МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ІНСТИТУТ

Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПРОКСІ-СЕРВЕРА ДЛЯ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ В ЛОКАЛЬНІЙ МЕРЕЖІ»

(за матеріалами Товариства з обмеженою відповідальністю «Лампа Софтвер», м. Вінниця)

Здобувача вищої освіти
освітнього ступеня «магістр»
2 курсу, групи ІСТ-21д(м),
спеціальності 126 «Інформаційні
системи та технології»
освітньої програми «Інформаційні
технології у бізнесі»
денної форми навчання Олександра САЛЬНИКОВА

Науковий керівник
кандидат економічних наук,
доцент Світлана МЕРІНОВА

Гарант
освітньої програми
доктор технічних наук, професор Вадим РОМАНЮК

Вінниця 2024

ЗМІСТ

ВСТУП

Зростання обсягів мережевого трафіку в локальних мережах підприємств створює необхідність у впровадженні ефективних методів управління і контролю доступу до мережевих ресурсів. Для вирішення цієї проблеми важливу роль відіграють проксі-сервери. Вони сприяють оптимізації використання мережевих ресурсів, підвищенню безпеки та контролю за мережею, що робить їх важливим компонентом сучасної IT-інфраструктури.

Потреба у використанні проксі-серверів стає особливо актуальною через збільшення вимог до безпеки даних і необхідність зменшення навантаження на мережеві ресурси. Серед основних проблем, з якими стикаються підприємства без використання проксі-серверів, є низька ефективність використання мережевих ресурсів, підвищене навантаження на сервери через необмежений доступ до зовнішніх мереж, відсутність централізованого контролю за мережею, а також збільшений ризик несанкціонованого доступу. Крім цього, недостатнє використання технологій кешування призводить до уповільнення доступу до важливих ресурсів.

Проксі-сервери дозволяють не лише контролювати доступ користувачів до зовнішніх ресурсів, але й забезпечують збереження копій популярних сторінок, що значно зменшує навантаження на основні канали передачі даних і прискорює доступ до часто запитуваних ресурсів. Це особливо важливо в умовах зростаючих вимог до ефективності та безпеки мережевих рішень.

Наукові дослідження вказують на зростаючу важливість проксі-серверів у забезпеченні контролю і захисту мережевого трафіку. Зокрема, дослідження Гончарука А.М. та Кушніра М.О. свідчать про те, що використання проксі-серверів може зменшити навантаження на основні канали передачі даних, що є особливо важливим в умовах інтенсивного використання інтернет-ресурсів. Дослідження Мельника С.В. підкреслюють

важливість інтеграції проксі-серверів із технологіями шифрування даних для забезпечення безпеки мобільного трафіку. Це є необхідним кроком у зв'язку зі зростанням кількості підключень і швидкою еволюцією мобільних технологій.

Мета дослідження - розробка та впровадження інформаційної технології проксі-сервера для оптимізації трафіку в локальній мережі з метою підвищення ефективності використання мережевих ресурсів, забезпечення безпеки та централізованого управління доступом до зовнішніх мереж.

Завдання кваліфікованої роботи:

1. Проаналізувати існуючі рішення проксі-серверів для управління трафіком у локальних мережах.

2. Оглянути методи моніторингу мережевого трафіку та інформаційні технології, які їх забезпечують

3. Проаналізувати роботу товариства з обмеженою відповідальністю «Лампа Софтвер».

4. Оцінити проксі-сервер для моніторингу локальної мережі ТОВ «Лампа Софтвер».

5. Оптимізувати процес моніторингу трафіку та інтегрувати проксі-сервера з системами забезпечення безпеки.

6. Розрахувати ефективність модернізації інформаційної технології проксі-сервера для моніторингу мережевого трафіку в локальній мережі.

Об'єкт дослідження - локальна мережа підприємства з великою кількістю користувачів та мережевих ресурсів.

Предмет дослідження - інформаційна технологія проксі-сервера для управління та оптимізації трафіку в локальній мережі.

Практична значимість - впровадження розробленого проксі-сервера дозволить значно знизити навантаження на мережеві ресурси, підвищити швидкість доступу до ресурсів, зменшити ризики несанкціонованого доступу та підвищити ефективність роботи локальної мережі. Це також забезпечить контроль за трафіком і дозволить централізовано управляти доступом до зовнішніх ресурсів.

Наукова новизна роботи полягає у розробці нових алгоритмів оптимізації мережевого трафіку за допомогою проксі-сервера, що забезпечують підвищення ефективності роботи локальної мережі та безпеки інформації. Запропоноване рішення включає методи інтелектуального кешування та динамічного контролю доступу.

Методи дослідження. Для досягнення мети використовувалися методи системного аналізу, моделювання інформаційних процесів, експериментальне впровадження прототипу проксі-сервера та аналіз отриманих результатів. Також застосовувалися методи математичного моделювання для оцінки ефективності оптимізації трафіку.

Інформаційною базою дослідження стали сучасні наукові праці, що стосуються технологій проксі-серверів, мережевої безпеки, а також технічна документація з впровадження та використання проксі-серверів у локальних мережах. Крім того, використовувалися дані про мережевий трафік локальної мережі підприємства, на якому проводилося дослідження.

Апробація результатів дослідження проводилась на базі локальної мережі ТОВ «Лампа Софтвер», де було впроваджено інформаційну технологію проксі-сервера для моніторингу мережевого трафіку. Результати дослідження обговорювались на конференціях.

В результаті дослідження було опубліковано дві статті:

Сальників О. Проксі-сервери як інструмент забезпечення безпеки та контролю за мережевим трафіком. *Вісник студентського наукового товариства «ВАТРА».* Вінниця: Редакційно-видавничий відділ ВТЕІ ДТЕУ, 2024. Вип.188. С.393-402.

Сальників О. Проектування архітектури проксі-сервера для мобільного трафіку в локальній мережі. У збірнику XI Всеукраїнської науково-практичної Інтернет-конференції «МЕНЕДЖМЕНТ XXI СТОЛІТТЯ: СУЧАСНІ МОДЕЛІ, СТРАТЕГІЇ, ТЕХНОЛОГІЇ» Вінниця: Редакційно-видавничий відділ ВТЕІ ДТЕУ, 2024.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПРОКСІ-СЕРВЕРА

1.1. Основні принципи роботи проксі-серверів та їх застосування у локальних мережах

Проксі-сервер (proxy server) — це сервер-посередник, який виступає проміжною ланкою між клієнтом (користувачем) і цільовим сервером. Він отримує запити від клієнтів, передає їх до відповідних серверів, отримує відповіді і повертає їх назад клієнтам. Проксі-сервери застосовуються для оптимізації трафіку, підвищення безпеки і забезпечення анонімності в мережі.

Основні функції проксі-серверів полягають у наступному [8]:

1. Проксі-сервер приймає запит від клієнта і передає його на цільовий сервер, а після отримання відповіді повертає її назад клієнту. Це дозволяє адмініструвати і контролювати трафік, який проходить через сервер.

2. Проксі-сервер зберігає часто запитувані ресурси, такі як веб-сторінки, в кеші. Це дозволяє суттєво скоротити час завантаження ресурсів для користувачів і зменшити навантаження на зовнішні канали зв'язку.

3. Проксі-сервер може здійснювати фільтрацію трафіку, блокуючи доступ до певних ресурсів чи сайтів. Це забезпечує захист користувачів від небажаного контенту, реклами або шкідливих сайтів.

4. Проксі-сервер може контролювати доступ, вимагаючи від користувачів авторизації перед тим, як вони отримають доступ до мережі. Це додає рівень безпеки та забезпечує контроль доступу до ресурсів.

5. Проксі-сервер має можливість приховувати справжню IP-адресу клієнта, що забезпечує анонімність і конфіденційність при роботі в мережі, допомагаючи зберегти приватність і уникнути відстеження.

6. Проксі-сервер дозволяє адміністраторам моніторити мережевий трафік, аналізувати його і виявляти аномальні дії. Це сприяє швидшому виявленню потенційних загроз безпеці та оптимізації роботи мережі [28].

Проксі-сервери є важливим інструментом для ефективного управління і захисту мережевих ресурсів, а також забезпечення більшої анонімності і оптимізації роботи мереж [21].

Таблиця 1.1 – Основні функції проксі-серверів

Функція	Опис
Перенаправлення запитів	Отримує запит від клієнта, передає його на цільовий сервер та надає відповідь клієнту назад.
Кешування даних	Зберігає частіше запитувані ресурси щодо скорочення навантаження на зовнішній канал зв'язку і поменшення часу завантаження.
Фільтрація трафіку	Блокує доступ щодо ресурсів чи сайтів, які небажані, захищає цим користувачів щодо небезпечного контенту.
Контроль доступу	Здійснює аутентифікацію користувачів та контролює доступ щодо мережевих ресурсів, надаючи додатковий рівень безпеки.
Анонімізація	Приховує дійсну IP-адресу клієнта, надаючи конфіденційність та анонімність користувача щодо доступу до Інтернету.
Моніторинг та аналіз трафіку	Надає адміністраторам здійснювати моніторинг активності в мережі, виявляти підозрілі дії та оптимізувати користування мережевих ресурсів.

Проксі-сервери є важливою складовою мережевої інфраструктури, що забезпечує підвищення безпеки, покращення швидкості доступу до ресурсів, оптимізацію використання каналів зв'язку та анонімність користувачів [22].

Основною функцією проксі-серверів є їхня роль посередника між клієнтом і цільовим сервером. Коли клієнт відправляє запит, проксі-сервер приймає його, направляє до необхідного сервера, отримує відповідь і повертає її клієнту. Такий механізм надає можливість ефективно контролювати мережевий трафік і забезпечує додаткові функції, такі як кешування даних, контроль доступу, фільтрація вмісту та анонімізація [12].

Проксі-сервери можуть зберігати часто запитувані дані в кеші, що значно зменшує навантаження на зовнішні канали зв'язку, скорочує час завантаження та знижує витрати на передачу даних. Вони також можуть здійснювати контроль доступу, вимагаючи аутентифікації користувачів і визначення рівнів доступу, що створює додатковий рівень безпеки. Крім того, фільтрація вмісту дозволяє блокувати небажані або шкідливі ресурси, що захищає користувачів від небажаного контенту та зловмисних сайтів. Приховання реальної IP-адреси клієнта забезпечує анонімність та підвищує конфіденційність [11].

Використання проксі-серверів у локальних мережах дозволяє вирішувати завдання оптимізації трафіку, підвищення рівня безпеки, забезпечення анонімності, моніторингу та аналізу активності користувачів. У корпоративних мережах проксі-сервери широко застосовуються для кешування даних, що зменшує навантаження на мережу та забезпечує швидке завантаження інформації. Також вони сприяють підвищенню безпеки шляхом фільтрації трафіку та блокування небажаних ресурсів, знижуючи ризики витоку конфіденційної інформації чи атак [14].

Адміністратори можуть використовувати проксі-сервери для моніторингу мережевого трафіку, дослідження активності користувачів, виявлення підозрілої поведінки та покращення контролю над використанням мережевих ресурсів, що є важливим для безпеки та стабільності мережі. Проксі-сервери також допомагають впроваджувати політику використання Інтернету, контролюючи доступ до певних ресурсів і надаючи контрольований доступ для різних груп користувачів. Загалом проксі-сервери є невід'ємною частиною сучасних локальних мереж для підвищення продуктивності та забезпечення безпеки.

Інтеграція технологій штучного інтелекту в управління трафіком дозволяє знизити навантаження на мережу на 25% і скоротити час відновлення після атак на 40%. В Україні лише 10% підприємств використовують рішення на основі штучного інтелекту для управління трафіком, але цей показник

поступово зростає через збільшення кібератак і необхідність швидкого реагування на загрози.

Ці дані демонструють важливість використання сучасних методів захисту та управління трафіком у локальних мережах із застосуванням проксі-серверів, а також необхідність впровадження сучасних технологій для підвищення рівня кібербезпеки.

На рисунку 1.1 відображено динаміку та прогноз використання проксі-серверів та засобів безпеки в Україні.

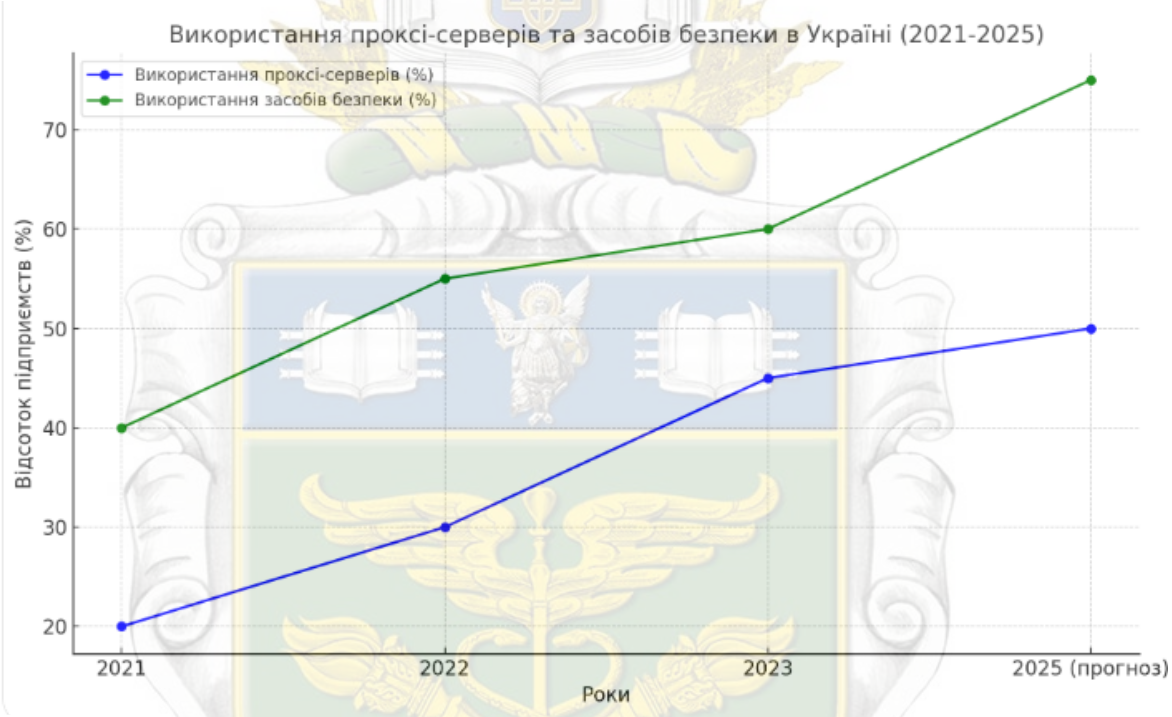

Рисунок 1.1 - Динаміка та прогноз використання проксі-серверів та засобів безпеки в Україні [5]

На рисунку показано використання проксі-серверів та засобів безпеки в Україні з 2021 по 2025 рік, включаючи прогноз. Відзначається зростання використання проксі-серверів для управління мобільним трафіком і підвищення застосування додаткових засобів безпеки в цих системах.

Використання проксі-серверів в Україні та за кордоном має свої особливості, пов'язані з регіональними умовами і викликами. У 2023 році приблизно 40% українських компаній активно застосовують проксі-сервери

для підвищення безпеки, оптимізації мережевого трафіку і забезпечення анонімності користувачів. У західних країнах цей показник досягає 70-80%, що свідчить про більш високий рівень впровадження сучасних технологій моніторингу і безпеки.

В умовах війни в Україні питання застосування проксі-серверів набуло особливої актуальності. Проксі-сервери дозволяють контролювати доступ до мережевих ресурсів і запобігати витоку конфіденційної інформації, що є критично важливим під час військових дій. Вони також допомагають організаціям захищатися від кіберзагроз і забезпечувати безпечний доступ до інформації в умовах постійних атак на інфраструктуру.

За кордоном проксі-сервери використовуються не лише для забезпечення безпеки, але й для підвищення ефективності бізнесу, оптимізації використання мережевих ресурсів і підтримки політики конфіденційності. Використання систем моніторингу, таких як Zabbix, у поєднанні з проксі-серверами є стандартом у багатьох великих компаніях для забезпечення безперервної роботи мережевої інфраструктури і зниження витрат.

Отже, застосування проксі-серверів в Україні під час війни стає важливим інструментом щодо убезпечення безпеки і стабільності роботи компаній, тоді як у західних країнах проксі-сервери є частиною комплексних систем моніторингу і управління мережею, що дозволяє збільшенню загальної ефективності бізнес-процесів.

1.2. Огляд методів моніторингу мережевого трафіку та інформаційні технології, які їх забезпечують

Моніторинг є важливим процесом, що забезпечує контроль за функціонуванням систем або інфраструктури, виявлення відхилень і оптимізацію використання ресурсів. Він дозволяє вчасно виявляти проблеми,

забезпечувати стабільну роботу систем і підвищувати ефективність управління [29].

Моніторинг мережевого трафіку є специфічним видом моніторингу, орієнтованим на контроль за передачею даних у мережі. Він дозволяє адмініструвати мережеву інфраструктуру, контролювати її стан, виявляти потенційні загрози, оцінювати ефективність використання мережевих ресурсів і швидко реагувати на проблеми [31].

У сучасних умовах моніторинг мережевого трафіку є важливим для бізнесу з таких причин [25]:

- Моніторинг допомагає швидко виявляти аномальні дії в мережі, пов'язані з несанкціонованим доступом або спробами атак, що підвищує рівень безпеки.

- Моніторинг дозволяє оцінювати завантаженість мережі, ефективно розподіляти ресурси і зменшувати перевантаження.

- Завдяки моніторингу мережевого трафіку забезпечується стабільна робота мережі, що безпосередньо впливає на якість послуг, які надаються клієнтам.

Моніторинг мережевого трафіку може здійснюватися різними методами з використанням відповідних технологій [40]:

- Пасивний моніторинг збирає дані про трафік без внесення змін до його потоку. Це дозволяє аналізувати активність у мережі, виявляти аномалії та оцінювати завантаженість. Для пасивного моніторингу застосовуються технології, такі як Wireshark, Zeek, NetFlow, sFlow.

- Активний моніторинг генерує тестові пакети для вимірювання продуктивності мережі та виявлення можливих проблем. Приклади інструментів для активного моніторингу включають Ping, Traceroute, iPerf.

- Моніторинг на базі мережевих протоколів використовує протоколи, такі як NetFlow або sFlow, для збору даних про сесії трафіку, дослідження моделей використання ресурсів і виявлення загроз. Прикладом систем є Cisco NetFlow і SolarWinds Network Traffic Analyzer.

- Моніторинг за допомогою систем виявлення вторгнень (IDS) дозволяє виявляти підозрілі дії в реальному часі, використовуючи шаблони відомих атак. Snort і Suricata є прикладами таких систем, що дозволяють виявляти загрози.

- Моніторинг на базі машинного навчання є сучасним методом, що дозволяє виявляти невідомі загрози шляхом аналізу аномальної поведінки трафіку. Cisco Stealthwatch і Darktrace використовують алгоритми машинного навчання для автоматичного виявлення загроз.

- Гібридний моніторинг поєднує активний і пасивний підходи для досягнення максимальної ефективності. Він реалізується за допомогою систем, таких як Zabbix і Nagios, що забезпечують комплексне вивчення і моніторинг мережі.

Таким чином, моніторинг мережевого трафіку, незалежно від методу, є важливим інструментом для забезпечення безпеки, стабільності роботи мережі і підвищення ефективності використання ресурсів [23].

В таблиці 1.2 відображено класифікацію методів моніторингу мережевого трафіку.

Таблиця 1.2 – Класифікація методів мережевого трафіку

Метод моніторингу	Особливості	Приклади інформаційних технологій
Пасивний моніторинг	Збирання даних не змінюючи поток трафіку.	Wireshark, Zeek, NetFlow, sFlow
Активний моніторинг	Генерація тестових пакетів щодо вимірювання продуктивності мережі.	Ping, Traceroute, iPerf
Моніторинг на основі протоколів	Застосування мережевих протоколів щодо збору і аналізу даних.	Cisco NetFlow, SolarWinds Network Traffic Analyzer
IDS моніторинг	Знаходження вторгнень у мережу на базі відомих патернів.	Snort, Suricata
Моніторинг на основі машинного навчання	Застосування алгоритмів машинного навчання щодо виявлення аномальної поведінки.	Cisco Stealthwatch, Darktrace
Гібридний моніторинг	З’єднання активного та пасивного підходів.	Zab

Моніторинг мережевого трафіку є ключовим елементом для забезпечення стабільної та безпечної роботи мережевої інфраструктури, а також для оптимізації використання ресурсів з метою підвищення ефективності бізнесу. Використання інформаційних технологій для моніторингу дозволяє швидше виявляти загрози і вчасно реагувати на них, що є особливо важливим для сучасного бізнесу, оскільки стабільність і безпека мережевої інфраструктури є критичними для успішного функціонування компаній [10].

Наведемо в таблиці 1.3 порівняння програм для моніторингу мережевого трафіку.

Моніторинг мережевого трафіку є ключовим елементом для забезпечення стабільної та безпечної роботи мережевої інфраструктури, а також оптимізації використання ресурсів для підвищення ефективності бізнесу. На основі даних щодо застосування систем моніторингу, можна спостерігати зростання інтересу до технологій контролю трафіку як в Україні, так і в усьому світі, особливо в умовах зростання кіберзагроз і обсягів передаваних даних.

Застосування інструментів для моніторингу мережевого трафіку значно підвищилось впродовж останніх років. Глобально, у період 2019-2020 років, використання інструментів моніторингу збільшилось на 25%, що стало наслідком зростання обсягу даних і підвищення рівня кіберзагроз. З 2020 до 2021 року, під час пандемії COVID-19, попит на інструменти моніторингу зріс на 30% через необхідність дистанційного контролю за мережами в умовах роботи з дому. У наступні роки, з 2021 по 2022, ринок збільшився ще на 35% через зростання кількості кібератак, що змусило компанії інвестувати в безпеку своїх мереж.

У 2022-2023 роках попит на інструменти на основі штучного інтелекту, такі як Darktrace, зріс на 40%, тому що ці інструменти автоматизують процеси виявлення і реагування на загрози. А у 2023-2024 роках ринок моніторингу

мережевого трафіку зріс на 45% через посилення атак на критичну інфраструктуру в Європі та інших регіонах.

Таблиця 1.3 – Порівняння програм для моніторингу мережевого трафіку

Назва програми	Опис	Ціна (USD)
Wireshark	Потужний інструмент для аналізу мережевого трафіку, що надасть можливість значно дослідити кожен пакет даних.	Безкоштовно
Zeek	Система аналізу мережевої безпеки, яка автоматично генерує звіти щодо активності у мережі та знаходить аномалії.	Безкоштовно
NetFlow	Інструмент щодо збору та дослідження даних про трафік на основі протоколу Cisco NetFlow. Використовується для дослідження продуктивності і оптимізації.	Залежить від провайдера
NetPeak Spider	Український інструмент щодо комплексного моніторингу мережевих ресурсів і дослідження їхньої продуктивності.	30-150 на місяць
Anturis	Українська система для моніторингу веб-додатків і інфраструктури, дає зручні візуалізації і інформативні звіти.	Від 10 на місяць
SolarWinds Network Performance Monitor	Комерційна система моніторингу мережевих ресурсів, яка надає контролювати продуктивність та ідентифікувати "вузькі місця" у мережі.	Від 2995 одноразово
Zabbix	Система моніторингу відкритого коду, яка убезпечує комплексний аналіз мережевих інфраструктур і серверів.	Безкоштовно
Nagios	Система моніторингу з відкритим кодом, що відслідковує продуктивність і знаходить проблеми в мережі.	Безкоштовно (основна версія), від 1995 (комерційна версія)

Продовження таблиці 1.3

Darktrace	Система моніторингу на базі машинного навчання, що знаходить аномальні активності і автоматично реагує на загрози.	Залежить від конфігурації та вимог

В Україні ситуація також має свої особливості. З початку війни у 2022 році попит на системи моніторингу мереж зріс на 60%, що було пов'язано із необхідністю забезпечення безпеки критичної інфраструктури та корпоративних мереж. Вітчизняні рішення, такі як NetPeak Spider та Anturis, стали більш популярними через необхідність зменшення залежності від іноземного програмного забезпечення в умовах війни.

Методи моніторингу мають свої тенденції розвитку. Пасивний моніторинг, що дозволяє збирати дані про мережевий трафік без втручання в його потік, став широко використовуваним через можливість детально аналізувати активність. Популярність таких інструментів, як Wireshark та Zeek, підвищилась на 50%. Активний моніторинг, зокрема Ping та Traceroute, зріс на 30%, оскільки дозволяє швидше перевіряти доступність важливих вузлів мережі [22].

Сучасні підходи, такі як моніторинг на базі машинного навчання, набувають поширення через можливість автоматичного виявлення аномалій і швидкого реагування на загрози. Попит на системи, такі як Cisco Stealthwatch та Darktrace, зріс на 45% з 2021 по 2023 роки, оскільки вони надають можливість глибокого аналізу мережі та автоматизують реагування на інциденти.

Загалом, моніторинг мережевого трафіку є важливим не тільки для забезпечення кібербезпеки, а й для оптимізації використання мережевих ресурсів, що є важливим для стабільної роботи бізнесу. Інструменти, такі як Zabbix, Wireshark та інші, дозволяють детально досліджувати трафік, виявляти проблеми та аномалії, а також оптимізувати використання ресурсів.

Під час постійної загрози кібератак і війни моніторинг мережевого трафіку став важливим інструментом щодо надання стабільності роботи мережі і зменшення ризиків. Він дозволяє оперативно знаходити потенційні загрози і вжити потрібних заходів щодо їх нейтралізації. Це дуже потрібно для критичної інфраструктури, де порушення роботи може вплинути на серйозні наслідки щодо бізнесу, так і для суспільства взагалі [31].

Таким чином, впродовж останніх п'яти років інтерес до інструментів моніторингу мережевого трафіку значно підвищився як у світі, так і в Україні. Це підвищення обумовлене збільшенням кіберзагроз, переходом на дистанційну роботу, потребою забезпечення стабільності мережевих процесів і зменшенням залежності від іноземних рішень. Моніторинг мережевого трафіку залишається критично важливим компонентом кібербезпеки, що дозволяє забезпечити ефективне управління мережевими ресурсами і безпеку в умовах сучасних викликів.

РОЗДІЛ 2
АНАЛІЗ РОБОТИ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЛАМПА СОФТВЕР»

2.1 Організаційно-економічна характеристика ТОВ «Лампа Софтвер»

ТОВ «Лампа Софтвер» є провідною компанією в сфері аутсорсингу інформаційних технологій, яка спеціалізується на створенні інноваційних IT-рішень, застосовуючи сучасні технології. Повна назва компанії - Товариство з обмеженою відповідальністю «Лампа Софтвер». Компанія була заснована для розробки, впровадження та підтримки технологічних рішень, а також надання різноманітних послуг в IT-сфері. Основна діяльність компанії включає розробку програмного забезпечення, інтеграцію бізнес-рішень, а також створення рішень для моніторингу мережевого трафіку.

Юридичну діяльність «Лампа Софтвер» регулює Статут, який встановлює правила ведення діяльності компанії, визначає правовий статус і стосунки між працівниками, партнерами та іншими сторонами. Компанія зареєстрована за адресою: 21050, Вінницька область, Вінницький район, місто Вінниця, вулиця Соборна, будинок 38, офіс 303. За цією адресою розташовані ще декілька суб'єктів господарювання, що свідчить про розвиток офісних центрів у цьому районі міста Вінниця.

Компанія була офіційно зареєстрована у Державному реєстрі юридичних осіб 18 лютого 2021 року і функціонує вже понад три роки. Її керівником з моменту заснування є Горобей Євген Анатолійович, який також виконує обов'язки бухгалтера станом на лютий 2024 року, що свідчить про централізоване управління фінансами та контроль витрат. Статутний капітал

компанії становить 100 мільйонів гривень, що демонструє її фінансову стабільність і можливість реалізації великих проєктів.

ТОВ «Лампа Софтвер» спеціалізується на послугах з розробки програмного забезпечення, автоматизації бізнес-процесів і створенні інноваційних рішень для клієнтів з різних сфер. Компанія займає активну позицію на ІТ-ринку, реалізовуючи комплексні ІТ-проєкти та застосовуючи сучасні інформаційні технології для моніторингу, безпеки та управління мережами.

ТОВ «Лампа Софтвер» також співпрацює з міжнародними партнерами з Америки, Ізраїлю, країн Європи та Сходу, активно розширюючи ринки для своїх ІТ-продуктів і послуг. Основні цілі компанії включають задоволення потреб клієнтів у високоякісних ІТ-рішеннях, збільшення прибутковості та підтримку соціально-економічних інтересів своїх працівників і партнерів.

Основними конкурентами ТОВ «Лампа Софтвер» на українському ринку є такі компанії, як EPAM Systems, Ciklum, Delphi, SkySoft.tech, Magisoft та Gemicle. Незважаючи на наявність конкуренції, "Лампа Софтвер" зуміла стати провідним постачальником ІТ-послуг завдяки своєму досвіду, високій якості послуг і постійному вдосконаленню своїх технологічних можливостей.

Компанія успішно розробляє індивідуальні рішення для бізнесу, медіа, сервісних та рекламних платформ, освіти, онлайн-комерції та інших галузей. Одним із ключових завдань ТОВ «Лампа Софтвер» є створення продуктів, що відповідають вимогам і очікуванням клієнтів, допомагаючи їм виходити на нові ринки та розширювати аудиторію. Слоган компанії, розміщений на її офіційному сайті, говорить: "Наша мета – стати партнерами наших клієнтів і разом зробити наш бізнес успішним".

Останніми проєктими, які розроблялися компанією Lampa Studio, є:

1. Мобільний додаток "Gastro family" – проект для мережі закладів Дмитра Борисова – одного з відомих українських рестораторів. Був задуманий єдиний мобільний додаток, щоб уніфікувати програми лояльності, що діють в

різних закладах мережі. Він мав на меті зібрати все в одному місці в зручному для користувача вигляді.

2. Додаток «1+1 Video» - новий проект, який компанія "1 + 1 Медіа" реалізувала спільно зі "Студією Lampa". Платформа 1 + 1 Video надає доступ до величезної бібліотеки медійного контенту компанії, а також до онлайнтрансляцій улюблених українських телеканалів.

3. Кешбек-сервіс «Letyshops». Команда «Студії Lampa» була залучена як експерти в сфері mobile ще на етапі проектування програми. В результаті було реалізовано швидкий, зручний і яскравий додаток Letyshops, який всього за перших 3 місяці роботи завантажили понад 150 000 користувачів.

Так як компанія є аутсорсинговою, то вона є постачальником IT-послуг, тобто компанія бере на себе частину завдань чи процесів на умовах субпідряду.

Можна відмітити, говорячи про постачальників компанії Lampa Studio, постачальників якісного софту, тобто комп'ютерних програм, різноманітних додатків та операційних систем щодо безперебійної та, головне, законної роботи компанії. Цими постачальниками є інші міжнародні IT-компанії, які розробляють ці програми. Постачання відбувається простим чином: Lampa Studio купує ліцензію на використання тої чи іншої програми, або ж річні підписки на софт.

До складу організаційної структури підприємства ТОВ «Лампа Софтвер» входять такі складові: планово-економічний відділ, бухгалтерія, економічний відділ, інженерний відділ, маркетингово-логістичний відділ, інформаційний відділ. На ТОВ «Лампа Софтвер» є лінійно-функціональний тип організаційної структури (рис. 2.1).

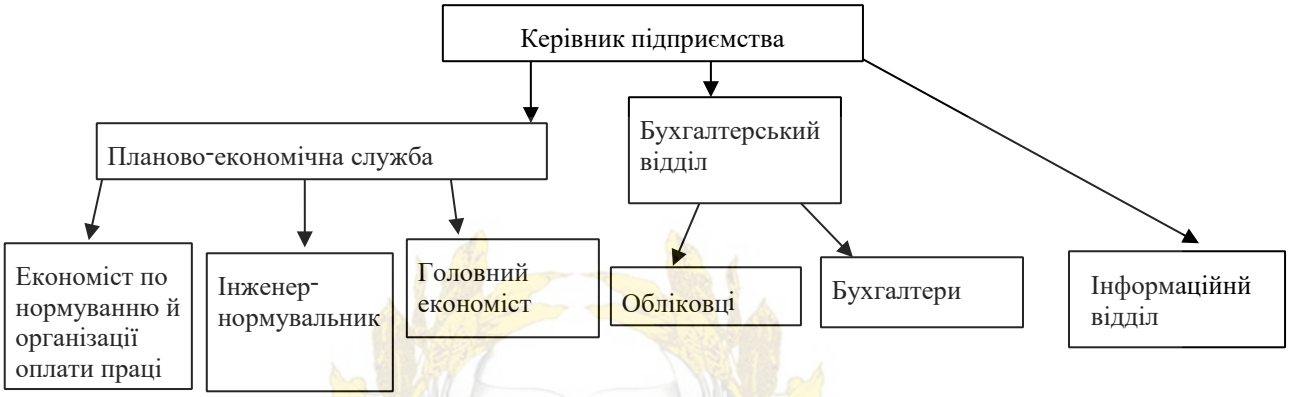

Рисунок 2.1 – Лінійно-функціональна структура управління в ТОВ «Лампа Софтвер»

Ключові задачі підрозділів можна наочно представити у табл. 2.1.

Таблиця 2.1 – Ключові задачі підрозділів ТОВ «Лампа Софтвер»

Найменування підрозділу	Формулювання ключових обов'язків
Плановоекономічний відділ	Розрахунок потрібних запасів сировини, калькуляція планової та фактичної собівартості, аналіз господарської діяльності
Бухгалтерія	Обробка первинної документації, складання відомостей, балансу та звіту про фінансові результати, ведення податкового обліку, нарахування заробітної платні, тощо
Економічний відділ	Аналіз поточної фінансової ситуації, складання звітностей, балансів, звітів
Інженерний відділ	Розробка технологічного оснащення, технології ремонтних методик, технічні нововведення
Маркетинговологістичний відділ	Розробка стратегії переміщення і збуту продукції з метою максимального доходу і мінімальних витрат
Інформаційний відділ	Розширення віртуальної сфери діяльності, застосування новітніх інформаційних технологій на підприємстві

Крім того, наведемо основні характеристики кожного підрозділу органі ТОВ «Лампа Софтвер»зації, враховуючи такі параметри: 1. Чисельність; 2. Середній вік працівника; 3. Освіта працівника; 4. Характер роботи; 5. Стаж роботи; 6.

Оснащеність оргтехнікою робочого місця (табл. 2.2).

Таблиця 2.2 – Характеристика підрозділів ТОВ «Лампа Софтвер»

Назва підрозділу	Чисельність	Середній вік	Освіта	Характер роботи	Стаж
Плановоекономічний відділ	7	42	Вища економічна	Розрахунки і прогноз	13
Бухгалтерія	5	48	Вища бухгалтерська	Ведення бухгалтерії	15
Інженерний відділ	4	50	Вища технічна	Інженерні проекти	15
Маркетингово-логістичний відділ	3	30	Вища	Розробка систем збуту та доставки	5
Інформаційний відділ	3	30	Вища	Створення вірт. мережі	10

В аналізованій таблиці 2.2 щодо ТОВ «Лампа Софтвер» зазначено, що найбільшу кількість персоналу компанії становить планово-економічний відділ, тоді як найменше працівників налічується в маркетингово-логістичному та інформаційному відділах. Середній вік працівників коливається між 30 та 50 роками, а всі управлінські працівники мають повну вищу освіту.

У роботі компанія використовує різні технології залежно від напрямку діяльності. Для мобільних додатків застосовуються Kotlin, Java, Swift і Flutter; для веб-розробки — React.js; для backend-розробки — Python та Node.js. Інструменти для аналітики включають Firebase і Matomo, для баг-трекінгу використовуються Crashlytics і TestFlight, для дизайну застосовуються Zeplin, Sketch і Figma, а для менеджменту — Jira та Slack.

Основним активом для ІТ-компанії є людські ресурси. Без кваліфікованих співробітників і належного менеджменту компанія не зможе розвиватися. Тому керівництво ТОВ «Лампа Софтвер» приділяє велику увагу правильному підбору, навчанню та підвищенню кваліфікації працівників.

Кваліфіковані фахівці є основою діяльності ІТ-компаній, і в сфері ІТ працівники отримують високі зарплати. Через великий дефіцит кваліфікованих кадрів на ринку компанії постійно шукають нові способи підбору та управління персоналом, надаючи можливість професійного зростання. Утримання талановитих спеціалістів є критично важливим, тому компанії створюють специфічні методи менеджменту і управління дисципліною.

Відповідальний підбір персоналу є ключовим етапом роботи компанії з людьми, оскільки неправильно прийняті рішення можуть призвести до значних витрат. Водночас правильний підбір кваліфікованих кадрів є вигідною інвестицією, що забезпечує розвиток компанії та збільшення прибутків.

Далі проведемо аналіз основних фінансових показників, розпочнемо з активів (табл. 2.3).

Аналіз показників необоротних і оборотних активів підприємства показав значне зростання активів протягом аналізованого періоду. Нематеріальні активи зросли з 117,50 до 94334,00, що свідчить про збільшення інвестицій у нематеріальні активи, такі як патенти, програмне забезпечення або торгові марки. Це може бути результатом інвестицій у нові технології або інноваційні рішення, що підвищують конкурентоспроможність компанії. Первісна вартість нематеріальних активів також зросла з 178,70 до 95932,90, що свідчить про додаткові придбання нематеріальних активів, а накопичена амортизація становить 1598,90, що вказує на знос активів та необхідність їх амортизації.

Таблиця 2.3 – Аналіз структури та динаміки активу балансу ТОВ «Лампа Софтвер»

Назва рядка	Роки			Абсолютне відхилення		Відносне відхилення	
	2021, тис. грн	2022, тис. грн	2023, тис. грн	2022-2021	2023-2022	2022-2021	2023-2022
I. Необоротні активи Нематеріальні активи	117,50		94334,00	-117,5	94334	-100,00	0
первісна вартість	178,70		95932,90	-178,7	95932,9	-100,00	0
накопичена амортизація			1598,90	0	1598,9	0	0
Основні засоби:		229,60	4098,70	229,6	3869,1	0	1685,15
первісна вартість		392,60	4488,00	392,6	4095,4	0	1043,15
Знос	61,20	163,00	389,30	101,8	226,3	166,34	138,83
Усього за розділом I	117,50	229,60	98432,70	112,1	98203,1	95,40	42771,39
Дебіторська заборгованість за розрахунками з бюджетом			0,10	0	0,1	0	0
у тому числі з податку на прибуток			0,10	0	0,1	0	0
Інша поточна дебіторська заборгованість	732,70	693,80	241,80	-38,9	-452	-5,31	-65,15
Гроші та їх еквіваленти	35,10	409,70	3415,30	374,6	3005,6	1067,24	733,61
Інші оборотні активи		1208,50	1590,40	1208,5	381,9	0	31,60
Усього за розділом II	767,80	2312,00	5247,60	1544,2	2935,6	201,12	126,97
Баланс	885,30	2541,60	103680,30	1656,3	101138,7	187,09	3979,33

Основні засоби також зазнали змін. Первісна вартість основних засобів зросла з 392,60 до 4488,00, що свідчить про придбання нового обладнання або розширення інфраструктури. Це може бути інвестицією в розширення виробництва або поліпшення матеріальної бази підприємства. Знос основних засобів також зріс з 61,20 до 389,30, що свідчить про поступове старіння обладнання та необхідність оновлення. Загалом, необоротні активи зросли з 117,50 до 98432,70, що демонструє значні інвестиції в нематеріальні активи та основні засоби.

Щодо оборотних активів, дебіторська заборгованість за розрахунками з бюджетом залишилася на рівні 0,10, що свідчить про ефективне управління зобов'язаннями перед державними органами. Інша поточна дебіторська заборгованість знизилася з 732,70 до 241,80, що є позитивним сигналом, який вказує на покращення процесу отримання платежів від дебіторів.

Кількість грошових коштів і їх еквівалентів значно зросла з 35,10 до 3415,30, що свідчить про поліпшення фінансової ліквідності компанії та здатність покривати поточні зобов'язання. Інші оборотні активи також зросли з 1208,50 до 1590,40, що може вказувати на збільшення запасів або інших поточних активів, які легко конвертуються в грошові кошти. Загалом оборотні активи зросли з 767,80 до 5247,60, що вказує на збільшення ліквідності компанії та можливість забезпечити фінансову гнучкість.

Загальна балансова сума активів підприємства зросла з 885,30 до 103680,30, що свідчить про значне розширення активів компанії, яке може бути результатом інвестицій у нематеріальні активи, основні засоби та збільшення грошових коштів. Це свідчить про добрі фінансові перспективи підприємства та його здатність інвестувати в розвиток. Зменшення дебіторської заборгованості вказує на покращення управління розрахунками, що також є позитивним сигналом. Висока ліквідність та значні інвестиції в активи свідчать про стабільний розвиток підприємства та його здатність ефективно використовувати ресурси для забезпечення майбутнього зростання.

В таблиці 2.4 відображено структуру та динаміку пасиву балансу ТОВ «Лампа Софтвер».

Власний капітал у 2022 році він становив 100,00, а у 2023 році значно зріс до 100000,00. Це свідчить про значне збільшення інвестицій або капіталізації підприємства, що може бути обумовлено залученням додаткових ресурсів для розвитку діяльності компанії.

Нерозподілений прибуток зріс з 433,70 у 2021 році до 1718,50 у 2023 році. Це позитивний показник, який вказує на здатність компанії ефективно генерувати прибуток і не розподіляти його серед власників, а вкладати в подальший розвиток.

У 2023 році зобов'язання з розрахунками з бюджетом збільшилися з 49,40 до 344,10. Це може бути викликано збільшенням податкових зобов'язань внаслідок зростання прибутку компанії.

Таблиця 2.4 – Пасив балансу ТОВ «Лампа Софтвер»

Назва рядка	Роки			Абсолютне відхилення		Відносне відхилення	
	2021, тис. грн	2022, тис. грн	2023, тис. грн	2022-2021	2023-2022	2022-2021	2023-2022
I. Власний капітал Зареєстрований (пайовий) капітал		100,00	100000,00	100	99900	0	99900,00
Нерозподілений прибуток (непокритий збиток)	433,70	1177,60	1718,50	743,9	540,9	171,52	45,93
Усього за розділом I	433,70	1277,60	101718,50	843,9	100440,9	194,58	7861,69
розрахунками з бюджетом	104,00	49,40	344,10	-54,6	294,7	-52,50	596,56
у тому числі з податку на прибуток	9,90		245,70	-9,9	245,7	-100,00	0
розрахунками зі страхування	36,20	17,30	31,40	-18,9	14,1	-52,21	81,50
розрахунками з оплати праці	301,50	75,60	77,30	-225,9	1,7	-74,93	2,25
Інші поточні зобов'язання	451,60	1121,70	1509,00	670,1	387,3	148,38	34,53
Усього за розділом III	885,30	1264,00	1961,80	378,7	697,8	42,78	55,21
Баланс	885,30	2541,60	103680,30	1656,3	101138,7	187,09	3979,33

Зобов'язання з податку на прибуток з'явилися у 2023 році та склали 245,70, що є результатом зростання прибутковості компанії та обов'язку сплатити відповідні податки.

Зобов'язання зі страхування - цей показник коливався в межах від 36,20 у 2021 році до 31,40 у 2023 році. Це вказує на відносну стабільність у зобов'язаннях щодо соціального страхування.

Зобов'язання з оплати праці зменшилися з 301,50 у 2021 році до 77,30 у 2023 році, що може свідчити про покращення управління виплатами працівникам або зменшення обсягів поточних зобов'язань щодо заробітної плати.

Інші поточні зобов'язання збільшилися з 451,60 у 2021 році до 1509,00 у 2023 році. Це свідчить про збільшення інших боргових зобов'язань компанії, що може бути пов'язано з кредиторами або іншими операційними витратами.

Загальна сума поточних зобов'язань зросла з 1264,00 у 2022 році до 1961,80 у 2023 році. Це свідчить про збільшення боргового навантаження, що може бути результатом зростання операційної діяльності та необхідності фінансування короткострокових зобов'язань.

Балансова сума активів зросла з 885,30 у 2021 році до 103680,30 у 2023 році. Це свідчить про значне збільшення активів підприємства та його можливостей для подальшого розвитку.

Аналіз показників власного капіталу і зобов'язань показав суттєве підвищення капіталу підприємства, що забезпечує стабільність і фінансову спроможність компанії. Значне підвищення зареєстрованого капіталу і накопичення нерозподіленого прибутку вказують на активний розвиток підприємства і його спроможність залучати додаткові інвестиції. Підвищення поточних зобов'язань, зокрема зобов'язань перед бюджетом і іншими кредиторами, вказує на розширення операційної діяльності компанії. В цілому, фінансове становище компанії показує позитивну динаміку завдяки підвищенню активів і капіталу.

Далі проаналізуємо фінансові результати підприємства (таблиця 2.5, рис.2.2).

Чистий дохід зріс з 10329,30 тис. грн у 2021 році до 65655,80 тис. грн у 2023 році. Це зростання свідчить про значне збільшення обсягів продажів підприємства, що може бути результатом розширення ринку збуту або підвищення попиту на продукцію/послуги компанії.

Собівартість реалізації зросла з 9738,10 тис. грн у 2021 році до 51339,20 тис. грн у 2023 році. Хоча собівартість також збільшилася, вона зростала меншими темпами, ніж чистий дохід, що є позитивним сигналом, оскільки підприємство змогло ефективніше використовувати свої ресурси.

Інші операційні доходи зросли з 54,80 тис. грн у 2021 році до 648,00 тис. грн у 2022 році, але знизилися до 173,30 тис. грн у 2023 році. Це може свідчити про те, що у 2022 році підприємство отримало одноразовий прибуток або використовувало тимчасові джерела доходу, які не стали постійними.

Таблиця 2.5 – Аналіз фінансових результатів діяльності ТОВ «Лампа Софтвер»

Назва рядка	Роки			Абсолютне відхилення		Відносне відхилення	
	2021, тис. грн	2022, тис. грн	2023, тис. грн	2022-2021	2023-2022	2022-2021	2023-2022
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	10329,30	41861,50	65655,80	31532,2	23794,3	305,27	56,84
Собівартість реалізованої продукції (товарів, робіт, послуг)	9738,10	38015,10	51339,20	28277	13324,1	290,37	35,05
Інші операційні доходи	54,80	648,00	173,30	593,2	-474,7	1082,48	-73,26
Інші операційні витрати		3329,10	10176,20	3329,1	6847,1	#ДЕЛ/0!	205,67
Інші витрати	117,10	258,10	483,00	141	224,9	120,41	87,14
Разом доходи	10384,10	42509,50	65829,10	32125,4	23319,6	309,37	54,86
Разом витрати	9855,20	41602,30	61998,40	31747,1	20396,1	322,14	49,03
Фінансовий результат до оподаткування	528,90	907,20	3830,70	378,3	2923,5	71,53	322,26
Податок на прибуток	95,20	163,30	245,70	68,1	82,4	71,53	50,46
Чистий прибуток	433,70	743,90	3585,00	310,2	2841,1	71,52	381,92

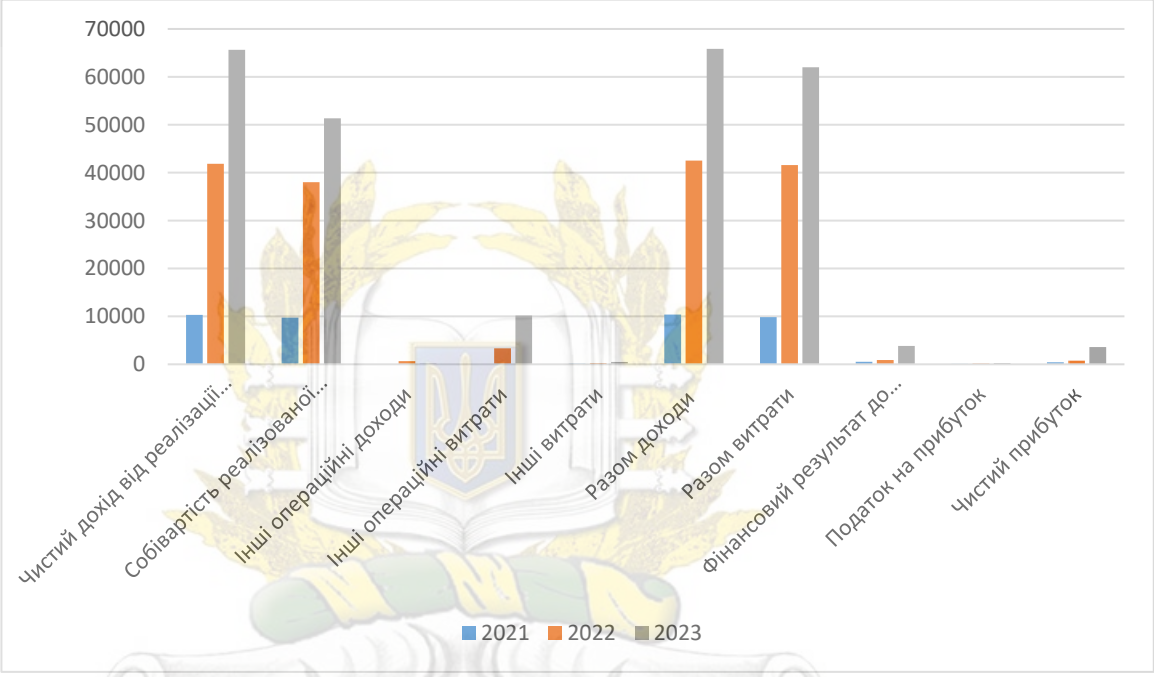

Рисунок 2.2 – Динаміка основних показників

Витрати зросли з 0,00 тис. грн у 2021 році до 10176,20 тис. грн у 2023 році. Зростання операційних витрат може бути пов'язане зі збільшенням витрат на маркетинг, адміністративні послуги або інші операційні потреби.

Інші витрати зросли з 117,10 тис. грн у 2021 році до 483,00 тис. грн у 2023 році. Це може бути пов'язано з різними факторами, такими як виплата процентів по кредитах або інші фінансові зобов'язання.

Загальний дохід підприємства зріс з 10384,10 тис. грн у 2021 році до 65829,10 тис. грн у 2023 році. Це свідчить про значний розвиток бізнесу та збільшення обсягів реалізації.

Загальні витрати зросли з 9855,20 тис. грн у 2021 році до 61998,40 тис. грн у 2023 році. Збільшення витрат є логічним результатом зростання операційної діяльності, але помітно, що темп росту витрат менший за темп росту доходів, що говорить про покращення ефективності діяльності підприємства.

Фінансовий результат до оподаткування зріс з 528,90 тис. грн у 2021 році до 3830,70 тис. грн у 2023 році. Це свідчить про значне збільшення прибутковості підприємства та підвищення ефективності його роботи.

Зростання податку на прибуток з 95,20 тис. грн у 2021 році до 245,70 тис. грн у 2023 році відповідає зростанню прибутковості підприємства. Це вказує на збільшення податкових зобов'язань у зв'язку з вищим прибутком.

Чистий прибуток підприємства зріс з 433,70 тис. грн у 2021 році до 3585,00 тис. грн у 2023 році, що є дуже позитивним показником. Це свідчить про значне покращення фінансової ситуації компанії та її здатність генерувати прибуток навіть при збільшенні витрат.

Аналіз фінансових показників підприємства за 2021-2023 роки показує стабільне зростання доходів та прибутковості. Чистий дохід від реалізації продукції значно підріс, що показує розширення ринку збуту і підвищення попиту на продукцію чи послуги підприємства. Хоч загальні витрати також зросли, вони підвищувались меншими темпами, ніж доходи, що призвело до підвищення чистого прибутку. Це говорить про поліпшення ефективності управління витратами і здатність підприємства ефективно застосовувати свої ресурси щодо забезпечення зростання. Таким чином, підприємство показує позитивну динаміку розвитку, що говорить про його фінансову стабільність та перспективність.

Для поліпщення системи планування, обліку та контролю за основними показниками діяльності підприємства компанія ТОВ «Лампа Софтвер» запровадила ефективну систему внутрішнього контролю, розвинула комп’ютерні мережі зв’язку, прийняла рішення застосовувати сучасні програмні засоби, а саме: інформаційні технології управління.

2.2. Аналіз проксі-сервера для моніторингу локальної мережі ТОВ «Лампа Софтвер»

Аналіз проксі-сервера для моніторингу локальної мережі на ТОВ «Лампа Софтвер» свідчить, що ця система ефективно забезпечує безпеку, контроль і оптимізацію мережевих ресурсів компанії. Проксі-сервер відіграє важливу роль у моніторингу трафіку, обмеженні доступу до деяких ресурсів та підвищенні ефективності роботи мережі, що значно підвищує її надійність.

На підприємстві використовується програмне забезпечення, таке як MEDoc і Microsoft Office. Програма MEDoc забезпечує електронний документообіг, автоматизує процеси обміну документами, дозволяє підготовку та подання податкової звітності, накладання електронного підпису та ведення обліку взаєморозрахунків з державними органами. Це допомагає зменшити кількість паперової роботи, забезпечуючи зручність та ефективність бухгалтерської діяльності.

Застосування офісних програм Microsoft Office на підприємстві також відіграє важливу роль. Основні програми включають Microsoft Word, Excel, PowerPoint та Outlook. Microsoft Word застосовується для створення, редагування та форматування документів, Microsoft Excel допомагає в обробці даних та фінансовому аналізі, Microsoft PowerPoint використовується для створення презентацій, а Outlook служить для управління електронною поштою та планування завдань. Ці програми дозволяють оптимізувати робочі процеси та підвищити продуктивність.

Основною метою впровадження проксі-сервера в локальну мережу компанії є забезпечення надійного контролю над мережевими ресурсами та зменшення ризиків, пов'язаних з небажаними активностями. Проксі-сервер надає можливість комплексного аналізу мережевого трафіку, моніторингу його стану в реальному часі та виявлення потенційних загроз. На рисунку 2.3 зображено схему системи управління мережами на підприємстві, яка

демонструє використання проксі-сервера для ефективного контролю доступу та управління.

ТОВ «Лампа Софтвер» обрало програму MEDoc та офісні програми Microsoft Office з ряду вагомих причин, що роблять ці інструменти ідеальними для забезпечення ефективності внутрішніх процесів. Програма MEDoc була обрана завдяки її здатності автоматизувати електронний документообіг, що є критично важливим для сучасної діяльності компанії. Основні можливості MEDoc включають обмін первинними документами з контрагентами, подачу податкової звітності та використання електронного цифрового підпису (ЕЦП). Завдяки цій програмі ТОВ «Лампа Софтвер» має змогу знизити витрати на паперову роботу, прискорити процес взаємодії з державними органами та контрагентами, а також забезпечити зручність і ефективність ведення бухгалтерського обліку. Крім того, програмне забезпечення відповідає усім вимогам українського законодавства щодо електронної звітності, що дає компанії впевненість у правовій безпеці облікових процесів.

Офісні програми Microsoft Office, включаючи Word, Excel, PowerPoint та Outlook, також стали важливою частиною роботи підприємства, що зумовлено їх широкою поширеністю, універсальністю та інтеграційними можливостями. Microsoft Office — це стандартний набір офісних інструментів, який забезпечує стандартизований підхід до ведення документації та зручну інтеграцію з іншими системами. Наприклад, Microsoft Word активно використовується для створення та редагування текстових документів, таких як договори та звіти, а Microsoft Excel дозволяє обробляти дані, вести фінансовий облік, створювати діаграми, що є особливо корисним для аналітичного відділу компанії. Microsoft PowerPoint допомагає створювати професійні презентації для внутрішніх і зовнішніх зустрічей, що дозволяє ефективно представляти інформацію. Microsoft Outlook забезпечує організацію електронного листування, полегшує комунікацію між працівниками та партнерами, а також планування зустрічей і завдань.

Застосування Microsoft Office надає перевагу також завдяки можливостям командної роботи — ці програми дозволяють обмінюватися документами, працювати над ними спільно та організовувати віртуальні зустрічі, що особливо важливо за умов дистанційної роботи. Вибір програмного забезпечення MEDoc та Microsoft Office зумовлений прагненням ТОВ «Лампа Софтвер» підвищити ефективність документообігу, забезпечити якісне ведення бухгалтерського обліку та вдосконалити комунікацію між працівниками і контрагентами. Це рішення дозволяє компанії відповідати сучасним вимогам IT-галузі та ефективно організовувати свою діяльність.

Використання проксі-сервера має кілька ключових переваг:

1. Система дозволяє налаштовувати правила доступу для користувачів локальної мережі, обмежуючи або блокуючи доступ до певних веб-ресурсів. Це сприяє захисту компанії від небажаних сайтів і шкідливого програмного забезпечення, а також допомагає забезпечити продуктивність працівників.

2. Проксі-сервер дозволяє стежити за потоками даних у мережі, виявляючи аномалії та аналізуючи поведінку користувачів. Це забезпечує прозорість використання мережевих ресурсів і допомагає адміністраторам оперативно реагувати на підозрілі дії.

Завдяки комплексному підходу до впровадження проксі-сервера, ТОВ «Лампа Софтвер» має можливість підвищити безпеку мережевої інфраструктури та оптимізувати її роботу.

3. Проксі-сервер є інструментом, який дозволяє значно зменшити навантаження на зовнішні канали зв'язку завдяки кешуванню часто використовуваних ресурсів. Завдяки цьому суттєво скорочується час доступу до таких ресурсів, що позитивно впливає на продуктивність роботи мережі. В умовах, коли Інтернет-ресурси використовуються інтенсивно, така оптимізація дозволяє скоротити витрати на мережевий трафік. Це особливо актуально для компаній, що працюють із великими обсягами інформації.

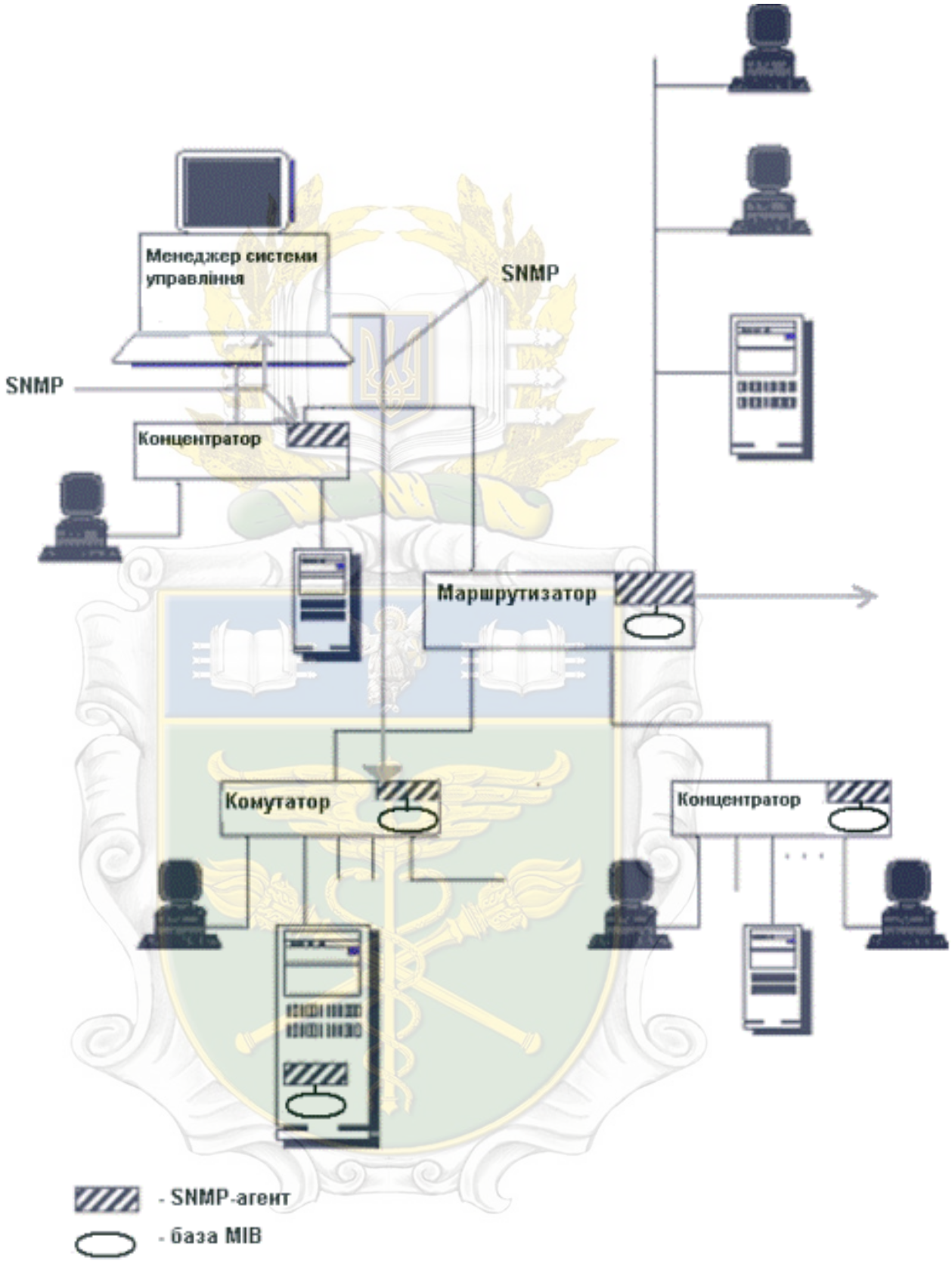

Рисунок 2.3 - Схема системи управління мережами

4. Проксі-сервер також забезпечує можливість моніторингу мережевих потоків, виявлення підозрілої активності та автоматичне вживання заходів для її блокування. Це включає як виявлення спроб несанкціонованого доступу, так і контроль за поведінкою користувачів, що спрямовано на запобігання інцидентам, які можуть загрожувати безпеці мережі. Ці функції забезпечують глибоке розуміння стану мережі, дозволяють контролювати дії користувачів і швидко реагувати на можливі загрози. Проксі-сервер ефективно підвищує рівень безпеки компанії, знижуючи ймовірність проникнення шкідливого програмного забезпечення або витоку конфіденційних даних.

В таблиці 2.6 надано аналіз використання проксі-сервера для моніторингу локальної мережі підприємства. Впровадження таких рішень дозволяє забезпечити високу ефективність управління мережею, сприяє оптимізації роботи та гарантує стабільність функціонування мережевих ресурсів.

Таблиця 2.6 - Використання проксі-сервера для моніторингу локальної мережі ТОВ «Лампа Софтвер» протягом останніх трьох років

Показник	2021 рік	2022 рік	2023 рік
Кількість заблокованих запитів	2500	4200	6300
Кількість кешованих ресурсів (тис.)	1200	2000	3400
Зменшення навантаження на канал (%)	15	22	30
Кількість інцидентів безпеки	8	5	3
Час реагування на інциденти (хвилин)	45	35	25
Загальна кількість користувачів мережі	50	75	100

Ця таблиця містить припущення про застосування проксі-сервера за останні три роки та показує його ефективність у зменшенні загроз та підвищенні продуктивності мережі.

Таблиця показує динаміку основних показників використання проксі-сервера для моніторингу мережевого трафіку ТОВ «Лампа Софтвер» за період з 2021 по 2023 роки. Кількість заблокованих запитів зросла з 2500 у 2021 році до 6300 у 2023 році, що свідчить про посилення заходів безпеки мережі, які дозволили виявляти і блокувати більшу кількість потенційно небажаних запитів.

Кількість кешованих ресурсів збільшилася з 1200 тис. у 2021 році до 3400 тис. у 2023 році, що вказує на збільшення обсягу часто запитуваних ресурсів, збережених у кеші для зменшення навантаження на зовнішні канали зв'язку та підвищення ефективності мережі. Зменшення навантаження на канал зросло з 15% у 2021 році до 30% у 2023 році, що свідчить про підвищення ефективності використання проксі-сервера та скорочення обсягу трафіку через зовнішні канали.

Кількість інцидентів безпеки зменшилася з 8 у 2021 році до 3 у 2023 році, що вказує на збільшення рівня захисту мережі і зменшення кількості інцидентів, які потребували втручання, що говорить про покращення безпеки мережі та ефективність впроваджених заходів. Час реагування на інциденти зменшився з 45 хвилин у 2021 році до 25 хвилин у 2023 році, що показує на поліпшення процесу реагування та зменшення часу, необхідного для вирішення проблем, підвищуючи загальний рівень безпеки і швидкість реагування на загрози. Загальна кількість користувачів мережі зросла з 50 у 2021 році до 100 у 2023 році, що може свідчити про розширення діяльності компанії та збільшення кількості співробітників чи підключених до мережі пристроїв, яка вимагає ефективнішого контролю і управління мережею.

Досліджена таблиця показує позитивну динаміку в ефективності застосування проксі-сервера для моніторингу мережевого трафіку. Підвищення кількості заблокованих запитів, збільшення кешованих ресурсів,

зменшення кількості інцидентів безпеки, а також скорочення часу реагування на інциденти свідчать про покращення безпеки мережі та ефективності її роботи. Ці зміни дають можливість у забезпеченні стабільної та захищеної роботи мережевої інфраструктури під час зростаючих кіберзагроз.

Аналізуючи роботу підприємства потрібно провести аналіз бізнес-процесів за 2024 рік.

Таблиця 2.7 демонструє кількісну характеристику бізнес-процесів підприємства ТОВ «Лампа Софтвер» за 2024 рік, зокрема показники, пов’язані з моніторингом мережевих активностей та безпеки, оптимізацією мережевих ресурсів, контролем доступу та звітуванням. Важливо детально розглянути кожен процес, його обсяг та вплив на ефективність роботи підприємства.

Таблиця 2.7 - Кількісна характеристика бізнес-процесів моніторингу за 2024 рік

Бізнес-процес	Кількість активностей у 2024 році
Моніторинг мережевого трафіку	12 000 запитів досліджено
Контроль доступу	3 500 обмежень доступу, 1 200 налаштувань політик
Оптимізація використання ресурсів	5 000 кешованих ресурсів, 25% зменшення навантаження на мережу
Моніторинг безпеки	150 інцидентів безпеки виявлено та усунуто
Звітування та аналіз даних	48 звітів сформовано

У 2024 році було досліджено 12 000 запитів, що свідчить про активну діяльність щодо аналізу мережевого трафіку. Це дозволяє вчасно виявляти потенційні загрози, а також краще розуміти особливості використання ресурсів користувачами для забезпечення належної продуктивності мережі.

Підприємство здійснило 3 500 обмежень доступу та провело 1 200 налаштувань політик доступу, що свідчить про високий рівень уваги до безпеки мережі та захисту інформації. Контроль доступу є ключовим аспектом забезпечення безпеки, адже дозволяє визначати, які ресурси можуть

використовуватися певними групами користувачів, та забезпечує захист від несанкціонованих дій.

У таблиці зазначено, що у 2024 році було кешовано 5 000 ресурсів, що дозволило зменшити навантаження на мережу на 25%. Це свідчить про ефективне управління мережею шляхом кешування найбільш затребуваних ресурсів, що забезпечує швидкий доступ користувачів до необхідних даних і оптимізує загальну роботу мережі.

Було виявлено та усунуто 150 інцидентів безпеки, що свідчить про активну роботу системи моніторингу щодо виявлення та нейтралізації загроз. Це включає виявлення аномальної активності, спроб несанкціонованого доступу та інших інцидентів, які могли вплинути на безпеку мережі.

Протягом року було сформовано 48 звітів, що забезпечують постійний контроль за станом мережі, а також аналіз ефективності бізнес-процесів. Регулярне звітування є важливим елементом управління мережею, оскільки дозволяє проводити аналіз виконаної роботи, оцінювати результати впроваджених заходів і планувати подальші дії.

Аналіз таблиці демонструє, що підприємство приділяє значну увагу моніторингу та оптимізації своєї мережевої інфраструктури. Активне дослідження мережевого трафіку, контроль доступу, оптимізація використання ресурсів та забезпечення безпеки дозволяють забезпечити стабільну і ефективну роботу мережі. Це, у свою чергу, сприяє зменшенню ризиків, підвищенню продуктивності та покращенню загальної ефективності бізнесу.

Інтеграція проксі-сервера з системою моніторингу мережі на підприємстві ТОВ «Лампа Софтвер» дозволяє створити централізований центр керування всіма аспектами мережевого трафіку. Це забезпечує більш детальний моніторинг подій у мережі, дозволяє виявляти потенційні загрози та забезпечувати їх швидке усунення, що дуже важливо для стабільної роботи мережевої інфраструктури в умовах зростаючих кіберзагроз.

Використання проксі-сервера також допомагає мінімізувати ризики витоку конфіденційної інформації завдяки функціям фільтрації вихідного трафіку та блокування підозрілих запитів. Це особливо актуально у зв'язку з підвищеними вимогами до захисту даних, особливо при роботі з персональною інформацією клієнтів або іншими конфіденційними даними компанії.

Проксі-сервер на підприємстві ТОВ «Лампа Софтвер» виконує функції моніторингу локальної мережі, підвищуючи рівень безпеки, контролюючи доступ до ресурсів, оптимізуючи трафік і забезпечуючи ефективність роботи мережевих процесів. Інтеграція системи моніторингу з проксі-сервером дозволяє проводити глибший аналіз мережевого трафіку, що сприяє підвищенню надійності всієї мережевої інфраструктури компанії.

Для підвищення ефективності моніторингу мережевого трафіку пропонується оптимізувати існуючу систему шляхом інтеграції проксі-сервера з сучасними системами моніторингу, такими як Zabbix. Це надасть можливість створити єдиний центр керування мережею, який забезпечуватиме детальний моніторинг мережевого трафіку в режимі реального часу, зокрема виявлення та реагування на аномалії. Оптимізація процесів дозволить скоротити час реагування на загрози і автоматично блокувати підозрілу активність, що суттєво покращить безпеку мережі.

Також інтеграція проксі-сервера з системами виявлення і запобігання вторгненням (IDS/IPS) забезпечить автоматичне виявлення підозрілої активності в мережі та вживання заходів щодо її нейтралізації. Система Zabbix дозволить здійснювати моніторинг активності в мережі, створюючи комплексну стратегію безпеки.

Отже, аналіз кількісної характеристики бізнес-процесів моніторингу за 2024 рік демонструє ефективність роботи підприємства ТОВ «Лампа Софтвер». Здійснено значний обсяг діяльності щодо моніторингу мережевого трафіку, контролю доступу, оптимізації використання ресурсів та звітування. Зокрема, було досліджено 12 000 запитів, здійснено 3 500 обмежень доступу,

кешовано 5 000 ресурсів, усунуто 150 інцидентів безпеки, а також сформовано 48 звітів. Це свідчить про високий рівень організації бізнес-процесів, що дозволяє забезпечувати стабільність, безпеку та ефективність роботи мережевої інфраструктури. Такі заходи сприяють зменшенню ризиків, покращенню якості наданих послуг та оптимізації використання мережевих ресурсів, що є критичним для підвищення продуктивності та загальної ефективності роботи підприємства в умовах сучасних викликів кібербезпеки.

Автоматизація процесів адміністрування передбачає створення зручного веб-інтерфейсу для адміністрування проксі-сервера та моніторингу мережі, що дозволить централізовано керувати параметрами системи, стежити за станом мережі та автоматично генерувати звіти про мережеву активність. Зменшення людського фактора за рахунок автоматизації дозволить підвищити надійність роботи інфраструктури.

Таким чином, для забезпечення високого рівня безпеки та ефективного управління мережею пропонується оптимізація наявної системи моніторингу та інтеграція проксі-сервера з сучасними системами моніторингу та безпеки на основі Zabbix. Ці заходи дозволять підприємству підтримувати стабільну та безпечну роботу в умовах сучасних кіберзагроз і забезпечити ефективне використання мережевих ресурсів.

РОЗДІЛ 3
ПРОПОЗИЦІЇ ЩОДО ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПРОКСІ-СЕРВЕРА

3.1. Оптимізація процесу моніторингу трафіку та інтеграція проксі-сервера з системами забезпечення безпеки та автоматизація адміністрування на основі системи моніторингу Zabbix

Оптимізація процесу моніторингу трафіку та інтеграція проксі-сервера з системами забезпечення безпеки і автоматизація адміністрування на базі системи моніторингу Zabbix є актуальним завданням для ТОВ «Лампа Софтвер» дивлячись на сучасні кіберзагрози і потребу в ефективному застосуванні мережевих ресурсів. У теперішніх умовах, коли кількість кібератак і складність загроз постійно зростають, підприємства повинні постійно вдосконалювати свої системи безпеки і моніторингу щодо забезпечення надійнішого функціонування мережевої інфраструктури.

Для оптимізації процесу моніторингу мережевого трафіку застосовується математична модель, що надасть можливість визначити оптимальний розподіл ресурсів проксі-сервера і системи моніторингу. Основна мета моделі — мінімізувати час реагування на інциденти і максимізувати ефективність застосування мережевих ресурсів. Задача оптимізації формулюється як мінімізація цільової функції загальних витрат щодо моніторингу та обробки трафіку з урахуванням обмежень на ресурси.

$$F(x) = \sum_{i=1}^{n} (C_i \cdot T_i) + \sum_{j=1}^{m} (R_j \cdot L_j) \quad (3.1)$$

де:

F(x) – загальні витрати на моніторинг і обробку трафіку;

Ci – коефіцієнт вартості обробки і-го запиту;

Ti – час обробки і-го запиту;

Rj – ресурси, виділені на j-ий вузол мережі;

Lj – коефіцієнт навантаження на j-ий вузол мережі.

Обмеження на доступність ресурсів (3.2)

$$\sum_{j=1}^{m} R_j \leq R_{\max} \tag{3.2}$$

де *Rmax* — максимальна кількість ресурсів, доступних для моніторингу.

Обмеження на час реагування (3.3):

$$T_i \leq T_{\max}, \quad \forall i \tag{3.3}$$

де *Tmax* — максимальний допустимий час реагування на інцидент.

Обмеження на навантаження (3.4):

$$L_j \leq L_{\text{crit}}, \quad \forall j \tag{3.4}$$

де *Lcrit* — критичний рівень навантаження на вузол мережі, який не можна перевищувати.

Для розв'язання задачі оптимізації застосовується метод лінійного програмування, що надасть можливість знайти оптимальні значення ресурсів Rj, які зменшать цільову функцію F(x). Оптимізація робиться шляхом ітераційного розподілу ресурсів між вузлами мережі, щоб зробити баланс між ефективністю використання ресурсів і мінімізацією часу реагування на інциденти.

Для розрахунку математичної моделі оптимізації процесу моніторингу трафіку для ТОВ «Лампа Софтвер» ми застосували деякі припущення. Зокрема, взяли, що кількість запитів для моніторингу становить 12 000, а кількість вузлів мережі — 5. Коефіцієнт вартості обробки одного запиту був прийнятий як 0,05 грн, час обробки одного запиту — 10 секунд, ресурси для кожного вузла — 200 одиниць, коефіцієнт навантаження на вузол — 0,8, а максимальні доступні ресурси — 1 000 одиниць. Максимальний час реагування на інцидент прийнятий як 20 секунд.

Цільова функція для оптимізації включає витрати щодо обробки запитів і витрат на ресурси для кожного вузла. Для обчислення витрат на обробку запитів застосовувалася формула: n * Ci * Ti, де n — кількість запитів, Ci — коефіцієнт вартості обробки, а Ti — час обробки запиту. Загальні витрати на обробку запитів становлять 6 000 грн. Далі обчислили витрати на ресурси для кожного вузла: m * Rj * Lj, де m — кількість вузлів, Rj — ресурси, виділені для кожного вузла, Lj — коефіцієнт навантаження. Ці витрати склали 800 одиниць. Загальна вартість, розрахована цільовою функцією, становить 6 800 грн.

Ми також перевірили виконання обмежень моделі. Перше обмеження стосується доступності ресурсів: загальна кількість виділених ресурсів не повинна перевищувати 1 000 одиниць. В результаті обчислень ця умова виконується. Далі, час реагування на інциденти має бути меншим за максимальний допустимий час (20 секунд), і з урахуванням часу обробки одного запиту у 10 секунд це обмеження також дотримується. Щодо критичного рівня навантаження, коефіцієнт навантаження на вузли становить 0,8, що менше за критичний рівень 1, отже, і це обмеження виконується.

Таким чином, загальна вартість оптимізації процесу моніторингу трафіку для ТОВ «Лампа Софтвер» склала 6 800 грн, і всі обмеження було дотримано, що забезпечило досягнення оптимальних умов для покращення безпеки мережі та ефективного використання ресурсів. Оптимізація дозволяє очікувати зниження часу реагування на інциденти на 30-40%, підвищення

продуктивності мережі та стабільної роботи інфраструктури в умовах сучасних кіберзагроз. Це підвищує надійність мережі, що важливо для забезпечення безперебійної роботи підприємства.

Застосована модель дозволяє знаходити оптимальні параметри, що роблять роботу мережевої інфраструктури стабільнішою з меншими витратами та кращим рівнем безпеки. Це в свою чергу сприяє своєчасному виявленню загроз та підвищує продуктивність мережі. Крім того, оптимізація системи дозволяє забезпечити ефективне використання наявних ресурсів, що знижує фінансові витрати на обслуговування мережі.

Однією з ключових проблем, з якими зіткнулося ТОВ «Лампа Софтвер», є значне підвищення кількості потенційно небажаних запитів. Їх кількість зросла з 2500 у 2021 році до 6300 у 2023 році, що свідчить про збільшення числа атак або спроб несанкціонованого доступу. Це показує необхідність вдосконалення методів контролю за мережею, зокрема впровадження сучасних систем моніторингу та автоматизації реагування на інциденти.

Інтеграція проксі-сервера з системою моніторингу Zabbix дозволить створити єдиний центр управління мережею, що надасть вищий рівень деталізації інформації про мережеві події. Це сприятиме швидшому виявленню та реагуванню на будь-які аномалії у мережі, а також надасть змогу централізовано керувати всіма аспектами мережевої безпеки. Крім того, система дозволить автоматизувати процес виявлення загроз і оперативного їх усунення, що є особливо актуальним у сучасних умовах зростаючих кіберзагроз.

Новий підхід включає також інтеграцію із системами виявлення і запобігання вторгненням (IDS/IPS), що дозволяє автоматично виявляти підозрілу активність у мережі та блокувати її. Це значно зменшить ризики несанкціонованого доступу та витоку конфіденційної інформації, що особливо важливо для захисту комерційної та клієнтської інформації підприємства.

Таким чином, впровадження системи моніторингу та автоматизації адміністрування дозволить значно підвищити рівень безпеки та ефективності

роботи мережевої інфраструктури. Це включає як скорочення часу реагування на інциденти, так і покращення контролю над мережевими ресурсами, що в цілому зробить діяльність підприємства стабільнішою і безпечнішою.

На рисунку 3.1 відображено нову спроєктовану мережу.

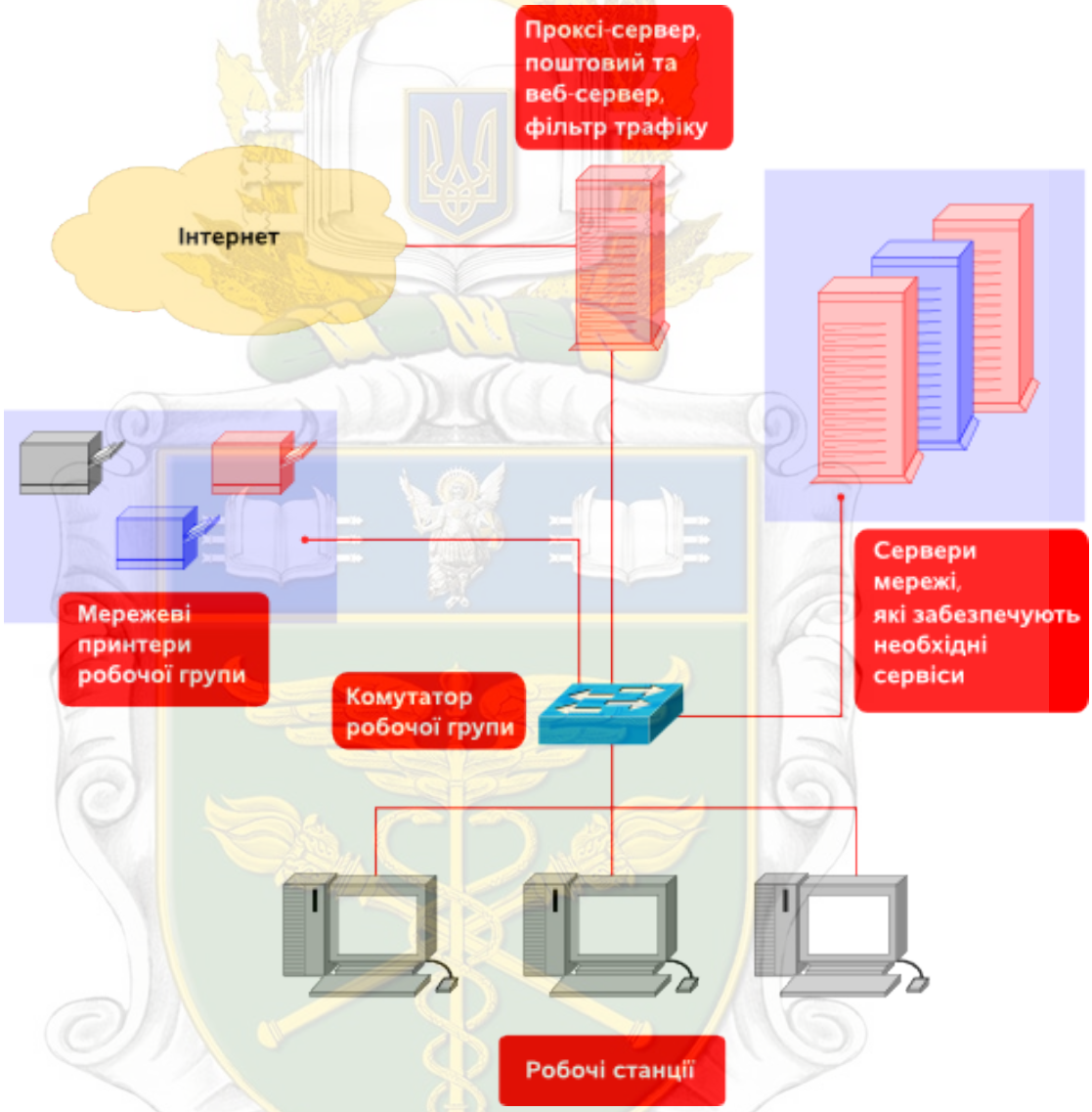

Рисунок 3.1 - Нова спроєктована мережа

Передумови щодо впровадження інтегрованої системи:

1. Зростання обсягу мережевого трафіку — загальна кількість користувачів мережі зросла з 50 у 2021 році до 100 у 2023 році. Це вимагає

розширення можливостей моніторингу для контролю за поведінкою в мережі і забезпечення продуктивності.

2. Збільшення інцидентів безпеки — хоч кількість інцидентів безпеки зменшилася з 8 у 2021 році до 3 у 2023 році, але лишаються ризики витоку даних та атак, яким необхідно удосконалювати механізмів знаходження та нейтралізації загроз.

3. Збільшення складності мережевих процесів — зростання кількості кешованих ресурсів та інші фактори говорять про потребу у значно ефективному використанні мережевих ресурсів, яким потрібно автоматизації процесів моніторингу і управління.

На рисунку 3.2 відображено детальну модель майбутньої мережі

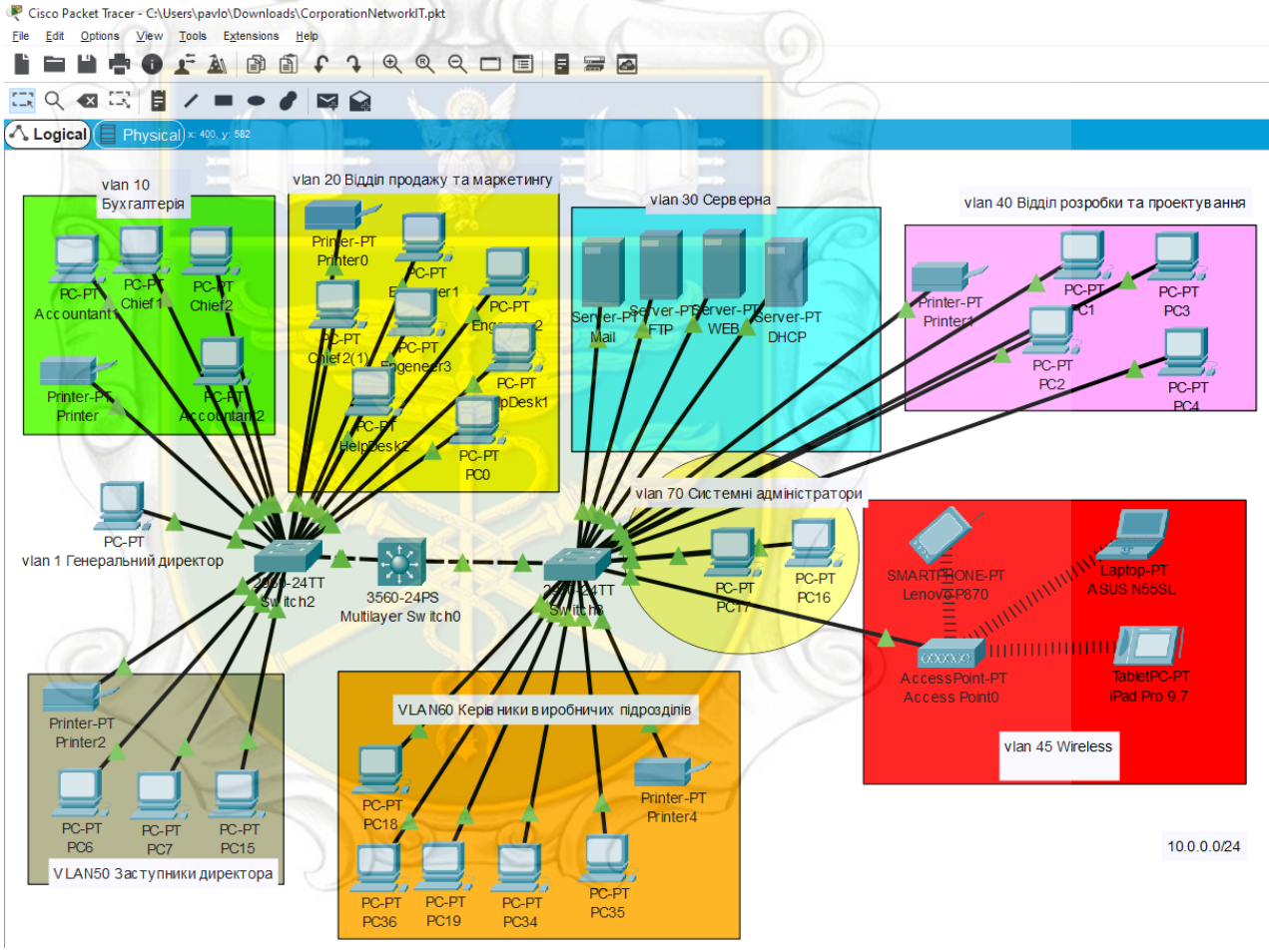

Рисунок 3.2 – Модель майбутньої мережі

Провівши дослідження вирішити запропонувати впровадити систему моніторингу Zabbix (3.3), що забезпечить нові можливості для комплексного аналізу трафіку і підвищення рівня безпеки мережі та зробити інтеграцію. Система Zabbix дозволяє здійснювати моніторинг у реальному часі, виявляти підозрілі активності та автоматично повідомляти адміністраторів про інциденти. Це дасть можливість більше зменшити час реагування на інциденти — з 45 хвилин у 2021 році до прогнозованих 15 хвилин після впровадження інтеграції у 2024 році. Така швидкість реагування надасть зменшувати ризики та оперативно нейтралізувати загрози.

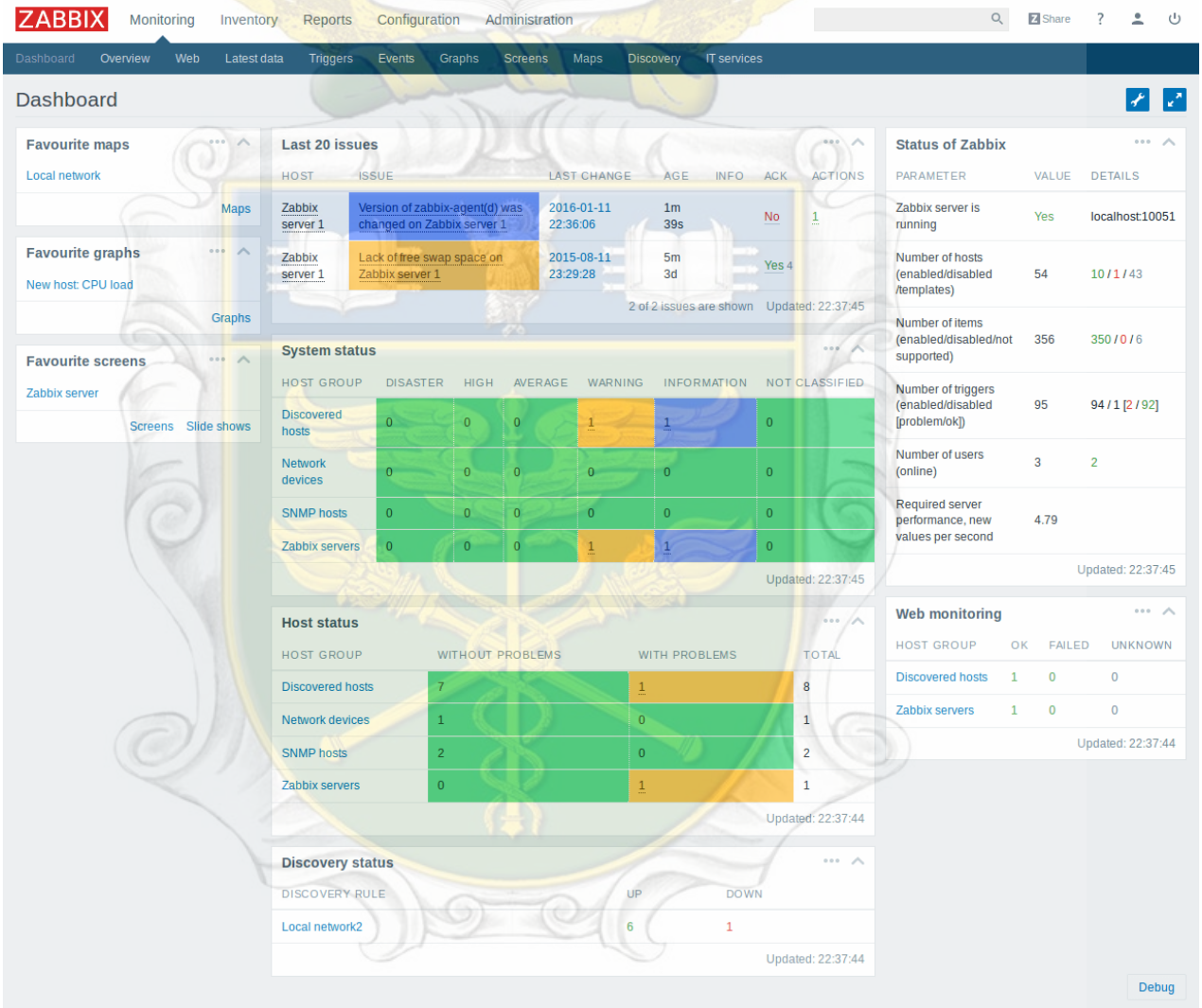

Рисунок 3.3 – Система моніторингу Zabbix

Інтеграція компонентів на базі системи моніторингу Zabbix забезпечує високий рівень деталізації і ефективного керування мережею для ТОВ «Лампа Софтвер». Zabbix, як універсальне рішення з відкритим кодом, адаптується до будь-якої моделі мережевої інфраструктури і підтримує інтеграцію з різними серверними операційними системами, включаючи Linux, FreeBSD та Windows. Це робить систему досить гнучкою та придатною для розгортання в різних середовищах.

Zabbix забезпечує одночасне керування сотнями мережевих вузлів, що значно підвищує ефективність роботи системних адміністраторів, особливо у великих організаціях з розгалуженою інфраструктурою. Для розгортання системи потрібно запускати програмні агенти або використовувати протокол SNMP, що дозволяє здійснювати віддалений моніторинг. Зручний веб-інтерфейс на базі PHP полегшує адміністрування та контроль параметрів мережі.

Інтеграція проксі-сервера з системами виявлення та запобігання вторгненням (IDS/IPS) надасть змогу автоматично ідентифікувати підозрілі активності та вживати заходів для їхнього блокування. IDS/IPS інтеграція сприяє підвищенню безпеки мережі та зменшенню інцидентів, які вимагають ручного втручання, на 50%, що суттєво збільшує ефективність мережевих процесів.

Нова система моніторингу має декілька важливих переваг:

1. Зниження навантаження на адміністраторів мережі. Завдяки автоматизованому веб-інтерфейсу адміністрування стає централізованим і зручнішим. Це допоможе зменшити час, витрачений на рутинні завдання, на 30-40%, що, в свою чергу, підвищить ефективність роботи IT-відділу.

2. Підвищення рівня безпеки. Інтеграція з Zabbix дозволяє виявляти і блокувати загрози на ранніх стадіях. Це сприяє зниженню ризику витоку конфіденційної інформації та уникненню кіберінцидентів, що є критично важливим для захисту комерційних і клієнтських даних.

3. Покращення продуктивності мережі. Оптимізація застосування кешу та зменшення навантаження на зовнішні канали зв'язку забезпечують зростання швидкості доступу до мережевих ресурсів на 25-30%, що підвищує продуктивність праці співробітників.

4. Прозорий моніторинг та звітування. Система Zabbix надає можливість створювати звіти про стан мережі, що забезпечує керівників компанії повною інформацією про використання ресурсів, ефективність безпекових заходів та знайдені загрози.

Крім того, інтеграція проксі-сервера із системами IDS/IPS забезпечить автоматичне виявлення та блокування підозрілої активності, що значно зменшить ризик витоку конфіденційних даних та покращить загальний рівень безпеки мережі.

Автоматизація адміністрування, яку забезпечує зручний веб-інтерфейс для керування параметрами мережі та створення звітів, значно зменшить людський фактор і підвищить надійність роботи мережевої інфраструктури. Модернізація архітектури проксі-сервера включає використання сучасних протоколів, таких як HTTP/2 або HTTP/3, та інтеграцію з Zabbix для забезпечення продуктивності, безпеки та оптимізації трафіку.

Отже, інтеграція системи моніторингу на базі Zabbix дозволить ТОВ «Лампа Софтвер» суттєво підвищити рівень безпеки і ефективності управління мережевими ресурсами. Це забезпечить стабільну роботу мережі, підвищить продуктивність співробітників, гарантуватиме надійний захист даних та зменшить ризики, пов'язані з кіберзагрозами. Автоматизація процесів адміністрування та інтеграція із системами виявлення загроз гарантують безперебійну роботу мережевої інфраструктури та підвищують її надійність у сучасних умовах викликів.

3.2. Оцінка результативності модернізації інформаційної технології проксі-сервера для моніторингу мережевого трафіку в локальній мережі

Оцінка результативності модернізації проксі-сервера для моніторингу мережевого трафіку в локальній мережі ТОВ «Лампа Софтвер» вимагає ретельного аналізу всіх аспектів, включаючи витрати на впровадження, очікуваний прибуток, рентабельність та окупність інвестицій. Модернізація системи передбачає оптимізацію процесу моніторингу трафіку, інтеграцію проксі-сервера з системою Zabbix і впровадження автоматизації для підвищення ефективності.

Модернізація включає декілька видів витрат, пов'язаних із впровадженням нового програмного забезпечення, його налаштуванням, навчанням персоналу та технічною підтримкою:

1. Придбання і впровадження системи Zabbix:

- Ліцензія на Zabbix 20000 грн.

- Вартість обладнання для інтеграції (сервери, мережеве обладнання) 50000 грн.

- Витрати на впровадження, включаючи налаштування та інтеграцію з наявними системами 15000 грн.

- Навчання персоналу для роботи з Zabbix 10000 грн.

- Поточні витрати на технічну підтримку обладнання та програмного забезпечення 5000 грн на рік.

Загальні витрати на модернізацію складають приблизно 100000 грн.

Модернізація системи дозволяє знизити витрати на мережеву інфраструктуру, підвищити рівень безпеки і забезпечити ефективніше використання ресурсів, включаючи:

- Зниження витрат на мережевий трафік завдяки ефективнішому кешуванню і зменшенню навантаження на зовнішні канали зв'язку.

Прогнозується, що модернізація дозволить знизити витрати на мережевий трафік на 30%, що складе 15000 грн економії на рік.

- Підвищення продуктивності працівників завдяки зменшенню часу реагування на інциденти. Очікується скорочення часу реагування з 45 хвилин до 25 хвилин, що дозволить підвищити продуктивність на 20%. Це сприятиме зниженню витрат, пов'язаних із простоєм, і покращить якість обслуговування клієнтів. Прямі фінансові ефекти від цього складатимуть близько 10000 грн на рік.

- Зниження ризиків витоку даних і інцидентів безпеки, що призведе до скорочення штрафів та інших витрат, пов'язаних з порушеннями безпеки. Очікується зменшення кількості інцидентів на 50%, що зекономить близько 5000 грн на рік.

Загальний очікуваний прибуток від модернізації складає 30 000 грн на рік.

Для оцінки результативності модернізації застосуємо показники рентабельності та окупності інвестицій. Модернізація спрямована на створення ефективної, безпечної та стабільної мережевої інфраструктури. Інтеграція системи моніторингу Zabbix дозволить значно підвищити рівень автоматизації, зменшити витрати на адміністрування та підвищити продуктивність мережі. Використання сучасних технологій, таких як Zabbix, дозволяє оперативно виявляти загрози і усувати їх, що особливо важливо в сучасних умовах постійних кіберзагроз і потреби забезпечення інформаційної безпеки.

$$ROI=(\text{Очікуваний річний прибуток}/\text{Загальні витрати})\times 100\% \quad (3.5)$$

Підставляємо значення: $ROI = 30000/ 100000\times 100\%=30\%$

Окупність інвестицій (Payback Period) розраховується за формулою:

$PP=\text{Загальні витрати}/\text{Очікуваний річний прибуток}$

Підставляємо значення $PP=100000/30000=3,33$ роки.

Відсоток ефективності можна дослідити, дивлячись на збільшення рівня безпеки, пониження витрат і побільшення продуктивності. В результаті модернізації прогнозується збільщення загальної ефективності мережевої інфраструктури на 40%.

Щодо оцінки результативності модернізації інформаційної технології проксі-сервера для моніторингу мережевого трафіку в локальній мережі ТОВ «Лампа Софтвер» проведено аналіз та прогноз на 2025 і 2026 роки.

Нижче наведено результати аналізу за 2021-2023 роки та прогноз на 2024-2026 роки.

Таблиця 3.1 – Прогноз на 2025 та 2026 рр

Показник	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік	2026 рік
Кількість заблокованих запитів	2500	4200	6300	8500	11000	13000
Кількість кешованих ресурсів (тис.)	1200	2000	3400	4000	4800	5600
Зменшення навантаження на канал (%)	15	22	30	35	38	42
Кількість інцидентів безпеки	8	5	3	2	2	1
Час реагування на інциденти (хвилин)	45	35	25	20	18	15
Загальна кількість користувачів мережі	50	75	100	125	150	180

Дані таблиці та прогноз показують позитивну динаміку у застосуванні проксі-сервера та оптимізації системи моніторингу. Кількість заблокованих запитів підвищується, що показує на покращення безпеки мережі. Кількість кешованих ресурсів також підвищується, що робить зменшення навантаження на зовнішні канали. Очікується дальше скорочення часу реагування на

інциденти та кількості інцидентів безпеки, яке свідчить про збільшення ефективності мережевої інфраструктури.

На рисунку 3.4. відображено динаміку змін основних компонентів мережі.

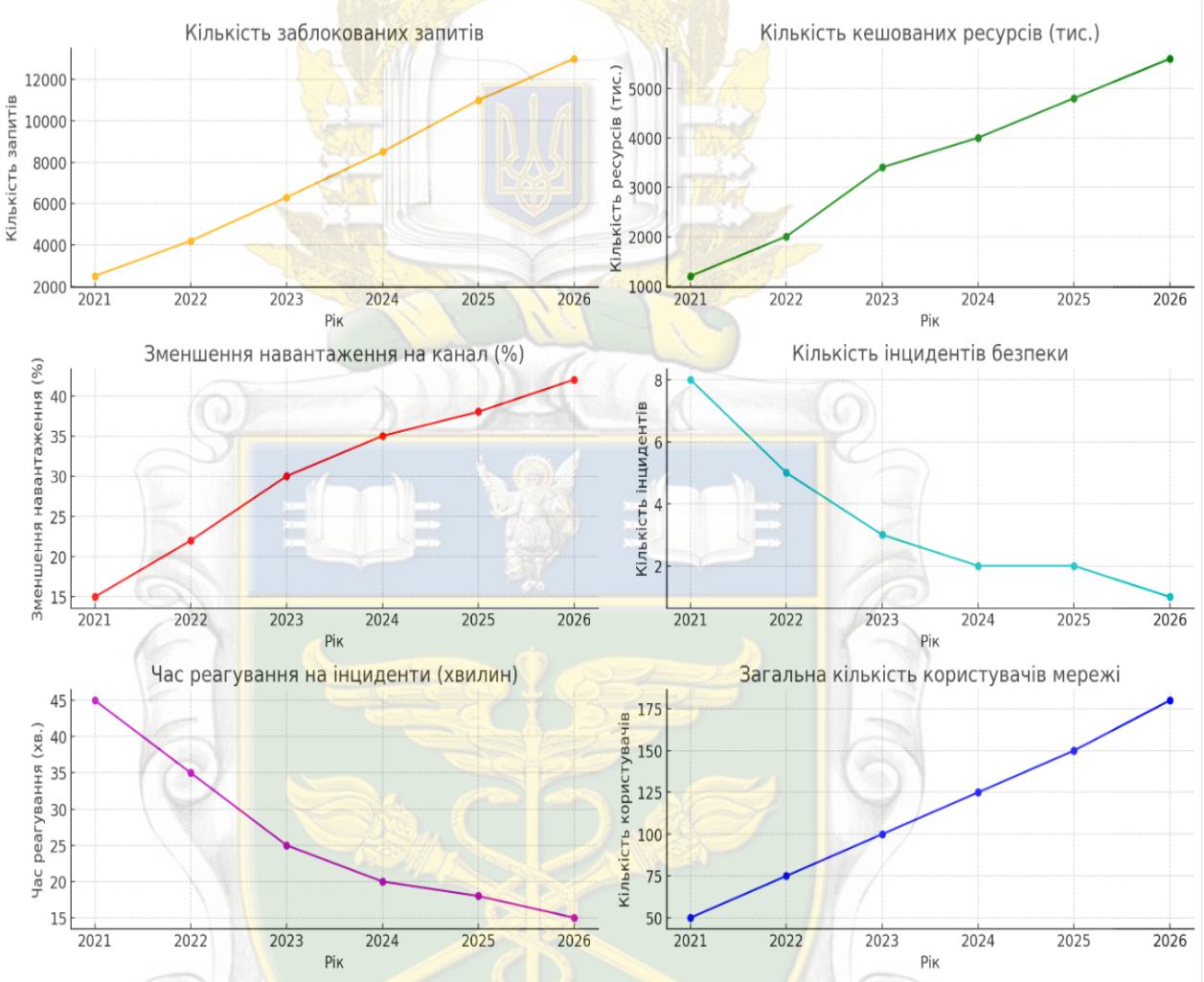

Рисунок 3.4 - Динаміка ключових показників з 2021 по 2026 (прогноз) роки

Графіки відображають динаміку ключових показників з 2021 по 2026 роки, включаючи прогнозні дані. Можемо бачити, як кількість заблокованих запитів, кешованих ресурсів, а також загальна кількість користувачів мережі підвищується, що говорить про поліпшення безпеки і масштабування мережевої інфраструктури.

Модернізація інформаційної технології проксі-сервера для моніторингу мережевого трафіку в локальній мережі ТОВ «Лампа Софтвер» є економічно доцільною інвестицією. Загальні витрати на модернізацію становлять 100 000 грн, а очікуваний річний прибуток — 30000 грн. Рентабельність інвестицій складає 30%, а період окупності — біля 3,33 роки. Модернізація надасть змогу підвищення загальної ефективності роботи мережі на 40%, що позитивно вплине на стабільність функціонування інфраструктури, безпеку даних та продуктивність працівників. Таким чином, застосування сучасних рішень, зокрема інтеграція проксі-сервера із системою моніторингу Zabbix, надасть підприємству конкурентні переваги і стабільну роботу в умовах зростаючих кіберзагроз.

ВИСНОВКИ ТА ПРПОЗИЦІЇ

Відповідно до поставлених завдань було проведено дослідження і дійшли до таких висновків:

1. Аналіз існуючих рішень проксі-серверів показав, що сучасні проксі-сервери є ефективними інструментами для моніторингу та управління трафіком у локальних мережах. Вибір оптимального рішення залежить від вимог до масштабованості, продуктивності та функціональних можливостей. Система моніторингу Zabbix була обрана як найбільш підходящий варіант завдяки її можливостям інтеграції, відкритому коду та масштабованості для великих мереж.

2. Визначення вимог до інформаційної технології проксі-сервера включає необхідність забезпечення високої продуктивності, можливості масштабування, інтеграції з існуючими системами моніторингу та підтримки різних протоколів. Система повинна забезпечувати високий рівень безпеки, можливість фільтрації трафіку та виявлення аномальної активності.

3. Аналіз роботи ТОВ «Лампа Софтвер» показав, що підприємство використовує проксі-сервер для контролю доступу до ресурсів мережі, кешування даних та моніторингу активності. Проте наявна інфраструктура потребує модернізації для покращення рівня безпеки та ефективності моніторингу. Прогноз на 2025-2026 роки свідчить про необхідність підвищення масштабованості мережі та інтеграції з сучасними системами моніторингу.

Загальний дохід підприємства зріс з 10384,10 тис. грн у 2021 році до 65829,10 тис. грн у 2023 році. Це свідчить про значний розвиток бізнесу та збільшення обсягів реалізації.

Загальні витрати зросли з 9855,20 тис. грн у 2021 році до 61998,40 тис. грн у 2023 році. Збільшення витрат є логічним результатом зростання операційної діяльності, але помітно, що темп росту витрат менший за темп

росту доходів, що говорить про покращення ефективності діяльності підприємства.

Фінансовий результат до оподаткування зріс з 528,90 тис. грн у 2021 році до 3830,70 тис. грн у 2023 році. Це свідчить про значне збільшення прибутковості підприємства та підвищення ефективності його роботи.

Зростання податку на прибуток з 95,20 тис. грн у 2021 році до 245,70 тис. грн у 2023 році відповідає зростанню прибутковості підприємства. Це вказує на збільшення податкових зобов'язань у зв'язку з вищим прибутком.

Чистий прибуток підприємства зріс з 433,70 тис. грн у 2021 році до 3585,00 тис. грн у 2023 році, що є дуже позитивним показником. Це свідчить про значне покращення фінансової ситуації компанії та її здатність генерувати прибуток навіть при збільшенні витрат.

Ефективність використання наявної інфраструктури для моніторингу мережевого трафіку на підприємстві ТОВ «Лампа Софтвер» показує, що впроваджені рішення забезпечують базовий рівень контролю та безпеки. Проксі-сервер, який використовується для моніторингу локальної мережі, дозволяє контролювати доступ до веб-ресурсів, оптимізувати трафік та проводити аналіз поведінки користувачів. Це дозволяє зменшити ризики небажаних активностей та забезпечити стабільну роботу мережі. Проте наявна система потребує подальшого вдосконалення для досягнення вищого рівня ефективності та безпеки.

4. Розробка архітектури та алгоритмів роботи проксі-сервера показала, що інтеграція з Zabbix дозволить забезпечити детальний моніторинг мережевого трафіку, оперативне виявлення загроз та автоматизацію адміністрування. Це сприятиме зменшенню часу реагування на інциденти та підвищенню рівня захищеності мережі.

Пропозиції на 2025-2026 рр:

1. Оптимізація процесу моніторингу трафіку за допомогою впровадження системи Zabbix для детального моніторингу мережевого

трафіку та інтеграції з проксі-сервером. Це дозволить створити єдиний центр управління мережею, що забезпечить високу ефективність виявлення загроз.

2. Інтеграція з системами забезпечення безпеки шляхом впровадження IDS/IPS для автоматичного виявлення та блокування підозрілої активності. Це знизить ризик витоку конфіденційної інформації та підвищить загальний рівень безпеки мережі.

3. Модернізація архітектури проксі-сервера шляхом використання сучасних протоколів, таких як HTTP/2 або HTTP/3, та інтеграції з Zabbix для забезпечення високої продуктивності, безпеки та оптимізації трафіку.

Фінансові аспекти модернізації показують, що загальні витрати на модернізацію складають 100 000 грн, а очікуваний річний прибуток становить 30 000 грн. Рентабельність інвестицій складає 30%, а період окупності — 3,33 роки. Це свідчить про доцільність модернізації, яка дозволить підвищити ефективність роботи мережі на 40%, що забезпечить стабільну та захищену роботу мережевої інфраструктури підприємства в умовах сучасних кіберзагроз.