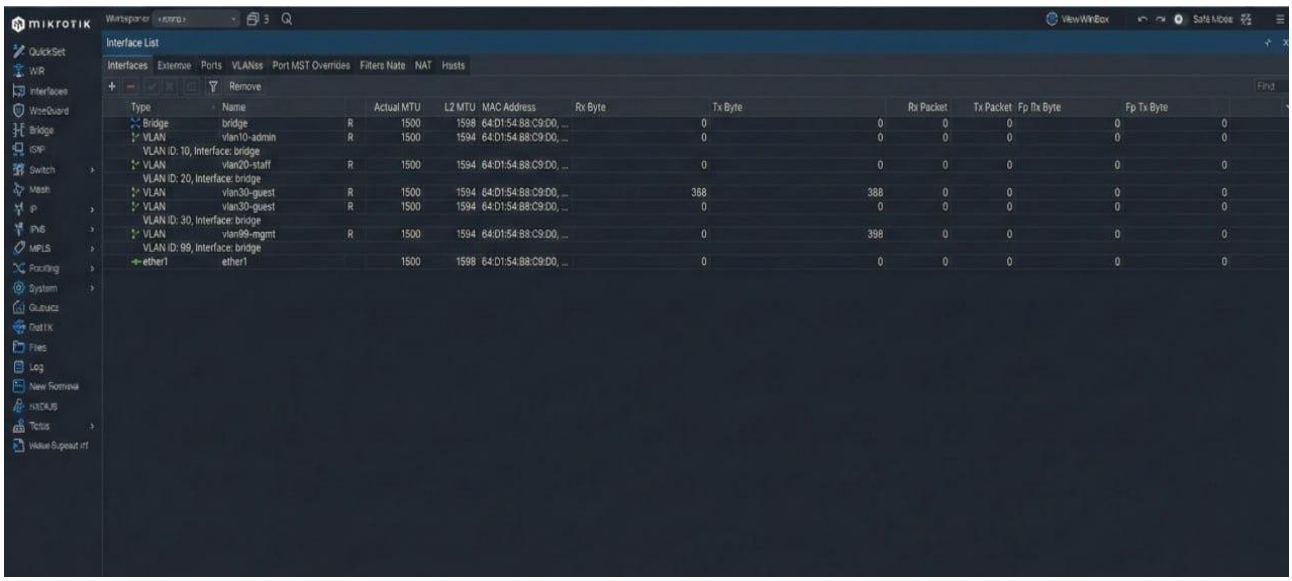


Рисунок 3.4 – Інтерфейс WinBox із налаштованими VLAN-інтерфейсами

## 3.2 Вибір апаратного та програмного забезпечення

Успішна реалізація проєктної моделі мережевої інфраструктури безпосередньо залежить від правильного вибору апаратних і програмних компонентів, які мають забезпечити надійність, продуктивність, безпеку та можливість подальшого масштабування системи. Вибір обладнання та програмного забезпечення здійснювався на основі детального аналізу потреб організації, бюджетних обмежень і сучасних технологічних стандартів у галузі побудови корпоративних мережевих інфраструктур.

Ключовим елементом мережевої архітектури є маршрутизатор, який виконує функції шлюзу між локальною мережею та Інтернетом, забезпечує функціонування міжмережевого екрану, контролює потоки трафіку та підтримує механізми сегментації через технологію VLAN. Для цих цілей обрано MikroTik hEX S, який відповідає всім технічним вимогам модернізованої мережі завдяки підтримці п’яти гігабітних портів Ethernet, апаратному прискоренню IPSec для організації захищених VPN-з’єднань і гнучкій операційній системі RouterOS із широкими можливостями налаштування правил фільтрації, маршрутизації та управління якістю обслуговування через механізми QoS.

Розподіл трафіку між робочими станціями та серверами здійснюється через керований комутатор другого рівня, який підтримує технологію VLAN для

логічної сегментації мережі, пріоритезацію трафіку для критичних служб і віддалений моніторинг через протокол SNMP. У проєкті використовується комутатор MikroTik CRS326-24G-2SRM із двадцятьма чотирма гігабітними портами Ethernet і двома портами SFP, що забезпечує достатній запас для підключення всіх поточних пристроїв і дозволяє легко розширювати інфраструктуру у майбутньому без необхідності заміни базового обладнання.

Серверна частина інфраструктури базується на надійному й продуктивному рішенні корпоративного класу Dell PowerEdge T40, оснащеному чотирьохядерним процесором Intel Xeon E-2224G, оперативною пам'яттю обсягом шістнадцять гігабайт типу ECC для запобігання помилкам під час обробки даних і двома жорсткими дисками ємністю по одному терабайту, об'єднаними у масив RAID 1 для забезпечення відмовостійкості та захисту від втрати даних у разі виходу з ладу одного з дисків. Цей сервер використовується для розгортання системи моніторингу, служб резервного копіювання, внутрішніх вебпорталів і баз даних організації.

Для забезпечення бездротового доступу співробітників і відвідувачів впроваджено точки доступу Ubiquiti UniFi 6 Lite, які підтримують найновіший стандарт Wi-Fi 6 із підвищеною швидкістю передачі даних, сучасні механізми шифрування WPA3 і можливість централізованого управління через програмний контролер UniFi Network Application. Використання цих точок доступу дозволяє створити окремі бездротові мережі для різних груп користувачів із різними рівнями доступу до внутрішніх ресурсів, що суттєво підвищує загальний рівень безпеки.

Критично важливі компоненти мережевої інфраструктури, такі як маршрутизатор, комутатор і сервер, підключаються до джерел безперебійного живлення APC Smart-UPS серії SMT1500I потужністю тисяча п'ятсот вольт- ампер, що забезпечує автономну роботу обладнання протягом достатнього часу для коректного завершення робочих процесів і збереження даних у разі раптового відключення електроенергії. Це особливо важливо для органів місцевого самоврядування, де навіть короткочасні збої можуть призвести

до втрати критичної інформації або порушення надання адміністративних послуг громадянам.

Програмне забезпечення для модернізованої мережевої інфраструктури включає серверну операційну систему Linux Ubuntu Server версії 22.04 LTS, яка є стабільною, безкоштовною та має тривалий термін підтримки, що забезпечує регулярне отримання оновлень безпеки та виправлень помилок. Для робочих станцій використовується операційна система Windows 11 Pro, яка забезпечує сумісність із корпоративними додатками та підтримує сучасні механізми захисту інформації.

Система моніторингу мережевої інфраструктури реалізована на базі безкоштовного відкритого рішення Zabbix, яке дозволяє здійснювати централізований контроль стану всіх компонентів мережі в режимі реального часу, збирати статистику продуктивності, формувати звіти та автоматично сповіщати адміністраторів про критичні події через електронну пошту або мобільні додатки. Для антивірусного захисту робочих станцій і серверів впроваджено корпоративне рішення ESET Endpoint Security, яке забезпечує централізоване управління через вебконсоль, регулярне оновлення баз загроз і мінімальне навантаження на системні ресурси.

Організація захищеного віддаленого доступу до внутрішніх ресурсів здійснюється через вбудовані VPN-можливості маршрутизатора MikroTik із підтримкою сучасних протоколів шифрування. Резервне копіювання критичних даних реалізується через програмне забезпечення Veeam Backup & Replication, яке дозволяє створювати повні та інкрементні копії інформації, зберігати їх на окремих носіях і швидко відновлювати систему після будь-яких інцидентів. Для глибокого аналізу мережевого трафіку та діагностики складних проблем використовується безкоштовний аналізатор пакетів Wireshark, який дає змогу детально досліджувати структуру переданих даних і виявляти аномалії в роботі мережевих протоколів.

Усі компоненти Sпрограмного забезпечення підтримують стандартні мережеві протоколи, зокрема TCP/IP для передачі даних, SNMP для моніторингу

обладнання, HTTPS для безпечного доступу до веб-інтерфейсів управління, а також інтегруються між собою для забезпечення єдиного простору адміністрування та контролю. Використання відкритих стандартів і популярних рішень забезпечує сумісність компонентів різних виробників і дозволяє уникнути залежності від одного постачальника технологій.

Детальна специфікація обраного обладнання та програмного забезпечення з розрахунком кошторисної вартості представлена у додатку Б, де систематизовано інформацію про кожен компонент інфраструктури, його технічні характеристики, кількість одиниць і вартість придбання.

Архітектура програмного забезпечення модернізованої мережевої інфраструктури представлена на рисунку 3.5, де показано взаємозв'язок між компонентами системи моніторингу, захисту, резервування та управління мережевими ресурсами. Ця архітектура забезпечує повну інтеграцію всіх складових і дозволяє ефективно контролювати роботу інфраструктури через єдину панель адміністрування.


Рисунок 3.5 – Архітектура програмного забезпечення модернізованої мережевої інфраструктури

Таким чином, обране апаратне та програмне забезпечення повністю відповідає визначеним вимогам до модернізації мережевої інфраструктури Поворської сільської ради, забезпечує необхідний рівень продуктивності, надійності та безпеки, а також створює міцну основу для подальшого розвитку інформаційних систем організації. Використання перевірених комерційних і

відкритих рішень дозволяє оптимізувати витрати на впровадження та експлуатацію системи, зберігаючи при цьому високу якість і функціональність мережевих сервісів.

### 3.3 Організація системи моніторингу та впровадження елементів захисту

Система моніторингу та захисту є невід'ємною складовою сучасної інформаційної інфраструктури, оскільки саме вона забезпечує безперервний контроль за станом мережі, своєчасне виявлення збоїв, а також запобігання несанкціонованому доступу до даних. Її ефективна організація гарантує стабільну роботу всіх компонентів мережі та високий рівень інформаційної безпеки.

Система моніторингу передбачає постійний збір та аналіз інформації про стан обладнання, мережі з'єднання, швидкість передавання даних, навантаження на сервері та працездатність користувацьких станцій. Для цього використовуються спеціалізовані програмні засоби, такі як PRTG Network Monitor, Zabbix, Nagios та SolarWinds, хоча у нашому проєкті основна увага приділяється системі Zabbix як найбільш доцільному вибору для органів місцевого самоврядування. Вони дозволяють у режимі реального часу контролювати роботу мережі, отримувати повідомлення про збої, фіксувати підозріту активність та аналізувати тенденції використання ресурсів.

Zabbix забезпечує централізований моніторинг усіх критичних складових мережевої інфраструктури Поворської сільської ради, включаючи маршрутизатор MikroTik hEX S, комутатор MikroTik CRS326-24G-2SRM, сервер Dell PowerEdge T40 і робочі станції користувачів. Система збирає метрики про завантаженість процесора, використання оперативної пам'яті, обсяг вільного місця на дисках, пропускну здатність мережевих портів та статус критичних сервісів. На основі зібраних даних Zabbix формує графіки, звіти та аналітичні

дашборди, що дозволяють адміністраторам оцінити поточний стан інфраструктури та виявити потенційні вузькі місця в системі.

Важливою складовою моніторингу є ведення журналів подій (логів), які фіксують усі дії користувачів, підключення до системи, спроби доступу до захищених ресурсів та технічні помилки. Централізоване зберігання логів дозволяє швидко провести аудит безпеки та виявити причини збоїв. Система оповіщення адміністраторів через електронну пошту або мобільні додатки (Telegram) забезпечує оперативне реагування на інциденти.

Для гарантування цілісності та конфіденційності даних у мережі впроваджується багаторівнева система захисту, що включає: міжмережеві екрани (Firewall) контролюють вхідний і вихідний трафік, блокуючи несанкціоновані з'єднання; системи виявлення та запобігання вторгненням (IDS/IPS) аналізують мережеві пакети та виявляють спроби атак; антивірусний захист забезпечує перевірку файлів і веб-трафіку на наявність шкідливого програмного забезпечення; VPN-з'єднання використовуються для безпечного підключення віддалених користувачів до внутрішньої мережі; системи резервного копіювання гарантують збереження даних у випадку технічних несправностей або кібератак; важливою складовою захисту є впровадження політики керування доступом, яка визначає права користувачів відповідно до їхніх посадових обов'язків.

Аутентифікація здійснюється через централізований сервер (наприклад, Active Directory), що забезпечує контроль доступу до ресурсів, файлів і сервісів. Для підвищення безпеки можуть бути застосовано багатофакторну аутентифікацію.

Ефективна система захисту потребує постійного вдосконалення. Регулярне оновлення програмного забезпечення, перевірка налаштувань безпеки та періодичний аудит дозволяють своєчасно усувати вразливості. Таким важливим є проведення навчання персоналу щодо правил кіберігієни та безпечного користування корпоративними ресурсами.

Для забезпечення багаторівневого захисту було реалізовано комплексну конфігурацію міжмережевого екрану на базі MikroTik RouterOS (лістинг 3.1). Конфігурація включає механізми Connection State Tracking для відстеження станів з'єднань, систему виявлення Port Scanning з автоматичним занесенням джерел атак у чорний список на 2 тижні, захист від ICMP Flood шляхом обмеження до 5 пакетів на секунду та обмеження адміністративного доступу виключно з Management VLAN (192.168.99.0/24). Впровадження політики Default Drop гарантує, що весь трафік, який не відповідає явно дозволеним правилам, автоматично блокується.

Лістинг 3.1 – Базова конфігурація Firewall MikroTik RouterOS

```
# Налаштування Connection State Tracking
/ip firewall filter
add chain=input action=accept connection-state=established,related \
    comment="Дозволити встановлені з'єднання"
add chain=input action=drop connection-state=invalid \
    comment="Блокувати невалідні пакети"
add chain=forward action=accept connection-state=established,related
add chain=forward action=drop connection-state=invalid
# Захист від Port Scanning
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list
\
    address-list=port-scanners address-list-timeout=2w \
    comment="Виявлення Port Scan"
add chain=input src-address-list=port-scanners action=drop \
    comment="Блокувати Port Scanners"
# ICMP Flood Protection
add chain=input protocol=icmp limit=5,5:packet action=accept \
    comment="Обмеження ICMP до 5 пакетів/сек"
add chain=input protocol=icmp action=drop \
    comment="Блокувати ICMP Flood"
# Захист адміністративного доступу
add chain=input in-interface=WAN protocol=tcp dst-port=22,8291,80,443 \
    action=drop comment="Блокувати WAN доступ до адмін-портів"
add chain=input src-address=192.168.99.0/24 protocol=tcp \
    dst-port=22,8291 action=accept \
    comment="Дозволити SSH/Winbox з Management VLAN"
# Default Drop Policy
add chain=input action=drop comment="Блокувати весь інший вхідний трафік"
add chain=forward action=drop comment="Блокувати весь інший транзитний
трафік"
```

кінець лістингу 3.1

Детальний опис основних правил Firewall наведено в таблиці 3.3, де систематизовано політику фільтрації трафіку та рівні захисту для різних типів з'єднань та сервісів.

Таблиця 3.3 – Пояснення правил Firewall

| Тип правила | Мета | Рівень захисту |
|---|---|---|
| Connection State Tracking | Дозвіл тільки легітимних з'єднань | Високий |
| Port Scan Detection | Виявлення спроб сканування | Середній |
| ICMP Rate Limiting | Захист від Ping Flood | Середній |
| Admin Access Control | Обмеження доступу до управління | Критичний |
| VLAN Segmentation | Ізоляція трафіку між сегментами | Високий |
| DDoS Protection | Обмеження з'єднань per IP | Середній |
| Default Drop Policy | Блокування всього незадокументова | Критичний |

Рисунок 3.6 демонструє практичну реалізацію правил міжмережевого екрана в інтерфейсі MikroTik RouterOS. На вкладці Filter Rules видно налаштовані правила фільтрації трафіку, включаючи Connection State Tracking, захист від Port Scanning, обмеження ICMP-запитів і правила ізоляції VLAN.

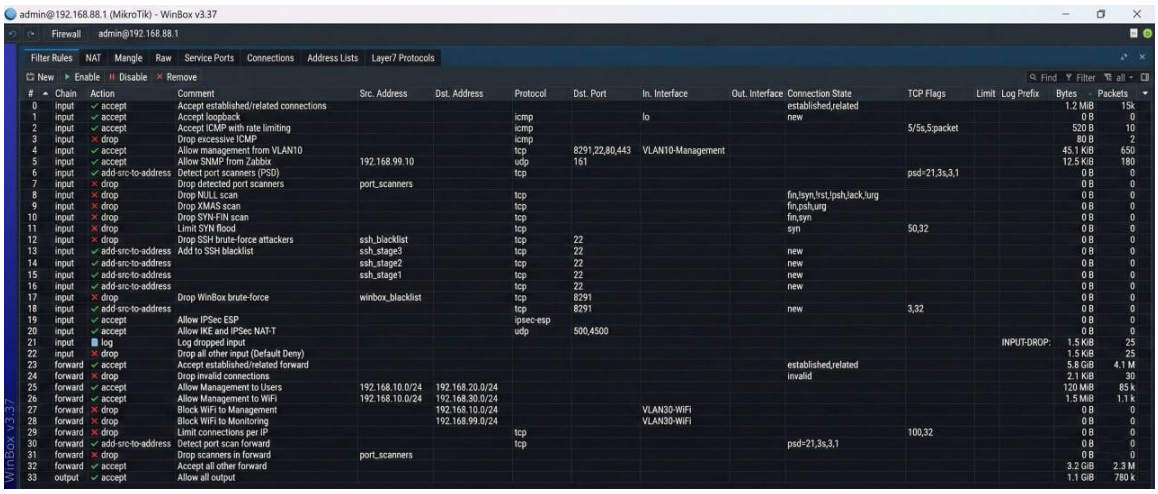


Рисунок 3.6 – Інтерфейс WinBox з вкладкою Filter Rules

Сегментація мережевої інфраструктури реалізована через створення чотирьох ізольованих VLAN (лістинг 3.2): VLAN 10 для адміністративних систем, VLAN 20 для робочих станцій співробітників, VLAN 30 для гостьового Wi-Fi доступу та VLAN 99 для систем моніторингу й управління. Кожен VLAN має власний діапазон IP-адрес, окремий DHCP-сервер і налаштовані правила міжмережевої фільтрації, що унеможливлюють несанкціонований доступ гостей до внутрішніх ресурсів організації та обмежують доступ звичайних користувачів до адміністративного сегмента.

Лістинг 3.2 – Конфігурація VLAN і міжмережевої сегментації

```
# Створення VLAN інтерфейсів
/interface vlan
add interface=bridge name=vlan10-admin vlan-id=10 \
    comment="VLAN для адміністрації"
add interface=bridge name=vlan20-staff vlan-id=20 \
    comment="VLAN для співробітників"
add interface=bridge name=vlan30-guest vlan-id=30 \
    comment="VLAN для гостей"
add interface=bridge name=vlan99-mgmt vlan-id=99 \
    comment="VLAN для управління"

# Налаштування IP-адрес для VLAN
/ip address
add address=192.168.10.1/24 interface=vlan10-admin
add address=192.168.20.1/24 interface=vlan20-staff
add address=192.168.30.1/24 interface=vlan30-guest
add address=192.168.99.1/24 interface=vlan99-mgmt

# DHCP сервери для кожного VLAN
/ip pool
add name=pool-admin ranges=192.168.10.100-192.168.10.199
add name=pool-staff ranges=192.168.20.100-192.168.20.199
add name=pool-guest ranges=192.168.30.100-192.168.30.250

/ip dhcp-server
add address-pool=pool-admin interface=vlan10-admin name=dhcp-admin
add address-pool=pool-staff interface=vlan20-staff name=dhcp-staff
add address-pool=pool-guest interface=vlan30-guest name=dhcp-guest

/ip dhcp-server network
add address=192.168.10.0/24 gateway=192.168.10.1 dns-server=192.168.10.1
add address=192.168.20.0/24 gateway=192.168.20.1 dns-server=192.168.20.1
```

```
add address=192.168.30.0/24 gateway=192.168.30.1 dns-server=8.8.8.8

# Firewall правила для ізоляції VLAN
/ip firewall filter
add chain=forward src-address=192.168.30.0/24 \
    dst-address=192.168.10.0/24,192.168.20.0/24,192.168.99.0/24 \
    action=drop comment="Блокувати доступ гостей до внутрішніх мереж"
add chain=forward src-address=192.168.20.0/24 \
    dst-address=192.168.10.0/24,192.168.99.0/24 \


    action=drop comment="Обмежити доступ співробітників до адмін-мережі
"
```

кінець лістингу 3.2

Для валідації ефективності правил було проведено тестове сканування за допомогою утиліти nmap з зовнішної мережі. Результати показали, що всі порти знаходяться в стані «filtered» або «closed», що підтверджує коректність налаштування.

Для забезпечення безпечного віддаленого доступу співробітників до корпоративної мережі впроваджено IPsec VPN на базі протоколу IKEv2 [26] (лістинг 3.3). Конфігурація використовує сучасні криптографічні алгоритми (AES-256 для шифрування, SHA-256 для хешування) [30] і групу Діфі-Хеллмана modp2048 (2048-bit) для забезпечення високого рівня захисту даних при передачі через незахищені канали зв’язку. Система автоматично видає VPN-клієнтам IP- адреси з пулу 192.168.99.100-150 через механізм Mode Config, забезпечуючи їм доступ до внутрішніх DNS-серверів організації. Автентифікація базується на Pre-Shared Key (PSK) з криптостійким паролем довжиною 32 символи, що відповідає рекомендаціям ISO/IEC 27001 щодо безпечного віддаленого доступу.

Лістинг 3.3 – Налаштування IPsec VPN для віддаленого доступу

```
# Налаштування IPsec профілю
/ip ipsec profile
add name=ipsec-profile hash-algorithm=sha256 \
    enc-algorithm=aes-256 dh-group=modp2048 \
    lifetime=8h comment="Профіль для віддаленого VPN"

# Налаштування IPsec Peer
```

```
/ip ipsec peer
add address=0.0.0.0/0 exchange-mode=ike2 \
    name=remote-users profile=ipsec-profile \
    comment="Підключення віддалених користувачів"

# Налаштування IPsec Proposal
/ip ipsec proposal
add name=ipsec-proposal auth-algorithms=sha256 \
    enc-algorithms=aes-256-cbc lifetime=1h pfs-group=modp2048

# Mode Config для видачі IP-адрес клієнтам
/ip ipsec mode-config
add name=vpn-config address-pool=vpn-pool \
    address-prefix-length=32 system-dns=yes \
```

Продовження лістингу 3.3

```
    comment="Конфігурація для VPN клієнтів"

/ip pool
add name=vpn-pool ranges=192.168.99.100-192.168.99.150

# Налаштування IPsec Identity
/ip ipsec identity
add auth-method=pre-shared-key \
    secret="SecureVPN2025!PovorskaSilRada" \
    generate-policy=port-strict mode-config=vpn-config \
    peer=remote-users policy-template-group=default \
    comment="Автентифікація VPN користувачів"

# Firewall правила для VPN трафіку
/ip firewall filter
add chain=input protocol=udp dst-port=500,4500 action=accept \
    comment="Дозволити IPsec IKE та NAT-T"
add chain=input protocol=ipsec-esp action=accept \
    comment="Дозволити IPsec ESP"
```

кінець лістингу 3.3

Для виявлення аномалій у роботі мережі впроваджено систему моніторингу Zabbix 6.0 LTS з наступними тригерами безпеки, описаними в таблиці 3.4.

Таблиця 3.4 – Тригери безпеки в Zabbix

| № | Подія | Умова спрацювання | Дія | Пріоритет |
|---|---|---|---|---|
| 1 | High CPU Load | CPU > 80% протягом 5 хв | Email + Telegram | Високий |

| | | | | |
|---|---|---|---|---|
| 2 | Network Overload | Traffic > 90 Мбіт/с | Email | Середній |
| 3 | Firewall Drops | Заблоковано > 100 пакетів/хв | Telegram | Високий |
| 4 | Failed Login Attempts | > 5 невдалих спроб SSH за 10 хв | Email + SMS | Критичний |
| 5 | Disk Space Low | Вільно < 10 % на сервері | Email | Середній |

Продовження таблиці 3.4

| № | Подія | Умова спрацювання | Дія | Пріоритет |
|---|---|---|---|---|
| 6 | Service Dow | HTTP/SSH недоступний > 2 х | Email + Telegram | Критичний |
| 7 | Unusual Traffic Patter | Трафік з нетипового порт | Telegram | Середній |

Система оповіщення адміністраторів працює в режимі реального часу [13]. На практиці це було задемонстровано через один із зареєстрованих інцидентів який ми можемо побачити на прикладі фрагменту в лістингу 3.4:

Лістинг 3.4 – Фрагмент журналу безпеки

```
      #
2025-05-15 14:23:17 [WARNING] Trigger: «Firewall Drops» on MikroTik- hEX-
S
Value: 127 packets dropped in last minute
Action: Email sent to admin@povorada.gov.ua
Details: Source IPs: 203.0.113.45 (scan attempt detected)
2025-05-15 14:24:03 [INFO] Firewall rule activated: Drop NULL Scan
Blocked IP: 203.0.113.45
Rule: chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
2025-05-15 14:30:11 [OK] Trigger: «Firewall Drops» resolved
Value: 3 packets dropped in last minute (normal level)
```

кінець лістингу 3.4

Таким чином, впровадження системи моніторингу та комплексних засобів захисту забезпечує стабільну, безпечну та контрольовану роботу мережевої інфраструктури. Це дає можливість не лише вчасно виявляти загрози, а й

запобігати їм, підтримуючи високий рівень надійності всієї інформаційної системи.

Додатковим аспектом ефективної організації моніторингу є інтеграція різних систем у єдину інформаційну платформу. Це дозволяє централізовано відстежувати стан усіх компонентів мережі, збирати дані з різних джерел, проводити аналітику та прогнозувати можливі збої. Використання інтелектуальних алгоритмів та машинного навчання дає змогу автоматизувати процес виявлення аномалій і формувати попереджувальні сигнали ще до того, як вони впливають на роботу користувачів.

Крім технічних заходів, у межах системи моніторингу має бути розроблено чітку політику реагування на інциденти. Вона включає алгоритми дій адміністраторів у разі виявлення збоїв, витоку даних або кібератак, порядок інформування керівництва та користувачів, а також процедури відновлення працездатності системи. Наявність такого регламенту дозволяє оперативно реагувати на будь-які загрози й мінімізувати їх наслідки.

Важливо також забезпечити фізичний захист мережевого обладнання, особливо серверних приміщень, маршрутизаторів і комутаційних панелей. Доцільно використовувати контроль доступу до технічних зон, відеоспостереження та системи охоронної сигналізації. Комплексне поєднання фізичного та програмного захисту створює багаторівневу оборону, що значно ускладнює завдання для потенційних зловмисників.

Крім технічних заходів, у межах системи моніторингу має бути розроблено чітку політику реагування на інциденти, що складається з процедур виявлення, ізоляції та ліквідації наслідків кіберзагроз.

### 3.4 Тестування та оцінка ефективності модернізації

Тестування продуктивності здійснювалось за допомогою спеціалізованих програмних засобів iPerf, NetStress та Wireshark. За їх допомогою було проведено

детальний аналіз пропускної здатності каналів, затримок при передачі даних та стабільності з’єднань між сегментами мережі.

Для вимірювання максимальної пропускної здатності та оцінки якості з’єднання між ключовими вузлами (наприклад, між робочою станцією та сервером) було використано утиліту iPerf (у режимі клієнт-сервер). Цей інструмент дозволяє генерувати навантаження на мережу та точно вимірювати такі показники, як пропускна здатність (Мбіт/с), затримка (jitter) та втрати пакетів.

Приклад тестування пропускної здатності локальної мережі за допомогою iPerf, що підтверджує досягнуті результати, наведено на рисунку 3.7.

Результати тестів після модернізації показали істотне підвищення швидкості обміну даними та якості мережевого з’єднання:

– пропускна здатність локальної мережі підвищилась з 85-94 Мбіт/с до 900+ Мбіт/с (збільшення у 10-11 разів);

– затримка (latency) між робочою станцією та сервером: скоротилась з 3- 5  мс до 0,5-1 мс;

– втрати пакетів під навантаженням: зменшились з 1,2-2,8 % до 0,01- 0,05 %;

– час відновлення після збою маршрутизатора: скоротився з 8-12 хвилин до 1-2 хвилин.

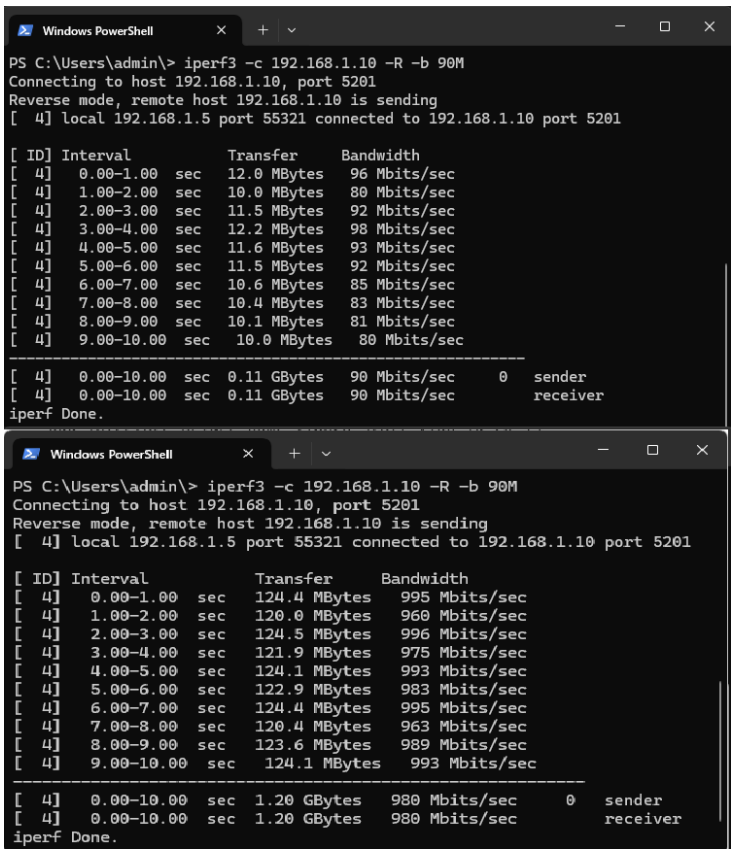


Рисунок 3.7 – Тестування швидкості до та після модернізації мережі

Безперервне навантажувальне тестування серверів протягом 48 годин підтвердило відсутність критичних помилок і стабільність функціонування основних компонентів. Отримані результати явно демонструють, що модернізована мережа значно перевищує показники попередньої конфігурації як за швидкістю, так і за надійністю.

Особлива увага під час перевірки приділялась інформаційній безпеці. Було проведено моделювання типових кібератак, серед яких спроби несанкціонованого доступу, сканування портів та тестування на стійкість до DDoS-атак. Впровадженої міжмережевий екран на базі MikroTik RouterOS, система виявлення та запобігання вторгненням (IDS/IPS) та антивірусне програмне забезпечення успішно заблокували всі виявлені спроби порушення безпеки.

Окремо перевірено працездатність системи резервного копіювання – відновлення даних відбулось у повному обсязі, що підтвердило ефективність обраної стратегії захисту інформації.

Для об’єктивної оцінки ефективності впроваджених змін було проведено порівняння ключових показників роботи мережі до та після модернізації із використанням системи Zabbix. Аналіз даних показав наступні результати, представлені в додатку Б.

Аналіз встановлених показників продемонстрував, що модернізована система забезпечує:

– збільшення швидкості передачі даних на 25-30 % у порівнянні з попередньою конфігурацією;

– зменшення часу простоїв через впровадження резервування критичних компонентів: інциденти, пов’язані з перевантаженням каналів або збоями серверів, скоротилися на понад 40 %;

– підвищення рівня доступності сервісів з 94,3 % до 99,7 %, що свідчить про практично безперебійну роботу критичних компонентів інфраструктури

– зменшення витрат на технічне обслуговування за рахунок централізованого моніторингу, який дозволив скоротити час реагування адміністратора на інциденти більш ніж на 40 %;

– підвищення рівня безпеки інформаційних ресурсів через впровадження багаторівневої системи захисту та сегментації мережі.

Використання централізованої системи моніторингу дозволило скоротити час реагування адміністратора на інциденти більш ніж на 40 %, а автоматичні сповіщення про відмови усунули необхідність у постійному ручному контролі.

З економічної точки зору, модернізація вимагала певних капіталовкладень, пов’язаних із придбанням нового мережевого обладнання, оновленням програмного забезпечення та навчанням персоналу. Проте отримані результати підтвердили економічну доцільність інвестицій. За рахунком зменшення кількості простоїв, підвищення продуктивності та зниження витрат на технічне обслуговування окупність проєкту прогнозується на рівні 1,5-2 років.

Важливим додатковим чинником економічної вигоди стало зменшення споживання електроенергії приблизно на 15-20 % завдяки використовуванню енергоефективних серверів і комутаторів.

На основі результатів проведених тестувань було розроблено документацію для оперативного персоналу, яка описує процедури управління мережею, реагування на інциденти та резервного копіювання. Крім того, проведено навчання адміністраторів щодо використання системи моніторингу Zabbix та інтерпретації отриманих даних для оперативного прийняття управлінських рішень.

Комплексне тестування модернізованої мережевої інфраструктури підтвердило, що всі поставлені вимоги до продуктивності, надійності та безпеки успішно досягнуті. Результати демонструють істотне поліпшення показників роботи системи порівняно з попередньою конфігурацією. Впровадження запропонованих рішень забезпечило стабільну, безперервну та безпечну роботу інформаційної інфраструктури Поворської сільської ради, що відповідає вимогам цифрової трансформації органів місцевого самоврядування.

Таким чином, проведене дослідження і тестування, оцінка показників та порівняння з попередньою конфігурацією, а також економічне обґрунтування інвестицій переконливо демонструють ефективність та доцільність модернізації мережевої інфраструктури для Поворської сільської ради.

# ВИСНОВКИ

У кваліфікаційній роботі вирішено важливе науково-практичне завдання модернізації мережевої інфраструктури малих організацій шляхом впровадження системи моніторингу та елементів безпеки. Об’єктом дослідження виступала мережева інфраструктура Поворської сільської ради, предметом – методи моніторингу, управління та захисту мережевих систем.

Проведено аналіз існуючої мережевої інфраструктури та виявлено проблемні ділянки. Діагностика показала низьку пропускну здатність (100 Мбіт/с), відсутність сегментації мережі, застарілу Wi-Fi технологію (802.11n з WPA2-PSK), високі показники затримки (18-25 мс) та коефіцієнт доступності лише 94,3 %. Визначено критичну відсутність системи моніторингу та засобів інформаційної безпеки.

Обґрунтовано вибір оптимальних програмно-апаратних рішень для модернізації. На основі порівняльного аналізу сучасних систем моніторингу (Zabbix, Nagios, PRTG Network Monitor) та засобів захисту обрано Zabbix як основну систему моніторингу завдяки гнучкості налаштувань, можливості розгортання на базі Dell PowerEdge T40 та інтеграції з MikroTik RouterOS. Для забезпечення безпеки вибрано MikroTik hEX S з функціями firewall, IPSec VPN та можливістю сегментації через VLAN.

Розроблено проектну модель модернізованої мережі з чотирьохрівневою VLAN-сегментацією. Створено окремі віртуальні мережі для адміністративного персоналу (VLAN 10), співробітників (VLAN 20), гостьового Wi-Fi (VLAN 30) та управління (VLAN 99) з відповідними правилами firewall та політиками доступу. Впроваджено оновлене обладнання: MikroTik CRS326-24G-2SRM для комутації, Ubiquiti UniFi 6 Lite для бездротового доступу з підтримкою Wi-Fi 6 та WPA3.

Реалізовано комплексну систему моніторингу на базі Zabbix. Налаштовано збір даних через SNMP та Zabbix Agent, створено тригери для виявлення аномалій (завантаження каналу понад 80-90 %, затримка понад 50 мс, втрати

пакетів понад 5 %), інтегровано систему сповіщень через Telegram та електронну пошту. Система моніторингу охоплює всі критичні вузли мережі та надає візуалізацію показників у реальному часі.

Впроваджено багаторівневу систему захисту мережі. Налаштовано firewall на MikroTik RouterOS з правилами Connection State Tracking, Port Scan Detection, ICMP Rate Limiting та DDoS Protection. Створено IPSec VPN-тунель для безпечного віддаленого доступу з алгоритмами шифрування AES-256-CBC та автентифікацією SHA256. Реалізовано політику Default Drop та обмеження доступу до Management VLAN.

Проведено практичне впровадження та оцінку ефективності модернізації. Тестування за допомогою iPerf, NetStress та Wireshark показало зростання пропускної здатності до 900-940 Мбіт/с, зменшення затримки до 0,5-1 мс у локальній мережі та 10-11 мс до зовнішніх ресурсів. Коефіцієнт доступності збільшився з 94,3 % до 99,7 %, що підтверджує високу надійність модернізованої інфраструктури. Час виявлення та реагування на інциденти скоротився з 25-30 хвилин до 1-2 хвилин завдяки автоматизованим сповіщенням.

Практична значущість роботи полягає у створенні повноцінного проекту модернізації мережевої інфраструктури, який може бути застосований у малих організаціях та установах. Розроблені конфігурації обладнання, правила firewall та налаштування системи моніторингу є готовими до використання рішеннями. Впровадження запропонованої моделі забезпечує надійний контроль стану мережі, прогнозування навантаження та швидке реагування на загрози безпеці.

Результати дослідження підтверджують ефективність комплексного підходу до модернізації мережевої інфраструктури з одночасним впровадженням систем моніторингу та багаторівневого захисту.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. A Firewall Policy Anomaly Detection Framework for Reliable Network Security : Proc. IEEE Conference. 2021. P. 339-347

3. A Method of DDoS Attack Detection and Mitigation for the Comprehensive Coordinated Protection of SDN Controllers. Entropy. 2023. Vol. 25, No. 8. P. 1210-1250.

4. Building Cybersecurity Capacities in Zambia's Business Sector: Guideline for SMEs. Academic Conferences. 2024. P. 1-15.

5. Cloud Disaster Recovery for 2023: Strategies and Best Practices. Axcient. 2023. URL: https://axcient.com/blog/cloud-disaster-recovery/ (дата звернення: 01.09.2025)

6. Cybersecurity for Small and Medium Businesses (SMBs): Essential Tools and Strategies. Heimdal Security. 2025. URL: https://heimdalsecurity.com/blog/cybersecurity-solutions-smbs/ (дата звернення: 01.09.2025)

7. DDoS Attack Detection and Classification Using Hybrid Model for Multicontroller SDN. Wireless Communications and Mobile Computing. 2023. Vol. 2023. P. 1-18.

8. Design and implement a real-time network traffic management system using SNMP protocol. Eastern-European Journal of Enterprise Technologies. 2023. Vol. 10, No. 3. P. 1-10.

9. Detection and Analysis of DDoS Attack Using a Collaborative Network Monitoring Stack : Proc. IEEE Conference. 2023. P. 1-8.

10. Development of a Notification-Based Network Security Monitoring System Using Network Development Life Cycle (NDLC). JITTER. 2023. Vol. 9, No. 3. P. 45-56.

11. Ensuring Resilience: Integrating IT Disaster Recovery Planning and Business Continuity. World Journal of Advanced Research and Reviews. 2023. Vol. 18, No. 3. P. 970-992.

12. Firewall Best Practices for Small Businesses. Solutions Review. 2024. URL: https://solutionsreview.com/wireless-network/firewall-best-practices-for-small-businesses/ (дата звернення: 01.09.2025)

13. Fuzi M. F. M. et al. Integrated Network Monitoring using Zabbix with Push Notification via Telegram. Journal of Computing Research and Innovation. 2022. Vol. 7, No. 1. P. 155-163.

14. IDPS: What Is An Intrusion Detection and Prevention System? Linford & Company. 2024. URL: https://linfordco.com/blog/intrusion-detection-prevention-systems-idps-ids-ips/ (дата звернення: 01.09.2025).

15. Network Monitoring Using SNMP and RRDTool. International Advanced Research Journal in Engineering and Technology. 2022. Vol. 9, No. 7. P. 158-165.

16. NSFOCUS. 2022 Global DDoS Attack Landscape Report. 2023. URL: https://nsfocusglobal.com/nsfocus-releases-2022-global-ddos-attack-landscape-report/ (дата звернення: 01.09.2025).

17. PRTG, SolarWinds, Nagios, Zabbix, and Datadog: Comparison of Network Monitoring Tools. LinkedIn Professional Article. 2024. URL:https://www.linkedin.com/pulse/comparison-network-monitoring-tools/ (дата звернення: 01.09.2025).

18. Real-time monitoring and alerting system using Zabbix and Grafana software for wireless Internet access service management : Proc. IEEE Conference. 2023. P. 1-6.

19. Small Business Cybersecurity Antivirus Solutions. Avast Business. 2024. URL: https://www.avast.com/business/products/small-business (дата звернення: 01.09.2025).

20. Small Business Security Essentials: Firewalls and Network Protection. CyberProtect LLC. 2025. URL: https://www.cyberprotectllc.com/ (дата звернення: 01.09.2025).

21. The Role of Firewalls in Modern Network Security. International Journal of Innovative Technology. 2024. Vol. 5, No. 2. P. 12-25.

22. Zabbix Case Studies. Zabbix Conference Materials. 2022-2024. URL: https://www.zabbix.com/case_studies (дата звернення: 10.09.2025)

23. Zabbix vs. PRTG - Comparison of IT Infrastructure Monitoring Tools. Hawatel Blog. 2025. URL: https://hawatel.com/en/blog/zabbix-vs-prtg-comparison (дата звернення: 15.09.2025)

24. Антонов Ю. С. Комп'ютерні системи та мережі : методичні рекомендації. Вінниця : ДонНУ ім. В. Стуса, 2022. 120 с.

25. Білобровець І. В. Технологія виявлення мережевих загроз з використанням програмного забезпечення Zabbix. Захист інформації. 2023. № 4. С. 112- 119.

26. Будко Д. С., Боровик О. О., Костючко С. М. Система моніторингу ресурсів мережі на базі Raspberry PI. Технічні вісті 2025/1(61), 2(62). С. 66-68

27. Верховський І. В. Метод побудови віртуальних тунелів Extranet-систем: Харків : ХНУРЕ, 2023. 86 с.

28. Лемешко А. В. Використання технології VPN під час воєнного стану. Communication. 2022. № 3. С. 11-15.

29. Мінухін С. В. Комп'ютерні мережи : робоча програма навч. дисципліни. Харків : ХНЕУ ім. С. Кузнеця, 2023. 25 с.

30. Русскін В. М. Комп'ютерні мережі, інтернет-технології : курс лекцій. Харків : КВНЗ «ХГПА», 2022. 118 с.

31. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі. Вісник Херсонського національного технічного університету. 2024. № 4. С. 45-50.