ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Метод підвищення ефективності моніторингу процесу дистанційної роботи на основі безпроводових мереж»

на здобуття освітнього ступеня магістра

зі спеціальності 172 Електронні комунікації та радіотехніка

освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій МАРТИНЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти
групи АРДМ-63
Олексій МАРТИНЮК

Керівник: Назарій БЛАЖЕННИЙ

Рецензент: _____

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Електронні комунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мартинюку Олексію Сергійовичу

1. Тема кваліфікаційної роботи: «Метод підвищення ефективності моніторингу процесу дистанційної роботи на основі безпроводових мереж»,
керівник кваліфікаційної роботи Назарій БЛАЖЕННИЙ, доктор філософії, затверджена наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 р. №320.

2. Строк подання кваліфікаційної роботи 25.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Основні елементи моніторингу бездротових мереж.
2. Існуючі системи моніторингу дистанційної роботи.
3. Протоколи моніторингу SNMP, RMON.
4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Аналіз сучасних методів моніторингу бездротових мереж.
2. Методи підвищення ефективності моніторингу.
3. Розробка та впровадження системи моніторингу.

4. Аналіз результатів дослідження.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	26.10.24	Викон.
2.	Аналіз сучасних методів моніторингу бездротових мереж	29.10.24	Викон.
3.	Методи підвищення ефективності моніторингу	01.12.24	Викон.
4.	Розробка та впровадження системи моніторингу	02.11.24	Викон.
5.	Аналіз результатів дослідження	11.12.24	Викон.
6.	Висновки, вступ, реферат	25.12.24	Викон.
7.	Розробка презентації	26.10.24	Викон.

Здобувач вищої освіти _____ Олексій МАРТИНЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Назарій БЛАЖЕННИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Мартинюка Олексія Сергійовича

на тему: «Метод підвищення ефективності моніторингу процесу дистанційної роботи на основі безпроводових мереж»

Актуальність:

Нова парадигма, яка швидко набирає оберти в сценарії безпровідного зв'язку та має унікальну ідентифікацію і дозволяє об'єктам взаємодіяти один з одним для отримання даних на веб-сервері, для зберігання і збору даних і для спільної роботи з користувачами.

Система моніторингу трафіку в режимі реального часу є надійною для користувачів є надійнішою, легко працює користувачами і недорогою системою і легко може бути встановлена у будь-якому місці.

Позитивні сторони:

1. Зміст магістерської роботи відповідає завданню. Її автор, показав високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.
2. Текст викладений грамотно, ясно, послідовно. Графічний матеріал оформлений якісно. Широко використовується сучасна науково-технічна література, включаючи англомовні видання.

Недоліки:

1. Не повністю проаналізовано зниження ризиків кіберзагроз та забезпечення стабільної роботи всієї мережевої інфраструктури
2. Необхідно більш детально висвітлити техніко-економічний ефект від впровадження запропонованих рішень.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «добре», а здобувач Мартинюк Олексій Сергійович заслуговує присвоєння кваліфікації: «Магістр з електронних комунікацій та радіотехніки».

Рецензент: _____

(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Мартинюк О.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Метод підвищення ефективності моніторингу процесу дистанційної роботи на основі безпроводових мереж

Кваліфікаційна робота і рецензія додаються.

В.о. директора ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Мартинюк Олексій Сергійович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Мартинюка Олексія Сергійовича на оцінку «добре» та присвоїти йому кваліфікацію «Магістр з електронних комунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Назарій БЛАЖЕННИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Мартинюк О.С.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедрою
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 70 стор., 12 рис., 7 табл., 33 джерел.

Мета роботи – розробка та впровадження методів підвищення ефективності моніторингу процесу дистанційної роботи на основі бездротових мереж.

Об'єкт дослідження - є процес моніторингу бездротових мереж, що забезпечують дистанційну роботу.

Предмет дослідження – методи та технології підвищення ефективності моніторингу процесу дистанційної роботи на основі бездротових мереж.

Короткий зміст роботи: В магістерській роботі досягнуто наступних результатів:

1. У першому розділі виконано огляд існуючих систем моніторингу дистанційної роботи, проаналізовано особливості бездротових мереж у процесі моніторингу, виклики та проблеми під час моніторингу віддалених процесів, а також описано практику використання технологій Wi-Fi, Bluetooth, та LTE у моніторингу.

2. У другому розділі розглянуто оптимізацію збору та обробки даних, використання протоколів SNMP для моніторингу, можливості інтеграції хмарних технологій для обробки великих обсягів даних, а також використання систем штучного інтелекту для аналізу даних моніторингу.

3. У третьому розділі досліджено архітектуру системи моніторингу, можливості використання програмного забезпечення для аналізу та збереження даних, механізми сповіщення, а також виконано тестування та оцінку ефективності системи.

4. У четвертому розділі побудовано графік порівняння розробленої системи з існуючими рішеннями, виконано практичні дослідження щодо економічної ефективності впровадженої системи та створено таблицю оцінки надійності та масштабованості системи.

КЛЮЧОВІ СЛОВА: ДИСТАНЦІЙНА РОБОТА, МОНІТОРИНГ БЕЗДРОТОВИХ МЕРЕЖ, WI-FI, SNMP, БЕЗПЕКА МЕРЕЖІ, ЕФЕКТИВНІСТЬ МОНІТОРИНГУ, АНАЛІЗ ДАНИХ, КІБЕРБЕЗПЕКА, ОПТИМІЗАЦІЯ МЕРЕЖЕВИХ ПРОЦЕСІВ, СИСТЕМА ПОПЕРЕДЖЕННЯ

ABSTRACT

Text part of the master's qualification work: 70 pages, 12 figures, 7 tables, 33 sources.

The purpose of the work - development and implementation of methods to improve the efficiency of monitoring the process of remote work based on wireless networks.

Object of research – there is a process of monitoring wireless networks that enable remote work.

Subject of research – methods and technologies to improve the efficiency of monitoring the process of remote work based on wireless networks.

Summary of the work: The following results were achieved in the master's thesis:

1. The first chapter reviews existing remote work monitoring systems, analyses the features of wireless networks in the monitoring process, challenges and problems in monitoring remote processes, and describes the practice of using Wi-Fi, Bluetooth, and LTE technologies in monitoring.

2. The second section discusses the optimization of data collection and processing, the use of SNMP protocols for monitoring, the possibilities of integrating cloud technologies for processing large amounts of data, and the use of artificial intelligence systems for analyzing monitoring data.

3. The third section examines the architecture of the monitoring system, the possibilities of using software for data analysis and storage, notification mechanisms, as well as testing and evaluation of the system's effectiveness.

4. In the fourth section, a graph comparing the developed system with existing solutions is built, practical studies on the economic efficiency of the implemented system are carried out, and a table for assessing the reliability and scalability of the system is created.

KEYWORDS: DISTANCE, WIRELESS NETWORK MONITORING, WI-FI, SNMP, NETWORK SECURITY, MONITORING EFFICIENCY, DATA ANALYSIS, CYBERSECURITY, NETWORK PROCESS OPTIMISATION, WARNING SYSTEM

ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів 9
ВСТУП 9
РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ МОНІТОРИНГУ БЕЗДРОТОВИХ МЕРЕЖ 11
1.1. Огляд існуючих систем моніторингу дистанційної роботи 13
1.2. Особливості бездротових мереж у процесі моніторингу 16
1.3. Виклики та проблеми під час моніторингу віддалених процесів 19
1.4. Використання технологій Wi-Fi, Bluetooth, та LTE у моніторингу 22
РОЗДІЛ 2. МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ 27
2.1. Оптимізація збору та обробки даних 30
2.2. Використання протоколів SNMP для моніторингу 34
2.3. Інтеграція хмарних технологій для обробки великих обсягів даних 39
2.4. Використання систем штучного інтелекту для аналізу даних моніторингу 42
РОЗДІЛ 3. РОЗРОБКА ТА ВПРОВАДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ 49
3.1. Архітектура системи моніторингу 49
3.2. Використання програмного забезпечення для аналізу та збереження даних 51
3.3. Механізми сповіщення .....**Помилка! Закладку не визначено.**
3.4 Тестування та оцінка ефективності системи 59
РОЗДІЛ 4. АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ 65
4.1. Порівняння розробленої системи з існуючими рішеннями 65
4.2. Економічна ефективність впровадження системи 70
4.3. Оцінка надійності та масштабованості системи 73
ВИСНОВКИ 79
ПЕРЕЛІК ПОСИЛАНЬ 80

Перелік умовних позначень, символів, скорочень і термінів

ЛОМ – локальні обчислювальні мережі.

ОС – операційна система.

API (Advanced Mobile Phone Service) – розширений сервіс мобільного зв'язку.

ARP (Address Resolution Protocol) – протокол адресного розширення.

CRC (Cyclic Redundancy Check) – контроль циклічної надлишковості.

HTTP (HyperText Transfer Protocol) – протокол передачі гіпертексту.

ICMP (Internet Control Message Protocol) – протокол керування повідомленнями Інтернету.

IETF (Internet Engineering Task Force) – організація, що займається розробкою технічних стандартів Інтернету.

IoT (Internet of Things) – інтернет речей.

IP (Internet Protocol) – Інтернет-протокол.

IT (Information Technology) – інформаційні технології.

MIB (Management Information Base) – база керування інформацією.

OSI (Open Systems Interconnection) – модель взаємодії відкритих систем.

RMON (Remote Network Monitoring) – віддалений моніторинг мережі.

SNMP (Simple Network Management Protocol) – простий протокол керування мережею.

TCP (Transmission Control Protocol) – протокол керування передачею.

ВСТУП

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що дозволяє впроваджувати нові форми організації праці, зокрема дистанційну роботу. Використання бездротових мереж для забезпечення віддаленого доступу до корпоративних ресурсів значно підвищило гнучкість і мобільність працівників. Однак, поряд з цими перевагами, зросли і ризики, пов’язані з безпекою та ефективністю таких мереж. Відсутність постійного фізичного контролю над інфраструктурою, різноманітність бездротових протоколів, а також збільшення кількості кіберзагроз ускладнюють процес управління та моніторингу мережевих процесів під час дистанційної роботи.

Одним з найважливіших аспектів успішної організації дистанційної роботи є забезпечення надійного моніторингу бездротових мереж, який дозволяє не тільки виявляти та усувати аномалії в режимі реального часу, але й запобігати потенційним інцидентам, пов’язаним з безпекою даних. Ефективний моніторинг сприяє підвищенню продуктивності працівників, зниженню ризиків кіберзагроз та забезпеченню стабільної роботи всієї мережевої інфраструктури.

Актуальність даного дослідження зумовлена необхідністю розробки нових підходів до моніторингу бездротових мереж в умовах дистанційної роботи, які враховували б специфіку використання різних бездротових технологій і дозволяли підвищити ефективність роботи мережі. Вивчення методів оптимізації моніторингу, а також використання сучасних інструментів для збору та обробки мережевих даних є важливим завданням для забезпечення безпеки та стабільності в сучасних організаціях.

Мета, завдання та структура роботи сформовані таким чином, щоб дослідити можливості підвищення ефективності моніторингу бездротових мереж та розробити відповідні рішення для дистанційної роботи.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ МОНІТОРИНГУ БЕЗДРОТОВИХ МЕРЕЖ

Моніторинг бездротових мереж є важливим завданням для забезпечення ефективності, надійності та безпеки мережевої інфраструктури, особливо в умовах дистанційної роботи. Сучасні методи моніторингу розвиваються разом із технологіями бездротового зв'язку, і кожен з них має свої переваги та виклики. Розглянемо основні підходи та інструменти, які використовуються для моніторингу бездротових мереж.

1. Протоколи моніторингу (SNMP, RMON)

Протоколи, такі як SNMP (Simple Network Management Protocol) та RMON (Remote Network Monitoring), є базовими інструментами для керування та моніторингу мереж. SNMP забезпечує збір даних про стан мережевих пристроїв у реальному часі, надаючи інформацію про навантаження на мережу, її продуктивність та можливі збої. SNMP широко використовується завдяки своїй простоті та здатності працювати з різними типами мережевих пристроїв, включно з бездротовими маршрутизаторами та точками доступу.

RMON доповнює SNMP, забезпечуючи розширені можливості моніторингу трафіку в бездротових мережах. Він дозволяє аналізувати не лише стан пристроїв, але й загальний мережевий трафік, що є корисним для виявлення аномалій або потенційних загроз.

2. Інструменти аналізу мережевого трафіку

Існує низка спеціалізованих інструментів, таких як Wireshark, Kismet, Aircrack-ng, які дозволяють здійснювати глибокий аналіз мережевого трафіку в бездротових мережах. Ці інструменти використовуються для перехоплення та аналізу пакетів даних, що циркулюють у мережі, і можуть допомогти виявити зловмисну активність, проблеми з продуктивністю або інші аномалії.

Wireshark дозволяє відслідковувати пакети в режимі реального часу та аналізувати їхню структуру, що є важливим для детальної діагностики проблем у мережі. Kismet спеціалізується на виявленні бездротових мереж, точок доступу та

аналізі трафіку. Aircrack-ng є інструментом для тестування безпеки Wi-Fi мереж, включно з виявленням уразливостей у шифруванні.

3. Системи моніторингу продуктивності та безпеки

Такі системи, як Nagios, Zabbix, та PRTG Network Monitor, надають комплексні рішення для моніторингу стану мережі, її продуктивності та безпеки. Ці системи дозволяють встановлювати індикатори стану мережі та налаштовувати сповіщення в разі виявлення проблем. Наприклад, Zabbix може бути використаний для постійного моніторингу стану точок доступу та маршрутизаторів у Wi-Fi мережах.

Завдяки інтеграції з SNMP, такі інструменти можуть збирати інформацію про стан мережевих пристроїв і аналізувати продуктивність мережі в реальному часі. Це дозволяє швидко виявляти вузькі місця в роботі бездротової мережі, а також попереджати потенційні інциденти, пов'язані з продуктивністю чи безпекою.

4. Хмарні рішення для моніторингу

З поширенням хмарних технологій з’явилися нові рішення для моніторингу мереж, такі як SolarWinds Cloud Monitoring та Datadog. Вони забезпечують централізоване спостереження за бездротовими мережами, дозволяючи збирати та аналізувати дані про стан мережі з будь-якої точки доступу. Такі системи забезпечують гнучкість, масштабованість і можливість аналізу великих обсягів даних в режимі реального часу.

5. Технології штучного інтелекту та машинного навчання

Останнім часом все більшого поширення набувають технології штучного інтелекту (AI) та машинного навчання (ML), які застосовуються для аналізу великих обсягів мережевого трафіку та виявлення аномалій. AI-рішення, такі як Cisco AI Network Analytics, дозволяють автоматизувати процес моніторингу, виявляти відхилення в трафіку та прогнозувати потенційні загрози або збої в роботі мережі.

6. Моніторинг Інтернету речей (IoT)

Зі зростанням кількості пристроїв, що належать до Інтернету речей (IoT), виникла необхідність у специфічних рішеннях для моніторингу таких пристроїв, які підключені до бездротових мереж. Спеціальні платформи, такі як Palo Alto IoT Security, дозволяють відстежувати трафік IoT-пристроїв і забезпечувати їхній захист у бездротових мережах.

Сучасні методи моніторингу бездротових мереж надають широкі можливості для збору та аналізу даних про стан мережі. Однак, вибір конкретного підходу або інструмента залежить від завдань, що стоять перед мережею, її масштабів і вимог до безпеки. Подальший розвиток технологій штучного інтелекту, хмарних рішень та IoT дозволить ще більше оптимізувати процес моніторингу та забезпечити стабільну роботу бездротових мереж в умовах дистанційної роботи.

1.1. Огляд існуючих систем моніторингу дистанційної роботи

Моніторинг дистанційної роботи став важливою частиною корпоративного управління в умовах віддаленої праці. Існує чимало систем, які допомагають роботодавцям контролювати продуктивність працівників, забезпечуючи баланс між ефективністю та конфіденційністю. Розглянемо основні категорії таких систем та кілька популярних рішень у кожній з них (табл.1.1).

1. Трекери часу та продуктивності

Ці програми фіксують час, який працівник використовує на різні завдання і добавки. Також вони часто пропонують аналіз активності та продуктивності працівників.

- Toggl Track – дозволяє працівникам самостійно вмикати і вимікати таймер для завдань, а також отримувати аналітичні звіти.
- RescueTime – автоматично аналізує продуктивність, розрізняючи продуктивні й непродуктивні дії.
- Clockify – простий інструмент трекінгу часу з можливістю налаштування на різних проектах [21].

2. Програмне забезпечення моніторингу активності

Ці системи моніторингу, які додатки та веб-сайти використовують під час роботи, а також рівень активності працівника.

- Time Doctor – фіксує відвідані веб-сайти, час роботи, а також робить скриншоти для підтвердження продуктивності.

Таблиця 1.1.

Існуючі системи моніторингу дистанційної роботи

Категорія систем	Опис	Популярні рішення
1. Трекери часу та продуктивності	Фіксують час роботи, аналізують продуктивність завдань.	**Toggl Track** – ручне вмикання/вимикання таймера, аналітичні звіти. **RescueTime** – автоматичний аналіз дій. **Clockify** – трекінг часу з проєктним налаштуванням.
2. Програмне забезпечення моніторингу активності	Відстежують активність, веб-сайти, використані програми та рівень роботи.	**Time Doctor** – фіксація сайтів та скриншоти. **Hubstaff** – активність із візуальними звітами. **ActivTrak** – аналітика активності та візуалізація робочих процесів.
3. Інструменти для комунікації та управління завданнями	Сприяють розподілу завдань, контролю виконання та прозорості робочих процесів.	**Asana** – розподіл та відстеження завдань. **Trello** – візуальне управління завданнями. **Jira** – контроль проєктів, популярний серед IT-команд.
4. Програмне забезпечення для автоматичного збору звітів	Генерують автоматизовані звіти та аналізують продуктивність на основі даних.	**Workpuls** – реальний час моніторингу та звіти. **Teramind** – аналітика ресурсів та виявлення порушень політики.
5. Системи на основі штучного інтелекту	Використовують алгоритми для аналізу даних та оптимізації робочого процесу.	**SentryPC** – машинне навчання для аналізу активності. **Controlio** – AI-аналіз поведінки та оптимізація роботи.

- Hubstaff – збирає дані про активність, включаючи скриншоти та трекінг відвіданих веб-сайтів, що дозволяє оцінити ефективність.

- ActivTrak – пропонує аналітику на основі активності, включаючи візуалізацію робочого процесу для кращого розуміння залученості команди [18].

3. Інструменти для комунікації та управління завданнями

Вони мають керівникам розподіляти завдання, контролювати їх виконання, а також забезпечують прозорість процесу роботи в команді.

- Asana – дозволяє створювати, відстежувати завдання та проекти, а також дає можливість керівникам бачити прогрес команди.
- Trello – система візуального управління завданнями, яка дозволяє спільно працювати над проектами та досліджувати їх виконання.
- Jira – більш розширена система для управління проектами, популярна серед IT-команд, з трекінгом завдань і контролем над робочим процесом [6].

4. Програмне забезпечення для автоматичного збору звітів та аналізу даних такі інструменти можуть автоматично генерувати звіти та видавати візуалізовану інформацію для керівництва, що дозволяє спростити аналіз продуктивності.

- Workpuls – відстежує активність працівників у режимі реального часу та надає докладні звіти, які допомагають краще розуміти продуктивність команди.
- Teramind – пропонує докладні звіти про використання ресурсів, активність працівників і керівникам, які виявляють точки ризику чи порушення політики компанії [12].

5. Системи на основі штучного інтелекту для аналізу робочого процесу

Інструменти на основі штучного інтелекту дозволяють прогнозувати продуктивність працівників та оптимізувати робочий процес, спираючись на зібрані дані.

- SentryPC – використовує машинне навчання для аналізу активності, передаючи керівництво про зниження продуктивності чи потенційні ризики.
- Controlio – з використанням алгоритмів аналізує поведінку працівників та пропонує сайти для оптимізації процесу роботи [13].

Системи моніторингу дистанційної роботи позбавляють керівництва контролювати продуктивність працівників та оптимізувати їхні робочі процеси. Вибір конкретного рішення залежить від особливостей діяльності компанії та її

потреб у моніторингу. Важливо знайти баланс між контролем і збереженням довіри та приватності працівників, оскільки більший контроль може негативно вплинути на мотивацію та лояльність.

1.2. Особливості бездротових мереж у процесі моніторингу

Бездротові мережі є елементом сучасного процесу моніторингу, особливо в умовах, коли багато працівників працюють віддалено або з мобільних пристроїв. Вони забезпечують гнучкість, доступність і масштабованість для обміну даними та відстеження різних параметрів роботи. Проте такі мережі мають і деякі особливості, які варто отримати (рис.1.1).



Рис. 1.1. Основні елементи моніторингу бездротових мереж

1. Безпека

Безпека є основним викликом для бездротових мереж, оскільки вони більш вразливі до кібератаків у порівнянні з дротовими. У моніторингу бездротової мережі потрібні такі заходи:

- Шифрування даних – використання протоколів WPA3, WPA2 або VPN для захисту від несанкціонованого доступу.
- Аутентифікація користувачів – забезпечення лише авторизованого доступу для захисту конфіденційності.
- Моніторинг загроз – відстеження аномалій у мережевому трафіку для виявлення можливих атак, наприклад, DDoS.

2. Пропускна здатність і стабільність зв'язку

Бездротові мережі можуть обмежити пропускну здатність, особливо якщо до них підключено велику кількість пристроїв.

- Контроль навантаження – важливо контролювати кількість підключених пристроїв, щоб уникнути перевантаження і зниження продуктивності.
- Покращення якості сигналу – використання точок доступу та антен для стабільного сигналу та зниження рівня затримок.
- Пріоритизація трафіку – налаштування QoS (Quality of Service), які не дозволяють пріоритизувати важливі типи трафіку для стабільної роботи критичних добавок.

3. Реагування на зміни мережевих умов

Бездротові мережі частіше піддаються впливу зовнішніх факторів, таких як погодні умови, фізичні перешкоди або інші електромагнітні джерела.

- Адаптація частоти – автоматичне або ручне регулювання для зменшення інтерференції від інших частотних пристроїв.
- Моніторинг продуктивності мережі – збір даних про швидкість передачі, рівень сигналу і затримки дозволяє реагувати на зміни в умовах мережі [11].

4. Мобільність і доступність

Однією з ключових переваг бездротових мереж є їхня мобільність, що дозволяє користувачам підключатися з будь-якої точки в зоні покриття.

- Моніторинг доступу до ресурсів – перевірка доступу користувачів до ресурсів мережі дозволяє контролювати, чи підтримує їх стабільне підключення в різних зонах покриття.
- Відстеження місця розташування – моніторинг місця розташування пристроїв дозволяє контролювати переміщення працівників і покращувати безпеку.

5. Інтеграція з іншими системами моніторингу

Бездротові мережі можуть бути інтегровані з іншими системами для підвищення ефективності моніторингу.

- Інтеграція з системами управління завданнями – дозволяє зберігати звіти про активність в режимі реального часу.
- Аналітика і машинне навчання – використання даних із бездротової мережі для прогнозування продуктивності та виявлення деяких загроз або проблем [3].

6. Моніторинг IoT-пристроїв

Бездротові мережі часто використовують для підключення пристроїв Інтернет-речей (IoT), що забезпечують додаткові можливості моніторингу.

- Відстеження стану IoT-пристроїв – моніторинг працездатності та передачі даних з IoT-пристроїв, які можуть бути корисними для аналізу різних параметрів роботи.
- Енергоефективність – остання IoT-пристрої можуть працювати від батарейок, важливо мінімізувати їхнє енергоспоживання шляхом оптимізації роботи бездротових з'єднань [28].

Бездротові мережі створюють гнучки і зручне середовище для моніторингу роботи, а також вимагають додаткових заходів безпеки, контролю продуктивності та адаптивності. Використання сучасних технологій, таких як штучний інтелект для аналізу даних і прогнозування, дозволяє забезпечити стабільний і захищений процес моніторингу в бездротових мережах.

1.3. Виклики та проблеми під час моніторингу віддалених процесів

Моніторинг віддалених процесів, особливо в умовах дистанційної роботи, має низку викликів і проблем, пов'язаних як із технічними аспектами, так і з управлінням персоналом. Нижче зазначено основні труднощі, з якими стикаються компанії та IT-відділи під час моніторингу віддалених процесів.

1. Забезпечення безпеки та конфіденційності

- Ризик кібератак і витоку даних . Віддалене підключення вимагає надійного захисту, після чого працівники можуть використовувати особисті або ненадійні пристрої та мережі. Використання VPN, шифрування даних і двофакторної аутентифікації стає необхідним для мінімізації ризиків.
- Конфіденційність працівників . Надмірний моніторинг може створити у працівників недовіри почуття та створити конфлікти щодо особистої інформації, яка потребує чіткого визначення, що саме відстежується та як використовується ці дані [21].

2. Технічні обмеження

- Проблеми з доступом до Інтернету . Не всі працівники мають стабільний або високошвидкісний доступ до Інтернету, що впливає на їх продуктивність і здатність виконувати певні завдання. Нестабільне з'єднання може переривати процеси моніторингу та зменшувати точність зібраних даних.
- Обмеження програмного забезпечення . Деякі системи моніторингу мають обмежені функції для віддаленого управління або контролю. Наприклад, не всі програми можуть ефективно відстежувати продуктивність без деяких прив’язок до локальної мережі [22].

3. Складність оцінки продуктивності

- Неможливість повної об'єктивності . Продуктивність працівника у віддаленому середовищі важко оцінити лише на основі часу, проведеного в мережі чи на певних ресурсах. Це можна вимагати додаткових показників, як-від оцінки виконаних завдань, якості роботи та загального вкладу в проект.

- Невизначеність ефективності моніторингу . Надмірна увага до часу та активності в мережі може призвести до мікроменеджменту та зниження мотивації працівників, особливо коли їхні реальні результати не залежать від цих показників [14].

4. Проблеми з комунікацією і координацією

- Відсутність особистого контакту . Віддалені команди можуть відчувати брак комунікації, що ускладнює координацію завдань, обмін знаннями та інтеграцію нових членів команди. Це також можна позначати на процесі моніторингу, коли потрібно оперативно реагувати на зміни або проблеми.
- Різниця в часових поясах . Для глобальних команд це можна ускладнити узгодження робочого часу, а також, й моніторинг виконання певних процесів у реальному часі [21].

5. Висока вартість і потреба у спеціалізованих інструментах

- Фінансові витрати на програмне забезпечення . Деякі системи моніторингу можуть бути дорогими у впровадженні та обслуговуванні. Також потрібні витрати на оновлення інструментів і забезпечення їх сумісності з іншими корпоративними системами.
- Навчання працівників . Використання складного програмного забезпечення для моніторингу може вимагати навчання працівників, що потребує додаткових ресурсів і часу [17].

6. Психологічні аспекти та вплив на працівників

- Виникнення стресу та тривоги . Працівники, які відчувають сильний контроль, можуть відчувати стрес і тривогу, що негативно впливають на їхню продуктивність і задоволеність роботою.
- Зниження рівня довіри . Постійний моніторинг може створити у працівників почуття, що їм не довіряють. Це може призвести до зниження мотивації та залученості в робочий процес [31].

7. Проблеми з дотриманням законодавства

- Відповідність законодавству про конфіденційність . У деяких країнах діють жорсткі закони щодо збору та зберігання персональних даних. Компанії

повинні дотримуватися законодавства, як-от GDPR в ЄС, яке регулює, з якими даними можна вибирати і як їх потрібно захищати [16].

- Врахування прав працівників . У деяких юрисдикціях моніторинг працівників може бути обмежений, і компанії повинні дотримуватися цих норм, щоб уникнути юридичних слідків [21].

Для унаочнення інформації моніторинг віддалених процесів відображено у таблиці 1.2.

Таблиця 1.2.

Моніторинг віддалених процесів

Категорія	**Проблема**	**Деталі**
Безпека та конфіденційність	Ризик кібератак і витоку даних	Використання VPN, шифрування даних, двофакторна аутентифікація
	Конфіденційність працівників	Чітке визначення, що саме моніториться, та як використовуються дані
Технічні обмеження	Проблеми з доступом до Інтернету	Нестабільне з'єднання впливає на продуктивність та точність даних
	Обмеження програмного забезпечення	Деякі програми мають обмеження на віддалене використання
Складність оцінки продуктивності	Неможливість повної об'єктивності	Потрібні додаткові показники, як-от виконані завдання та якість роботи
	Невизначеність ефективності моніторингу	Мікроменеджмент знижує мотивацію працівників
Комунікація та координація	Відсутність особистого контакту	Брак комунікації ускладнює координацію завдань та обмін інформацією
	Різниця в часових поясах	Узгодження робочого часу для глобальних команд
Висока вартість та інструменти	Фінансові витрати на програмне забезпечення	Вартість впровадження та обслуговування програмного забезпечення
	Навчання працівників	Витрати на навчання персоналу для роботи з інструментами
Психологічні аспекти	Виникнення стресу та тривоги	Надмірний контроль викликає стрес та тривогу
	Зниження рівня довіри	Моніторинг створює відчуття недовіри та знижує мотивацію
Дотримання законодавства	Відповідність законодавству про конфіденційність	Дотримання законів, як-от GDPR, щодо захисту персональних даних
	Врахування прав працівників	Дотримання прав працівників у різних юрисдикціях

Моніторинг віддалених процесів вимагає важливого підходу, де потрібні технічні, організаційні, правові та психологічні аспекти. Ідеальне рішення повинно підтримувати продуктивність і захищати дані, не створюючи додаткового стресу для працівників. Для цієї компанії необхідно вибирати адаптивні системи моніторингу та підтримувати прозорі політики щодо збору та використання даних.

1.4. Використання технологій Wi-Fi, Bluetooth, та LTE у моніторингу

Технології Wi-Fi , Bluetooth та LTE виконують важливу роль у моніторингу віддалених процесів, надаючи можливість передачі даних і взаємодії пристроїв без прив’язки до дротових мереж. Кожна з цих технологій має свої особливості та використовує в різних сценаріях моніторингу. Розглянемо їхні основні функції та обмеження.

1. Wi-Fi

Wi-Fi є найбільш популярною технологією великого бездротового зв'язку, яка дозволяє швидко передавати обсяги даних на коротких і середніх відстанях.

- Використання в моніторингу : Wi-Fi активно використовується для підключення комп'ютерів, IoT-пристроїв і мобільних пристроїв до мереж в офісних і домашніх умовах. Це дозволяє відстежувати активність співробітників, відстежувати продуктивність та обмін даними між пристроями.
- Переваги : Wi-Fi забезпечує високу швидкість передачі даних, стабільність з'єднання та можливість підключення багатьох пристроїв одночасно.
- Недоліки : Wi-Fi вимагає наявності доступної мережі або точки доступу, і це може бути проблемою в регіонах з обмеженим покриттям. Також Wi-Fi піддається впливу перешкод і є вразливим до кібератаку, що вимагає посиленого захисту.

2. Bluetooth

Bluetooth – це технологія бездротового зв'язку на короткій відстані, яка споживає мало енергії, що робить її популярною для підключення портативних пристроїв.

- Використання у моніторингу : Bluetooth часто використовується для збору даних із портативних пристроїв, сенсорів та носіїв гаджетів (наприклад, фітнес-трекерів). Вона дозволяє відстежувати рухи працівників у межах робочих зон, передавати дані від IoT-сенсорів у реальний час та здійснювати моніторинг зони покриття.
- Переваги : Низьке енергоспоживання та зручність для пристроїв, які потребують частого підключення та передачі невеликих обсягів даних на обмеженій відстані.
- Недоліки : Bluetooth має невелику зону покриття (до 10 метрів для додаткових пристроїв) та обмеження швидкості передачі даних, що робить його менш придатним для об’єднання великих мереж або передачі інформації великих обсягів.

3. LTE (4G/5G)

Технологія LTE забезпечує широкомасштабне підключення до Інтернету для мобільних пристроїв та дає можливість високошвидкісної передачі даних на великих відстанях.

- Використання в моніторингу : LTE ідеально підходить для віддаленого моніторингу в реальному часі, особливо для мобільних пристроїв, розташованих поза офісом або в різних географічних точках. Ця технологія дозволяє відстежувати пересування співробітників, відстежувати стан транспортних засобів і підключатися до віддалених систем.
- Переваги : Висока швидкість, надійне покриття та можливість підтримувати велику кількість підключених пристроїв. LTE також дозволяє використовувати мережеві ресурси у віддалених регіонах, де немає доступу до Wi-Fi.
- Недоліки : Залежність від оператора зв'язку і тарифи на мобільний Інтернет можуть бути високими, що вимагає витрат на моніторинг. LTE також має нижчу швидкість передачі даних у порівнянні з Wi-Fi у зоні стабільного захисту.

Таблиця 1.3

Порівняльна таблиця використання технологій у моніторингу

Технологія	**Зона покриття**	**Швидкість передачі даних**	**Енергоспоживання**	**Основні сценарії використання**
Wi-Fi	Коротка-середня	Висока	Середнє	В офісах, для пристроїв IoT
Bluetooth	Коротка	Низька	Низьке	Носімі гаджети, внутрішній моніторинг
LTE (4G/5G)	Велика (місто, регіон)	Висока (особливо 5G)	Високе	Віддалений моніторинг, GPS-трекінг

Варто звернути увагу на енергоспоживання технологій у моніторингу (рис.1.2).

Перший графік демонструє, що LTE забезпечує найбільшу дальність дії – до 10 км, що робить його ідеальним для широкомасштабного моніторингу та роботи у віддалених регіонах. Wi-Fi має середню дальність близько 0,1 км, що обмежує його використання у межах закритих просторів або локальних мереж. Bluetooth демонструє найменшу дальність (0,01 км), що робить його підходящим для моніторингу на близькій відстані, наприклад, у носимих пристроях чи IoT-середовищі.

На другому графіку видно, що Wi-Fi забезпечує найвищу швидкість передачі даних – до 600 Мбіт/с, що є критично важливим для моніторингу, який потребує великих обсягів інформації, наприклад, відеопотоків. LTE забезпечує швидкість близько 100 Мбіт/с, що також є достатнім для передавання даних у режимі реального часу, проте поступається Wi-Fi. Натомість Bluetooth має найменшу швидкість – до 3 Мбіт/с, що обмежує його використання для моніторингу невеликих обсягів даних.

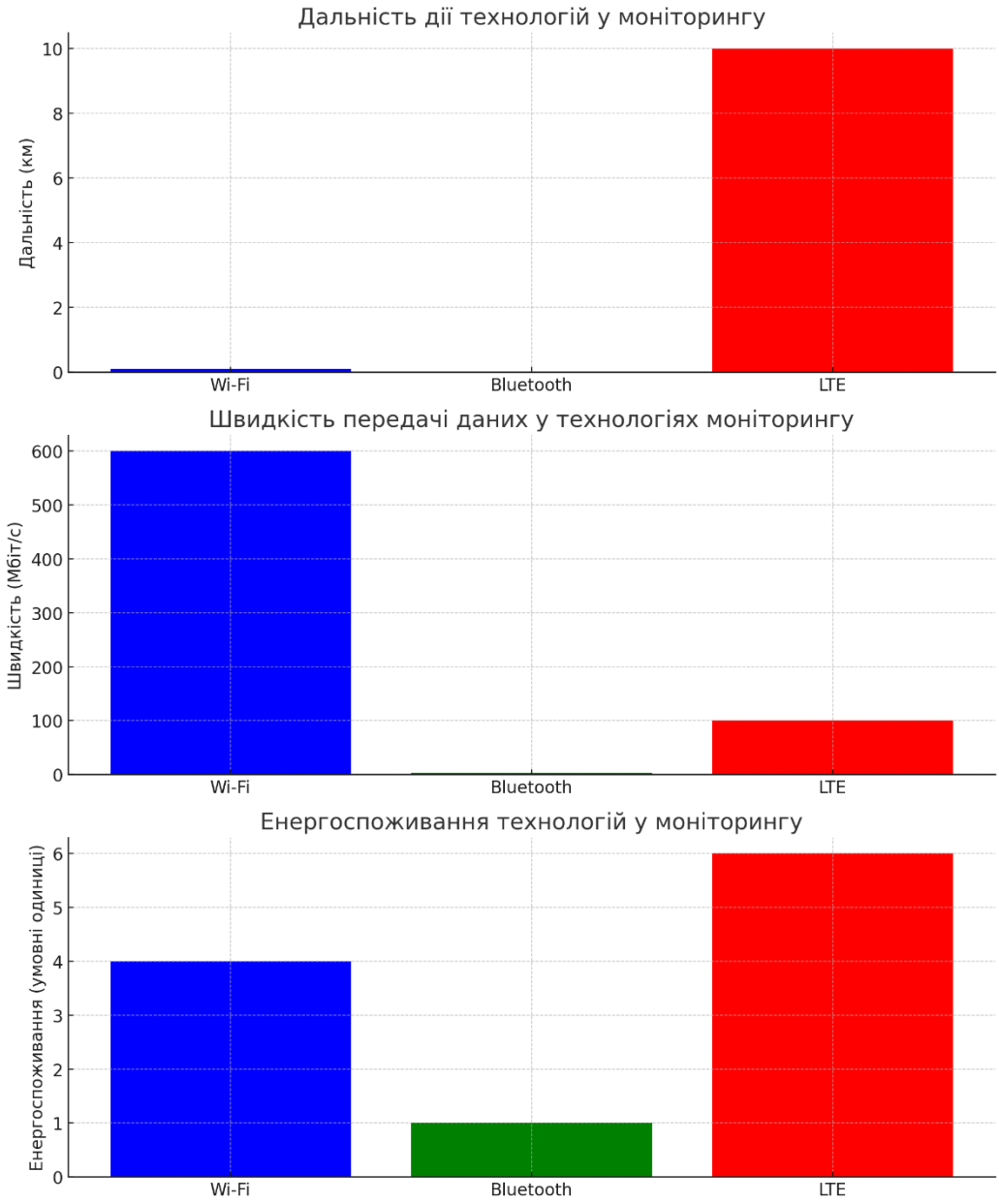


Рис. 1.2. Енергоспоживання технологій у моніторингу

Третій графік демонструє енергетичну ефективність технологій. Bluetooth є найбільш енергоощадним рішенням (1 умовна одиниця), що робить його оптимальним для пристроїв з обмеженими ресурсами живлення, наприклад, сенсорів або носимих пристроїв. Wi-Fi споживає помірну кількість енергії (4 одиниці), тоді як LTE є найбільш енерговитратною технологією (6 одиниць), що обмежує його використання у пристроях з обмеженою автономністю.

Виклики і проблеми використання технологій

- Безпека . Усі три технології потребують надійних заходів безпеки, після чого можуть стати об’єктом атак або бути вразливими до перехоплення даних.
- Сумісність . Деякі пристрої можуть підтримувати тільки Wi-Fi або Bluetooth, що створює проблеми для інтеграції різних пристроїв в єдину систему моніторингу.
- Якість зв'язку . Зовнішні фактори, такі як погода або перешкоди, можуть вплинути на якість з'єднання (особливо для Wi-Fi і LTE), що може негативно відображатися в процесі моніторингу.

Використання Wi-Fi, Bluetooth і LTE у моніторингу дозволяє ефективно відслідковувати процеси, оптимізувати роботу пристроїв і забезпечити стабільний зв'язок. Вибір технологій залежить від конкретних потреб: Bluetooth підходить для локального моніторингу з невеликим споживанням енергії, Wi-Fi забезпечує стабільний зв'язок у середніх масштабах, а LTE – оптимальне рішення для віддаленого моніторингу на великих відстанях.

Вибір технології для моніторингу залежить від поставлених завдань. Wi-Fi є оптимальним для високошвидкісного локального моніторингу. Bluetooth підходить для моніторингу у невеликих приміщеннях та носимих пристроях завдяки низькому енергоспоживанню. LTE є незамінним для моніторингу на великих відстанях, забезпечуючи стійкий зв'язок у віддалених регіонах.

РОЗДІЛ 2. МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ

Для забезпечення високої ефективності моніторингу бездротових мереж і віддалених процесів важливо використовувати різноманітні методи та підходи, які можуть суттєво поліпшити якість збору та аналізу даних. Одним з основних методів є автоматизація процесів моніторингу. Автоматизація збору даних та їхнього аналізу дозволяє зменшити навантаження на адміністративний персонал і підвищити швидкість реакції на інциденти. Використання інструментів автоматизованого моніторингу, таких як Zabbix або Nagios, дозволяє оперативно отримувати інформацію про стан мережі та виявляти аномалії, що значно знижує ризики, пов’язані з людським фактором.

Ще одним важливим аспектом є використання аналітики та технологій штучного інтелекту. AI та машинне навчання можуть допомогти в аналізі великих обсягів даних, виявленні патернів і аномалій у мережевому трафіку. Наприклад, системи, які використовують AI, можуть автоматично виявляти потенційні загрози та реагувати на них, що суттєво підвищує рівень безпеки і зменшує час реагування на інциденти.

Не менш важливим є інтеграція з системами управління інформаційною безпекою (SIEM). Системи SIEM (Security Information and Event Management) дозволяють централізовано збирати, аналізувати та зберігати дані про безпеку мережі. Інтеграція моніторингових рішень із SIEM забезпечує комплексний підхід до управління безпекою, дозволяючи виявляти загрози на ранніх етапах. Це не лише підвищує ефективність моніторингу, а й забезпечує зручний інтерфейс для аналізу даних.

Використання спеціалізованих протоколів також відіграє важливу роль у моніторингу. Протоколи, такі як SNMP (Simple Network Management Protocol), RMON (Remote Monitoring), та NetFlow, забезпечують ефективний моніторинг мережевих пристроїв і трафіку. Ці протоколи дозволяють отримувати детальну

інформацію про стан мережі та її продуктивність, що сприяє своєчасному виявленню проблем і аномалій.

Регулярні перевірки та тестування безпеки є ще одним важливим методом підвищення ефективності моніторингу. Проведення регулярних перевірок безпеки, таких як тестування на проникнення або аудит конфігурацій пристроїв, допомагає виявляти вразливості в системі. Це забезпечує своєчасне реагування на потенційні загрози і підвищує загальний рівень безпеки мережі.

Оптимізація параметрів бездротової мережі також може суттєво підвищити ефективність моніторингу. Налаштування параметрів, таких як канали, потужність сигналу та шифрування, може покращити якість з'єднання та зменшити затримки. Використання сучасних технологій, таких як 802.11ac або 802.11ax (Wi-Fi 6), дозволяє підвищити продуктивність бездротових мереж і зменшити ризики, пов’язані з нестабільним з'єднанням.

Крім того, навчання персоналу є важливим аспектом підвищення ефективності моніторингу. Проведення навчань для працівників щодо основ безпеки інформації та використання моніторингових інструментів дозволяє збільшити їхню обізнаність про можливі загрози і методи реагування. Це, в свою чергу, знижує ризики, пов'язані з людським фактором, і підвищує загальну безпеку системи.

Застосування хмарних технологій також може істотно підвищити ефективність моніторингу. Хмарні платформи для моніторингу забезпечують масштабованість та доступність даних з будь-якої точки, що дозволяє ефективно управляти віддаленими процесами. Хмарні рішення дозволяють зберігати та аналізувати великі обсяги даних, а також забезпечують гнучкість у виборі інструментів моніторингу.

Нарешті, впровадження систем оповіщення та сповіщення є важливим елементом підвищення ефективності моніторингу. Налаштування автоматизованих систем оповіщення, які повідомляють про виявлені проблеми, допомагає своєчасно реагувати на інциденти. Це може бути реалізовано через SMS, електронну пошту або інтеграцію з месенджерами, такими як Telegram.

Таким чином, використання різноманітних методів підвищення ефективності моніторингу дозволяє забезпечити надійність, безпеку та продуктивність бездротових мереж. Інтеграція новітніх технологій, автоматизація процесів, навчання персоналу, а також оптимізація параметрів мережі є ключовими аспектами для досягнення успіху в цій сфері.

Підвищення ефективності моніторингу за допомогою візуалізацій (картинок, графіків, схем тощо) може значно полегшити аналіз інформації. Розглянемо основні методи, які допомагають зробити моніторинг видимо ефективнішим (рис. 2.1).

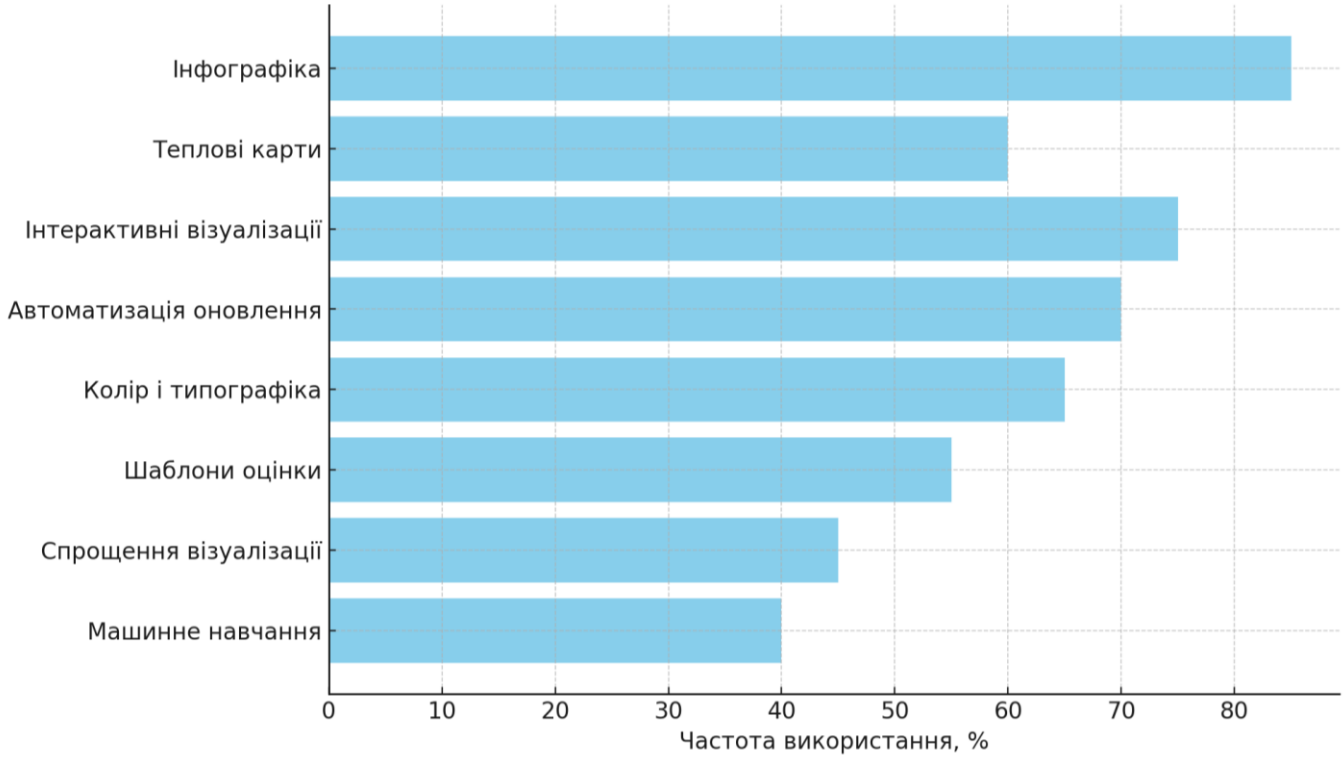


Рис. 2.1. Методи підвищення моніторингу

1. Інфографіка

- Використовуйте інфографіку для зведення великих обсягів даних до зрозумілих видимих форм.
- Створюйте графіки, діаграми, карти, які чітко відображають ключові тренди та закономірності.

2. Теплові карти

- Для географічних даних або великих матриць використовуйте теплові карти, щоб легко визначити область з високою або низькою активністю.

3. Інтерактивні візуалізації

- Інтерактивні елементи, як-от масштабування графіків чи клікабельні деталі, дозволяють користувачам досліджувати дані глибше без перезавантаження інформації.

4. Автоматизація оновлення

- Інтегруйте дані в реальний час, щоб уникнути застарілості. Це особливо корисно для моніторингу змінюваних процесів, як-от економічні показники чи природні явища.

5. Колір і типографіка

- Використовуйте контрастні кольори, щоб виділити ключову інформацію.
- Не перевантажуйте дизайн, дотримуйтесь принципу «менше — краще».

6. Шаблони для швидкої оцінки

- Розробіть стандартизовані шаблони для аналізу різних видів даних (наприклад, окремі графіки для фінансових, соціальних чи екологічних даних).

7. Спрощення візуалізації

- Не перевантажуйте картинки деталями — використовуйте зрозумілі елементи й залишайте лише місце для глядача.

8. Аналіз з використанням машинного навчання

- Використовуйте алгоритми машинного навчання для ідентифікації шаблонів у даних і видачі їх у зручному візуальному форматі.

2.1. Оптимізація збору та обробки даних

Оптимізація збору та обробки даних є завданням для будь-якої компанії, особливо в умовах стрімкого зростання обсягів інформації та необхідності її швидкої обробки. Для досягнення ефективності у зборі та обробці даних

використовуються різноманітні технології та підходи, які дозволяють мінімально збільшити час, ресурси та підвищити точність аналізу. Розглянемо ключові аспекти та методи оптимізації цього процесу (табл. 2.1).

Таблиця 2.1.

Ключові методи оптимізації збору та обробки даних

№	Метод	Основні інструменти та підходи
1	**Вибір джерел даних**	Аналіз релевантності, інтеграція з CRM, ERP-системами
2	**Автоматизація збору даних**	IoT-пристрої, сенсори, API, Webhooks, RPA
3	**Хмарні рішення**	Хмарне зберігання (AWS, Google Cloud), аналітичні платформи
4	**Попередня обробка даних**	Фільтрація, очищення, нормалізація, агрегування
5	**Обробка даних у реальному часі**	Стрімінгові платформи (Apache Kafka, Flink), Edge Computing
6	**Оптимізація сукупних даних**	Формати (Parquet, ORC), інтеграція сховищ, кешування
7	**Штучний інтелект і машинне навчання**	Аналітика, прогностичні моделі, автоматичне виявлення аномалій
8	**Оптимізація витрат і ресурсів**	Масштабування ресурсів, автоматизоване управління ресурсами

1. Вибір підходящих джерел даних

- Аналіз релевантності . Важливо застосувати, які є дійсно необхідними для аналізу, щоб уникнути зберігання зайвої інформації та оптимізувати обсяг зібраних даних.
- Інтеграція з ключовими джерелами . Підключення до надійних джерел даних, таких як CRM, ERP-системи або інші корпоративні бази даних, дозволяє отримувати релевантну інформацію без дублювання та з мінімальними підтримками.

2. Автоматизація процесу збору даних

- Використання IoT-пристроїв і сенсорів . Для автоматизованого збору даних із фізичних об’єктів часто використовувалися датчики та пристрої Інтернету речей (IoT), які можна зібрати інформацію в реальному часі.

- API та веб-хуки . Взаємодія із зовнішніми системами через API та Webhooks автоматизує збір даних і дозволяє об'єднувати різні платформи в єдину систему.
- Впровадження RPA (роботизованої автоматизації процесів) . RPA-технології не дозволяють автоматизувати ручні процеси збору даних, наприклад, копіювання інформації між всіма системами, що прискорює процес і знижує ймовірність помилок.

3. Застосування хмарних рішень

- Хмарне зберігання і обробка . Зберігання даних у хмарних сховищах (наприклад, Amazon AWS, Google Cloud, Microsoft Azure) дозволяє забезпечити швидкий доступ до інформації та масштабувати ресурси залежно від потреби.
- Хмарні аналітичні платформи . Використання хмарних рішень для аналітики дозволяє обробляти великі обсяги даних у реальному часі без потреби в локальній інфраструктурі, що особливо важливо для аналізу даних з великою варіативністю (Big Data).

4. Попередня обробка даних

- Фільтрація і очищення . Видалення дубльованих, неповних або помилкових записів ще на етапі збору хоче зменшити обсяг і підвищити якість інформації для подальшої аналітики.
- Нормалізація і структурізація . Приведення даних до єдиного формату та їх структурація значно покращує їх обробку та забезпечує коректність аналізу.
- Агрегація даних . Замість зберігання первинних, детальних записів можна агрегувати інформацію (наприклад, звести до середніх значень чи загальних підсумків), що зменшує обсяг і прискорює доступ до важливих показників.

5. Використання технологій для обробки даних у реальному часі

- Стрімінгові платформи . Використання Apache Kafka, Apache Flink або інших стрімінгових платформ дозволяє обробляти потоки даних у реальному часі, що є кількість для швидкого реагування та моніторингу.

- Edge Computing (периферійні обчислення) . Обробка даних на пристроях ближче до джерела, а не в центрі, зменшує затримку та зменшує навантаження на основні обчислювальні ресурси.

6. Оптимізація сукупних даних

- Вибір відповідного формату даних . Використання легких форматів зберігання, таких як Parquet або ORC, які оптимізовані для зберігання великих обсягів інформації з мінімальними вимогами до дискового простору.
- Інтеграція загальних даних . Інтеграція різних баз даних і сховищ (озер даних, сховищ даних) дозволяє оптимізувати обробку і доступ до даних в одній інфраструктурі.
- Кешування . Застосування кешування даних прискорює доступ до часто використовуваної інформації, зменшуючи потребу в повторних запитах до бази.

7. Використання алгоритмів штучного інтелекту і машинного навчання

- Аналітика і прогностичні моделі . Штучний інтелект дозволяє автоматизувати процес аналізу великих обсягів даних і дозволяє прогнозувати поведінку, тенденції або ризики на основі історичних даних.
- Автоматичне виявлення аномалій . Машинне навчання дозволяє виявляти аномальні дані або непередбачені події в реальному часі, що покращує безпеку і дозволяє швидко реагувати на зміни.

8. Оптимізація витрат і ресурсів

- Масштабування ресурсів . Динамічне масштабування серверів і сховищ залежно від обсягу даних дозволяє економити ресурси, використовуючи їх тільки тоді, коли це необхідно.
- Автоматизоване управління ресурсами . Використання інструментів для управління ресурсами та витратами в хмарі дозволяє ефективно розподіляти навантаження та оптимізувати витрати на обробку великих обсягів даних.

Унаочнення оптимізації збору та обробки даних зображено на рисунку 2.2.

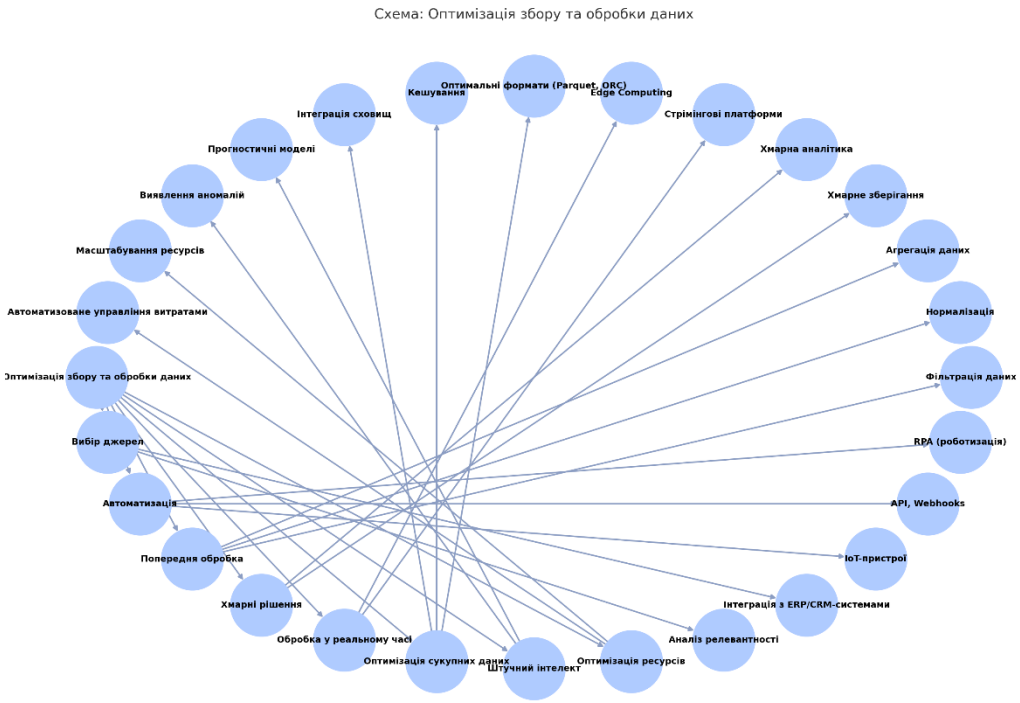


Рис. 2.2. Оптимізація збору та обробки даних

Оптимізація збору та обробки даних забезпечує комплексний підхід, який охоплює автоматизацію процесів, використання хмарних рішень, передові методи обробки та структурування даних. Інтеграція сучасних інструментів для аналізу та алгоритмів штучного інтелекту дозволяє компаніям не лише збирати дані, але й оперативно отримувати корисну інформацію для прийняття бізнес-рішень**.**

2.2. Використання протоколів SNMP для моніторингу

Протокол SNMP (Simple Network Management Protocol) є одним із найрозширеніших протоколів для моніторингу мережевих пристроїв та управління ними. Він дозволяє адміністраторам мережі отримати інформацію про стан пристроїв, як маршрутизатори, комутатори, сервери, принтери та інші пристрої, підключені до мережі. SNMP забезпечує централізований підхід до моніторингу, що дозволяє швидко виявляти й вирішувати проблеми, підвищуючи надійність і стабільність мережі.

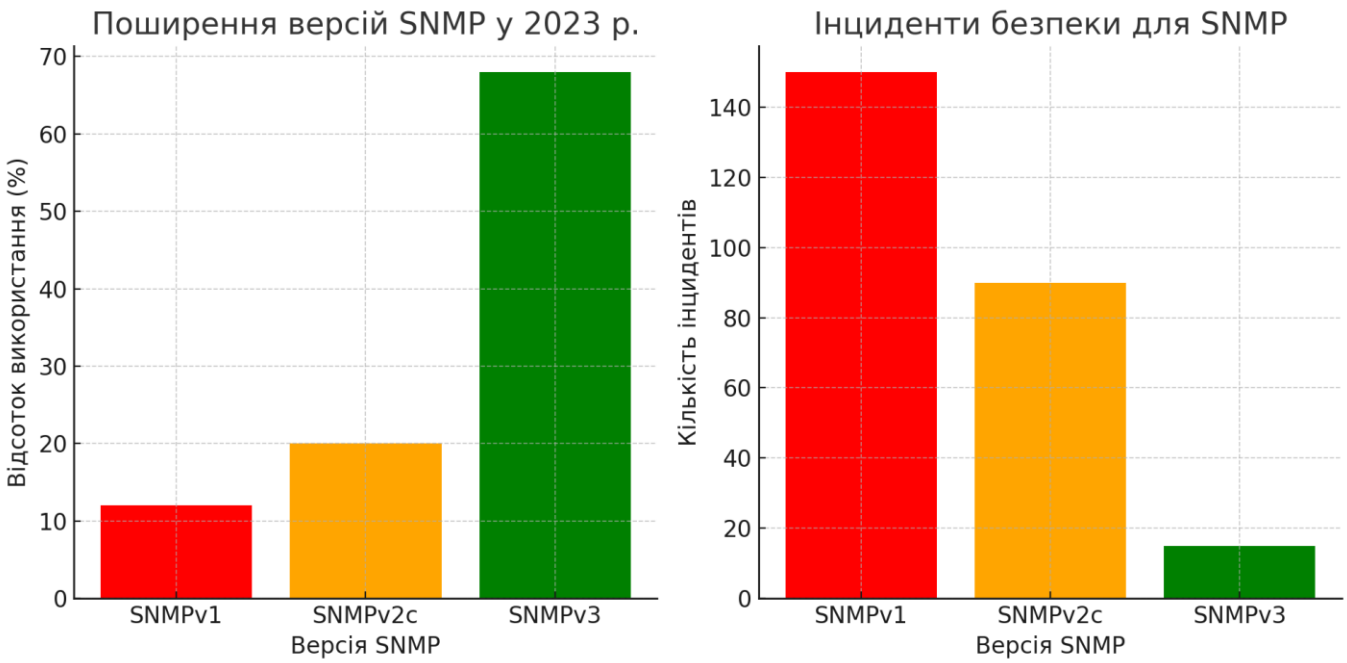


Рис. 2.2. Використання протоколів SNMP для моніторингу

Перший графік нам демонструє поширення версій SNMP у 2023 році:

1. SNMPv3 займає лідируючу позицію з 68% використання завдяки надійній безпеці та можливості шифрування.

2. Старі версії SNMPv1 та SNMPv2c мають значно нижчу популярність (12% та 20%) через слабкий захист.

На другому графіку відображено інциденти безпеки:

1. SNMPv1 має найвищу кількість інцидентів (150 випадків) через відсутність шифрування.

2. SNMPv2c показує помірне зменшення інцидентів завдяки покращеній продуктивності, але безпеки все ще бракує.

3. SNMPv3 демонструє найнижчий рівень інцидентів (15 випадків), що підтверджує його надійність та важливість переходу на цю версію для забезпечення безпеки мережі.

Ці дані демонструють, що використання SNMPv3 є ключовим для ефективного та безпечного моніторингу мережевих ресурсів.

Тож, варто розглянути основи роботи SNMP.

SNMP працює за принципом "клієнт-сервер" і має три основні компоненти:

1. Менеджер SNMP – центральний пристрій або сервер, який отримує і аналізує дані від підключених пристроїв.

2. Агент SNMP – програмне забезпечення, що встановлюється на кожен мережевий пристрій і збирає дані про його роботу.

3. База інформації управління (MIB) – структура даних, яка зберігає інформацію про характеристики та параметри пристроїв і доступна для запитів.

Ключові функції SNMP

SNMP дозволяє виконати кілька основних операцій:

- GET – отримання інформації про параметри пристрою.
- SET – зміна значення параметрів пристрою.
- GETNEXT і GETBULK – отримання серії параметрів для оптимізації збору інформації.
- TRAP – повідомлення про події. Агент надсилає повідомлення менеджеру, коли виконується певна подія (наприклад, відключення або перезавантаження пристрою).

Використання SNMP для моніторингу

1. Моніторинг продуктивності мережі

- SNMP дозволяє збирати інформацію про швидкість передачі даних, завантаження процесора та використання пам'яті на кожному пристрої, що дозволяє відстежувати продуктивність мережі в реальному часі.
- Наприклад, системи моніторингу на основі SNMP, такі як Nagios , Zabbix або PRTG Network Monitor , задають дані SNMP для створення графіків завантаження та розміщення "вузьких місць" у мережі.

2. Відстеження стану пристроїв

- SNMP допомагає виявляти відмови та відключення пристроїв. Наприклад, якщо комутатор або маршрутизатор перестає відповідати, SNMP-менеджер може отримати TRAP-повідомлення про несправність і передати його адміністратору.
- таке сповіщення може надсилатися автоматично, що дозволяє швидко реагувати на проблеми без потреби в постійному ручному моніторингу.

3. Аналіз і прогнозування трафіку

- SNMP дозволяє збирати статистику мережевого трафіку, що є корисним для аналізу патернів використання мережі. Це може допомогти оптимізувати ресурси та запобігти перевантаженням.
- Наприклад, за допомогою SNMP можна прогнозувати завантаження піків і швидко розширювати мережеві ресурси.

4. Виявлення аномалій і підвищення безпеки

- SNMP-менеджер може виявити незвичайну активність, наприклад, різке підвищення завантаження або появу нових пристроїв у мережі, що може свідчити про якусь загрозу.
- За допомогою SNMP також можна контролювати активність портів на мережевих пристроях, які потім виявляють недоліки підключення або включення.

Переваги використання SNMP

- Централізований контроль . SNMP дозволяє об'єднувати моніторинг і управління всіма мережевими пристроями в одному інтерфейсі.
- Масштабованість . Протокол підтримує моніторинг як невеликих мереж, так і великих корпоративних інфраструктур.
- Автоматизація повідомляєлень . SNMP TRAP-сповіщення не допускає автоматичного порушення змін у стані мережевих пристроїв.

Недоліки SNMP і виклики

- Безпека . Стандартний SNMP версій 1 і 2 передає дані в незашифрованому вигляді, що створює ризики для безпеки, особливо у відкритих або незахищених мережах. Версія SNMPv3 підтримує шифрування, але її впровадження вимагає додаткових налаштувань.
- Нестача гнучкості . SNMP може не забезпечити потрібну деталізацію даних або інтеграцію з новими системами моніторингу.
- Труднощі з настройками . Для ефективної роботи SNMP потрібно налаштувати як менеджера, так і агентів, а також розуміти структуру MIB для правильної обробки даних.

Найкращі практики використання SNMP для моніторингу

1. Використання SNMPv3 . Для захисту даних і аутентифікації пристроїв бажано використовувати SNMPv3, який підтримує шифрування і підвищену безпеку.

2. Налаштування порогових значень . Встановлення порогових значень (порогів) для різних параметрів (наприклад, завантаження процесора) дозволяє автоматично надсилати сповіщення при перевищенні критичних значень.

3. Регулярне оновлення MIB . Оновлення MIB-файлів забезпечує доступ до нових параметрів і функцій пристроїв, що покращує якість моніторингу.

4. Інтеграція з іншими системами . Використання SNMP у поєднанні з іншими інструментами моніторингу та аналізу даних забезпечує комплексний підхід до управління мережею.

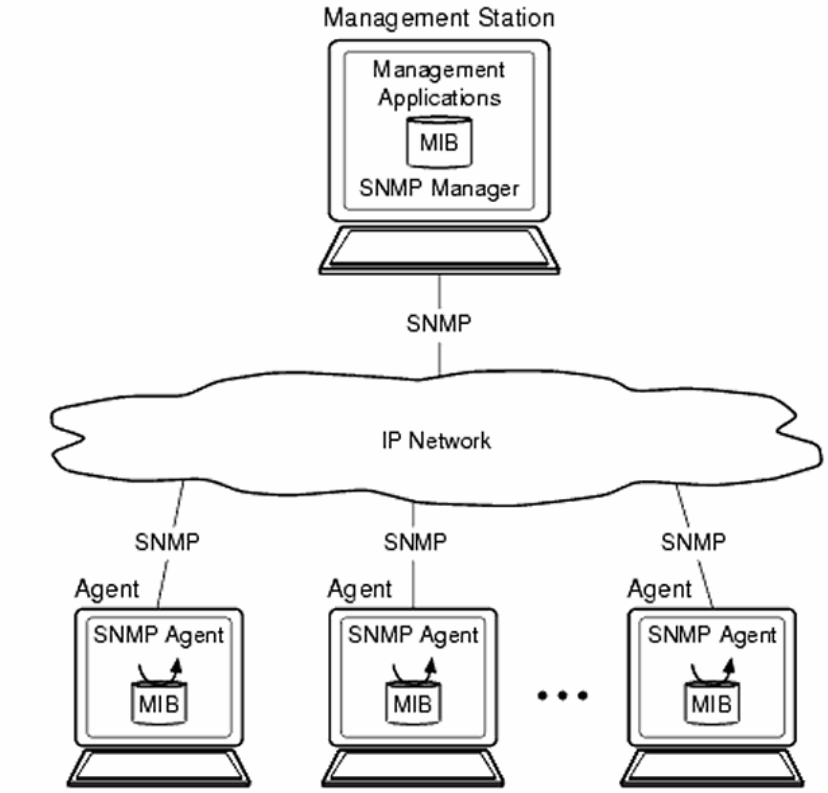


Рис. 2.3. Використання SNMP для моніторингу

SNMP є потужним і зручним протоколом для моніторингу мережі, який дає можливість централізовано контролювати стан і продуктивність пристроїв, а також швидко реагувати на проблеми. Використання SNMP дозволяє зменшити

кількість простих і оптимізувати роботу мережевих ресурсів. Проте важливо слідувати заходам безпеки і налаштування для забезпечення захищеного й ефективного моніторингу.

2.3. Інтеграція хмарних технологій для обробки великих обсягів даних

Інтеграція хмарних технологій є кроком у забезпеченні ефективної обробки великих обсягів даних (Big Data), крім того, вона дозволяє компаніям швидко і масштабовано збирати, зберігати, обробляти й аналізувати дані. Хмарні рішення пропонують гнучкість, високу доступність і потужні ресурси для обробки даних, які можуть бути економічно невигідними при використанні локальної інфраструктури. Розглянемо ключові аспекти використання хмарних технологій для Big Data (табл. 2.2).

Таблиця 2.2.

Ключові аспекти використання хмарних технологій для Big Data

Категорія	Опис	Інструменти/Рішення
Переваги хмарних технологій	Масштабованість, зниження витрат, доступність, інтеграція інструментів	Amazon AWS, Google Cloud Platform, Microsoft Azure
Хмарні платформи	Надають послуги для зберігання, обробки та аналітики великих даних	Amazon S3, Google BigQuery, Azure Synapse Analytics
Процес інтеграції Big Data	Міграція даних, налаштування сховищ, автоматизація процесів	Apache Airflow, Amazon Snowball, Data Lake
Обробка потоків даних	Обробка в реальному часі для моніторингу та аналітики	Apache Kafka, Amazon Kinesis, Edge Computing
Машинне навчання та аналітика	Впровадження ML/AI для прогнозування, аналізу трендів та автоматичного виявлення аномалій	Amazon SageMaker, Google AI Platform, Azure ML
Безпека даних	Шифрування, контроль доступу, резервне копіювання	Керування доступом, резервне копіювання на хмарних платформах
Оптимізація витрат	Масштабування ресурсів на вимогу, контроль споживання ресурсів	Моніторинг витрат на AWS Cost Explorer, Google Cloud Billing

1. Переваги хмарних технологій для Big Data

- Масштабованість . Хмарні провайдери не можуть динамічно масштабувати ресурси (сервери, сховища, потужність збільшення) відповідно до

потреб. Це особливо важливо для аналізу великих обсягів даних, коли завантаження може швидко змінюватися.

- Зниження витрат . Оплата за використані ресурси дозволяє оптимізувати витрати. Компанії не потрібно інвестувати в потужне обладнання, а також у технічну підтримку локальних серверів.
- Доступність і мобільність . Дані можна обробляти з будь-якого місця, що робить хмарні технології особливо корисними для команд, які працюють віддалено.
- Інтеграція інструментів . Більшість хмарних провайдерів (Amazon Web Services, Google Cloud, Microsoft Azure) пропонують повний набір інструментів для роботи з Big Data, включаючи інструменти для обробки потоків даних, аналізу та машинного навчання.

2. Основні хмарні платформи для обробки Big Data

- Веб-сервіси Amazon (AWS) . AWS пропонує широкий вибір послуг для великих даних, таких як Amazon S3 для зберігання даних, Amazon EMR для обробки великих обсягів даних на основі Hadoop і Spark, а також Amazon Redshift для аналітичних баз даних.
- Google Cloud Platform (GCP) . GCP надає потужні інструменти для обробки даних, такі як BigQuery (високошвидкісна аналітична база даних), Google Dataflow для обробки потоків даних і Google Dataproc для кластерів Hadoop та Spark.
- Microsoft Azure . Azure також має великий вибір сервісів, таких як Azure Data Lake для збору даних, Azure Synapse Analytics для аналізу великих обсягів інформації та Azure Machine Learning для побудови моделей машинного навчання.

3. Процес інтеграції Big Data в хмару

- Міграція даних . Перший етап включає перенесення даних з локальної інфраструктури в хмару. Для цього можна використовувати інструменти експорту-експорту даних або навіть фізичні рішення, такі як Amazon Snowball, для перенесення великих обсягів інформації.

- Налаштування сховищ . Після перенесення даних їх необхідно організувати в сховищах даних, наприклад, в Data Lake або Data Warehouse. Це дозволяє зберегти як структуровані, так і неструктуровані дані для подальшого аналізу.
- Організація обчислювальних ресурсів . На етапі обробки даних розглядаються кластери, наприклад, для Hadoop або Spark, щоб забезпечити високу продуктивність і швидкість обчислення.
- Автоматизація процесів обробки . За допомогою оркестрових інструментів, таких як Apache Airflow або інструментів від хмарних провайдерів, можна автоматизувати обробку даних і запуск аналітичних моделей.

4. Обробка потоків даних у реальному часі

- Apache Kafka та Amazon Kinesis . Для обробки потокових даних у хмарі використовуються такі інструменти, як Apache Kafka або Amazon Kinesis, які забезпечують обробку великих обсягів даних у реальному часі, що особливо корисно для моніторингу, аналітики та виявлення аномалій.
- Периферійні обчислення (Edge Computing) . Обробка частини даних на периферії дозволяє зменшити обсяги даних, які надходять до хмари, зменшуючи затримки. Це підходить для IoT-пристроїв, які збирають дані в реальному часі.

5. Аналітика і машинне навчання на базі хмарних технологій

- Машинне навчання (ML) та штучний інтелект (AI) . Хмарні платформи пропонують інструменти для будівництва та навчання моделей машинного навчання на великих масивах даних (наприклад, Amazon SageMaker, Google AI Platform, Azure Machine Learning).
- Аналітика та прогнозування . Дані, зібрані у великих обсягах, можна використовувати для аналізу трендів, поведінкових моделей і прогнозування. Це забезпечується аналітичними інструментами BigQuery, Amazon Redshift або Azure Synapse.

6. Безпека та управління даними

- Контроль доступу . Використання розширених механізмів аутентифікації та авторизації дозволяє обмежувати доступ до даних, забезпечуючи конфіденційність.
- Шифрування . Дані можна шифрувати як при зберіганні, так і під час передачі, що забезпечує захист від несанкціонованого доступу.
- Резервне копіювання та відновлення . Хмарні провайдери зазвичай пропонують інструменти для резервного копіювання, що важливо для відновлення даних у випадках помилок або збоїв.

7. Оптимізація витрат у хмарі

- Масштабування на вимогу . Хмарні ресурси можна динамічно масштабувати, підвищуючи обсяги зберігання та переробляючи під поточні потреби, що дозволяє зменшити витрати.
- Керування витратами . Інструменти управління витратами допомагають оптимізувати використання ресурсів і уникати зайвих витрат. Багато платформ пропонує можливості моніторингу споживання ресурсів і прогнозування витрат.

Інтеграція хмарних технологій для обробки великих обсягів даних дозволяє компаніям отримати максимальне мінімальне використання Big Data, мізуючи витрати на інфраструктуру та зменшуючи можливості гнучкової та масштабованої обробки даних. Хмарні рішення також спрощують впровадження інновацій, як-от машинне навчання та реальний час, створюючи процес аналізу більш точним і ефективним.

2.4. Використання систем штучного інтелекту для аналізу даних моніторингу

Системи штучного інтелекту (ШІ) надають широкі можливості для аналізу даних моніторингу, допомагаючи автоматизувати процеси, підвищувати точність прогнозів і виявляти приховані закономірності. Використання ШІ в аналізі даних моніторингу дозволяє оптимізувати продуктивність, знизити витрати та покращити реакцію на критичні ситуації.

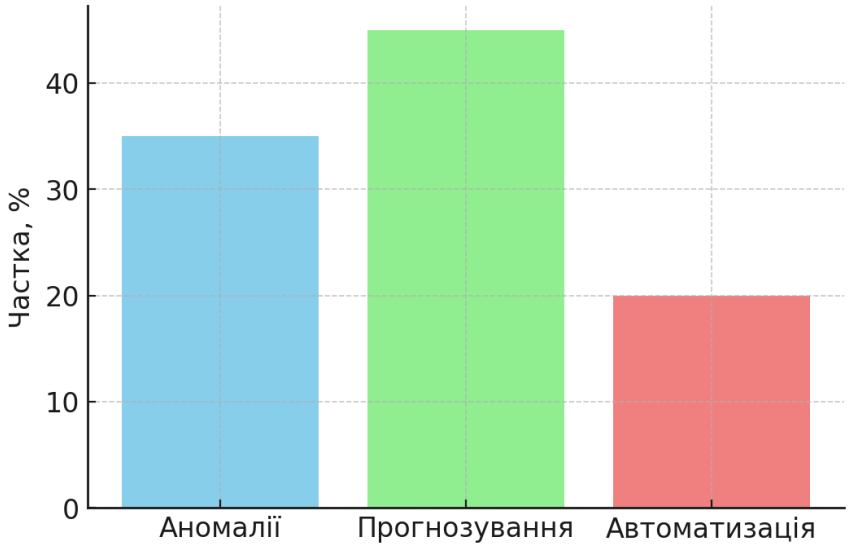


Рис. 2.4. Розподіл використання ШІ для аналізу даних моніторингу

На рисунку 2.4 відображено основні напрями застосування штучного інтелекту в системах моніторингу:

1. Виявлення аномалій займає 35%, оскільки ШІ здатний автоматично виявляти невідповідності та аномальні ситуації у великих наборах даних.

2. Прогнозування охоплює найбільшу частку 45% завдяки здатності моделей машинного навчання будувати прогностичні моделі для попередження збоїв чи відхилень.

3. Автоматизація процесів аналітики складає 20%, спрощуючи регулярну обробку та інтерпретацію даних.

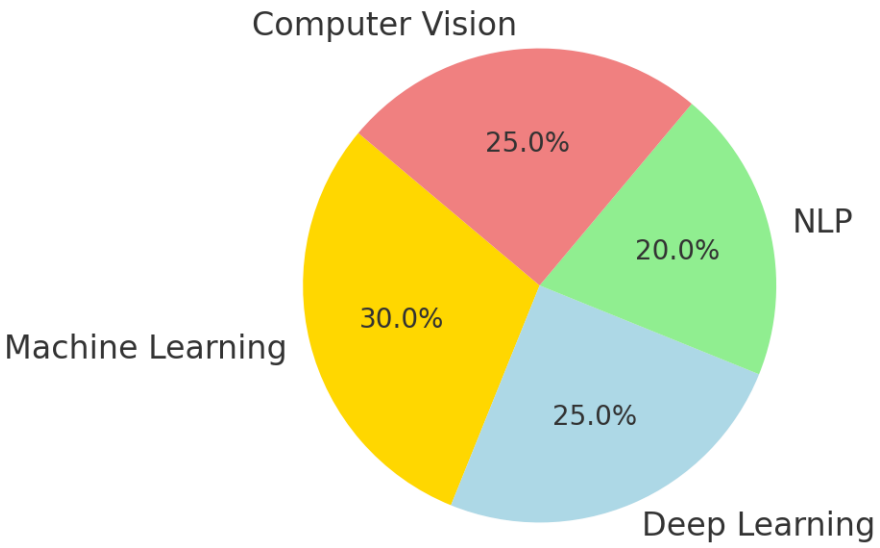


Рис. 2.5. Інструменти ШІ для аналізу даних моніторингу

Діаграма (рис. 2.5) демонструє ключові інструменти, які використовуються в системах моніторингу:

1. Machine Learning (30%) – основний метод для навчання моделей аналізу даних.

2. Deep Learning (25%) – використовується для складних завдань, таких як обробка відео чи зображень.

3. Natural Language Processing (20%) – ефективно працює для текстової аналітики у звітах моніторингу.

4. Computer Vision (25%) – застосовується для візуального аналізу, наприклад, у відеоспостереженні.

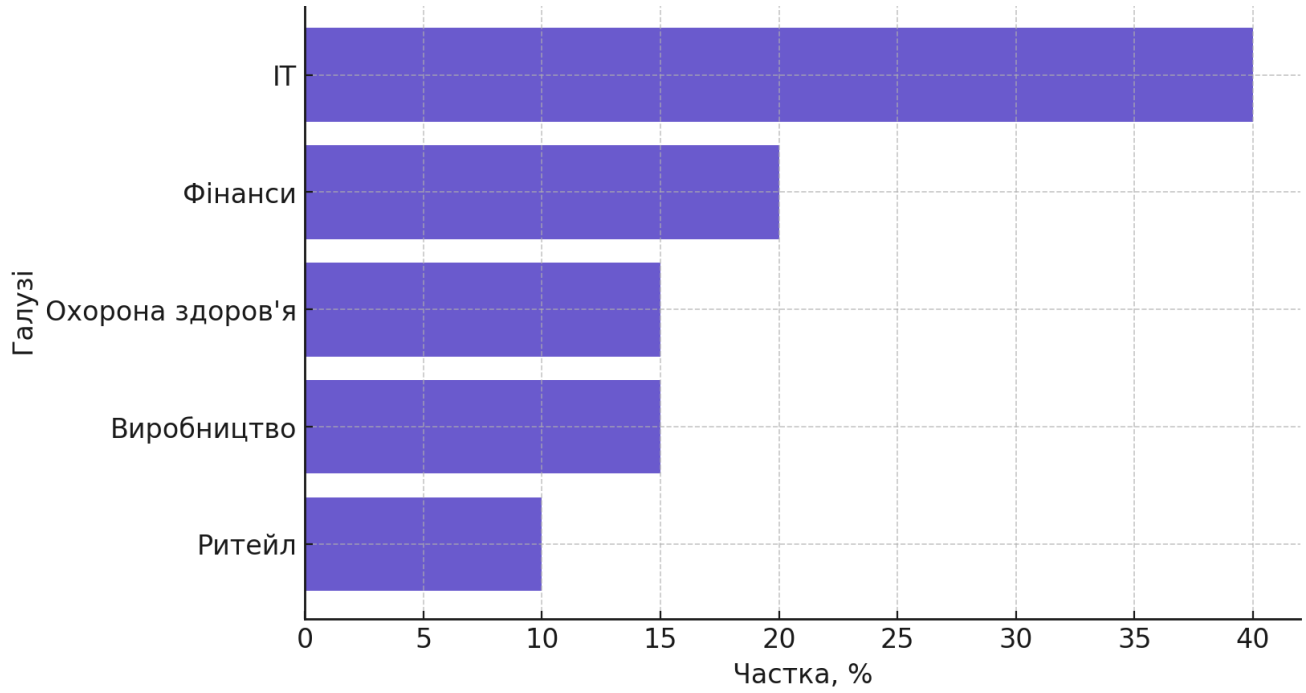


Рис. 2.6. Використання ШІ в аналізі даних за галузями

Графік на рисунку 2.6 відображає розподіл впровадження ШІ для моніторингу за секторами економіки:

1. IT-сектор є лідером із 40% через потребу у відстеженні роботи систем та кібербезпеці.

2. Фінансові установи застосовують ШІ у 20% випадків для моніторингу транзакцій і виявлення шахрайства.

3. Охорона здоров'я та Виробництво по 15% використовують ШІ для моніторингу медичних даних і виробничих процесів.

4. Ритейл – 10%, де ШІ аналізує поведінку клієнтів та управління логістикою.

Таке застосування підкреслює значну роль штучного інтелекту у сучасних моніторингових системах для різних галузей

Розглянемо основні аспекти використання ШІ в цій сфері.

1. Аналіз великих обсягів даних

- Big Data і машинне навчання . Дані моніторингу часто накопичуються в дуже великих обсягах (лог-файли, дані з сенсорів, метрики продуктивності), що

ускладнює їх ручний аналіз. Системи штучного інтелекту здатні швидко аналізувати масиви даних, виявляючи значущі закономірності та аномалії.

- Зниження впливу "шуму" . ШІ-системи можуть фільтрувати незначні або неважливі дані, зосереджуючи увагу лише на критично важливих показниках. Це забезпечує точність аналізу і зменшує витрати на обробку даних.

2. Прогнозування і превентивний аналіз

- Прогнозування збоїв . За допомогою алгоритмів машинного навчання ШІ можна прогнозувати можливості збої або аварії, наприклад, на основі історичних даних про роботу обладнання або сервісів. Це запобігає простоям і зменшує витрати на ремонт.
- Превентивне обслуговування . На основі аналізу показників, таких як температура, вібрація, навантаження, можна автоматично визначити час для обслуговування обладнання до виникнення проблеми. Це ефективність експлуатації та знижує ризик несподіваних поломок.

3. Виявлення аномалій і підвищення безпеки

- Автоматичне виявлення аномалій . Алгоритми ШІ можуть виявити аномальні відхилення від нормальних показників, такі як різке підвищення навантаження на сервер або незвичайну активність у мережі, що може свідчити про можливу атаку.
- Виявлення кіберзагроз . Системи ШІ аналізують активність у реальному часі і можуть виявляти враження поведінки, виявляючи якісь загрози, як-от несанкціонований доступ або спроби зламати мережу. Це важливо для захисту конфіденційної інформації та критичної інфраструктури.

4. Аналіз поведінки користувачів і мережевого трафіку

- Вивчення батьківської поведінки . ШІ дозволяє аналізувати поведінку користувачів у мережі (кількість відвідувань, типи дій, час активності), щоб виявити незвичайну активність. Це може бути корисним для оптимізації ресурсів або для забезпечення безпеки.
- Оптимізація трафіку і завантаження . Аналіз потоків мережевого трафіку дозволяє передбачити піктограми завантаження та відповідно

перерозподілити ресурси. Це зменшує затримки, оптимізує пропускну здатність мережі та покращує загальну продуктивність.

5. Автоматизоване прийняття рішень і самонавчання

- Системи, що самонавчаються . Сучасні ШІ-системи здатні постійно вдосконалюватися, використовуючи нові дані з моніторингу. Це дозволяє їм коригувати моделі поведінки, підвищуючи точність прогнозів та адаптуючись до нових умов.
- Автоматизоване прийняття рішень . Використання ШІ дозволяє автоматизувати реакцію на події. Наприклад, система може автоматично вимічати проблемне обладнання або сповіщати технічну підтримку при отриманні аномалій [30].

6. Обробка даних у реальному часі

- Стрімінг-аналітика . ШІ здатний обробляти дані з моніторингу в реальному часі, що особливо корисно для завдань, де потрібна миттєва реакція, наприклад, у фінансовому секторі або системах безпеки.
- Зменшення затримок у рішенні . Завдяки обробці в реальному часі ШІ може миттєво реагувати на критичні ситуації, що дозволяє скоротити час реагування та підвищити ефективність роботи в усій системі [29].

7. Візуалізація та аналітичні звіти

- Інтерактивна візуалізація . Інструменти ШІ можна створити візуалізацію складних показників і змін у фігурах і діаграмах. Це пропонує аналіз для менеджерів та IT-спеціалістів, які можуть швидко оцінити термін.
- Автоматичне створення звітів . ШІ може формувати регулярні звіти про стан мережі, продуктивність обладнання або поведінку користувачів, що дозволяє керівництву оперативно приймати рішення на основі достовірних даних [9].

8. Використання мовного аналізу і НЛП

- Аналіз текстових даних . Системи ШІ з використанням обробки природної мови (NLP) здатні обробляти текстові дані з подій журналів, переглядів

користувачів або документів. Це кожен виявити тенденції, настрої користувачів і визначити причини виникнення проблеми.

- Чат-боти для підтримки . Використання ШІ-чат-ботів дозволяє автоматизувати підтримку, обробку запитів від користувачів та аналізувати частину запитів для покращення роботи сервісу.

Виклики у впровадженні ШІ для аналізу даних моніторингу

- Конфіденційність і безпека . Використання ШІ для аналізу великих обсягів даних може привести до ризиків витоку конфіденційної інформації, тому необхідно забезпечити захист даних і дотримуватись вимог конфіденційності.
- Якість даних . Для ефективної роботи ШІ-системи потрібні точні та якісні дані. Наявність помилок або неповних даних може знизити ефективність прогнозів і виявлення аномалій.
- Високі вимоги до обчислювальних ресурсів . Обробка великих обсягів даних з використанням ШІ потребує значних ресурсів, які можуть бути дорогими, особливо для малих компаній [4].

Використання системи штучного інтелекту для аналізу даних моніторингу дозволяє автоматизувати процеси, виявляти приховані закономірності та швидко реагувати на зміни. Завдяки компаніям ШІ можна підвищити ефективність, покращити безпеку та забезпечити надійну роботу інфраструктури. Протест для успішного впровадження ШІ повинен викликати виклики, такі як якість даних та конфіденційність, і налаштувати обробку даних відповідно до специфіки організації.

РОЗДІЛ 3. РОЗРОБКА ТА ВПРОВАДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ

У процесі розробки та впровадження системи моніторингу бездротових мереж важливо врахувати архітектуру системи, вибір програмного забезпечення для аналізу та зберігання даних, реалізацію механізмів попередження та оповіщення про інциденти, а також тестування та оцінку ефективності системи. Це допоможе створити комплексне рішення, яке забезпечить надійний моніторинг і контроль за станом мережі.

3.1. Архітектура системи моніторингу

Варто розглянути основні елементи архітектури системи моніторингу (рис 3.1).

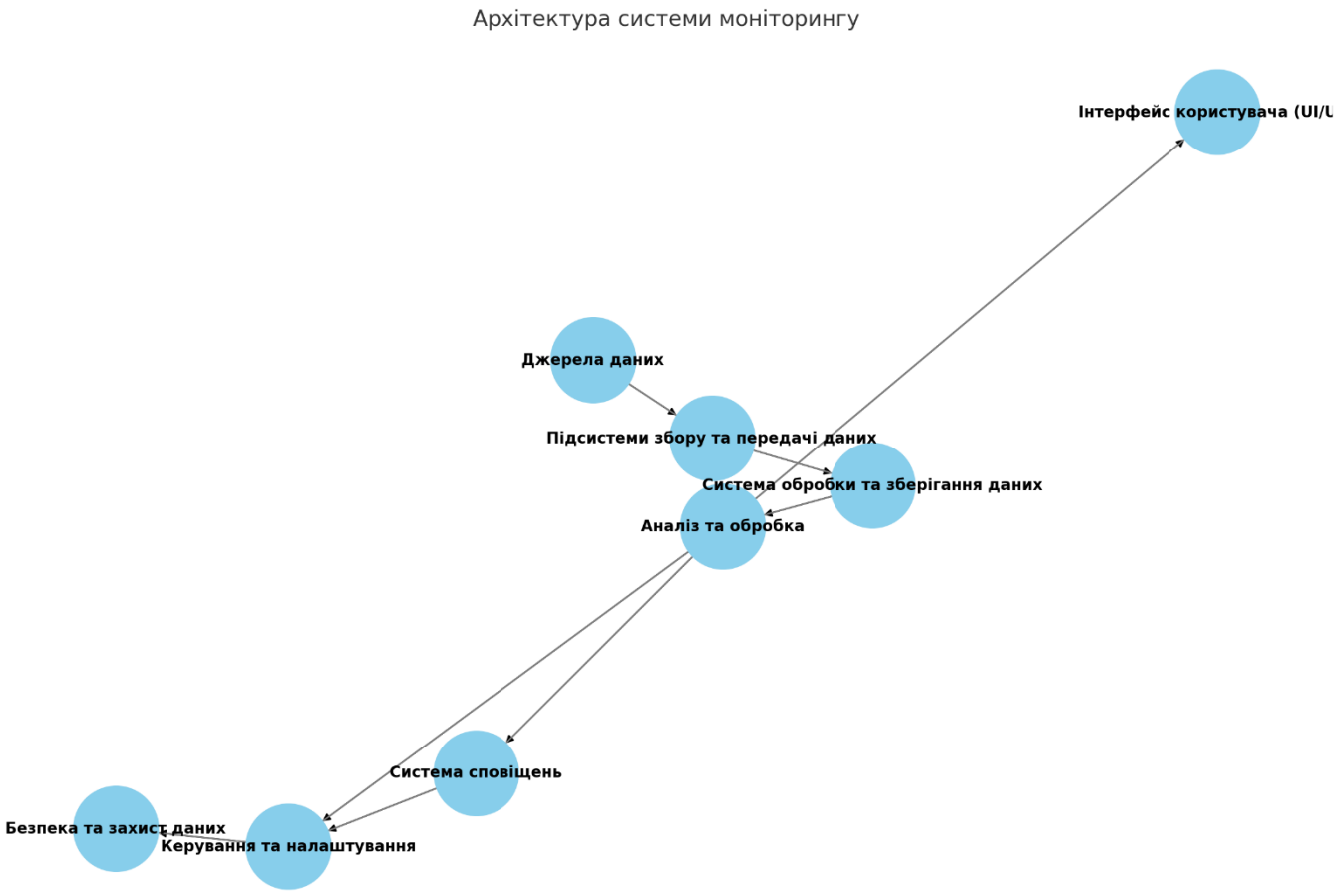


Рис. 3.1. Архітектура системи моніторингу

1. Джерела даних (сенсори, пристрої):

- Ці компоненти займаються збором даних із фізичних чи віртуальних об'єктів. Наприклад, це можуть бути температурні датчики, датчики вологості, камери відеоспостереження або програмні модулі для моніторингу серверів.

2. Підсистеми збору та передачі даних:

- Вони відмовляються від передачі даних із пристроїв на сервери для подальшої обробки. Це можуть бути локальні збори даних за допомогою мережі або віддалене підключення через Інтернет або спеціалізовані протоколи (наприклад, MQTT, SNMP, Modbus).

3. Система обробки та зберігання даних:

- Тут виконується аналіз і обробка даних, що дозволяє створити зведену інформацію, виконати фільтр або обчислення певних показників. Дані можуть зберігатися в базах даних (SQL або NoSQL), на серверах, у хмарних системах.

4. Аналіз та обробка:

- Після того як дані зібрані і збережені, вони повинні бути оброблені для видалення корисної інформації. Це може бути автоматичний аналіз для аномалій, трендів або подій. Інструменти машинного навчання або статистичні моделі можуть бути використані для прогнозування та прийняття рішень.

5. Інтерфейс користувача (UI/UX):

- Система моніторингу має надавати зрозумілий інтерфейс для користувачів, які мають доступ до результатів моніторингу. Це можуть бути таблички, графіки, сповіщення про події та інші дані візуалізації.

6. Система сповіщень:

- Важливим елементом є система оповіщення, яка інформує користувачів про важливі події чи аномалії, що потребують уваги. Сповіщення може бути надіслано через електронну пошту, SMS, push-сповіщення або інші канали.

7. Керування та налаштування:

- Для адміністратора системи важливо мати можливість налаштувати моніторинг, налаштувати порогові значення для сповіщення, керувати доступом до даних, оновити програмне забезпечення та забезпечити безпеку системи.

8. Безпека та захист даних:

- Система моніторингу повинна забезпечувати конфіденційність і цільність даних. Це включає в себе шифрування, аутентифікацію, авторизацію та інші засоби захисту від несанкціонованого доступу або модифікації даних.

Типи системи моніторингу:

- Фізичні системи моніторингу: наприклад, для моніторингу температури, вологості, рівня забруднення повітря.
- IT-системи моніторингу: Для моніторингу серверів, мережевих пристроїв, баз даних та ін.
- Програмні системи моніторингу: Для моніторингу додатків та сервісів, як для веб-сайтів, мобільних додатків чи пристроїв IoT.

Архітектурні моделі:

1. Централізована архітектура: усі дані з різних джерел передаються на центральний сервер, де вони обробляються та зберігаються.
2. Розподілена архітектура: Дані збираються і обробляються на місцях (на пристроях або в локальних системах), після чого передаються на центральний сервер лише для зберігання або аналізу.
3. Гібридна архітектура: завдяки цьому елементи централізованої та розподіленої архітектури, що дозволяють оптимізувати обробку даних.

Ця структура забезпечує ефективне та надійне спостереження за об'єктами або процесами, а також прийняття обґрунтованих рішень на основі аналізу отриманих даних.

3.2. Використання програмного забезпечення для аналізу та збереження даних

Вибір програмного забезпечення для аналізу та збереження даних є критично важливим для успішної реалізації системи моніторингу. Ми будемо

використовувати комбінацію існуючих рішень, таких як Elasticsearch, Logstash та Kibana (ELK Stack) для аналізу та візуалізації даних, а також PostgreSQL або MongoDB для зберігання даних.

Elasticsearch забезпечить швидкий і потужний механізм для виконання пошукових запитів і аналізу великих обсягів даних у реальному часі. Logstash дозволить налаштувати канали збору даних з різних джерел, обробляючи та конвертуючи дані в потрібний формат перед їхньою відправкою в Elasticsearch. Kibana надасть можливість візуалізувати дані, що дозволить адміністраторам легше виявляти тренди, патерни та аномалії в мережі.

Для збереження даних ми оберемо PostgreSQL як реляційну базу даних для структурованих даних, оскільки вона забезпечує високу надійність та можливість виконання складних запитів. MongoDB, в свою чергу, буде використовуватися для зберігання неструктурованих даних, таких як логи та інші вхідні дані, що дозволяє зберігати інформацію у гнучкому форматі.

Завдяки інтеграції цих технологій, система зможе забезпечити ефективний аналіз, збереження та візуалізацію даних, що суттєво підвищить загальну продуктивність моніторингу.

1. Програмне забезпечення збору та зберігання даних:

- Бази даних:

Дані, зібрані системою моніторингу, часто зберігаються в базах даних, де вони можуть бути організовані та структуровані для подальшої обробки. Існують різні типи баз даних:

- Реляційні бази даних (SQL): Для організованого зберігання структурованих даних, таких як MySQL, PostgreSQL, Microsoft SQL Server.
- Нереляційні бази даних (NoSQL): Для роботи з великими обсягами неструктурованих або слабо структурованих даних, таких як MongoDB, Cassandra, Elasticsearch.

Дані можуть бути збережені в хмарних сховищах (наприклад, AWS S3, Google Cloud Storage) або в приватних дата-центрах, відповідно до вимог безпеки та доступності.

- Системи обробки даних (ETL):

Системи ETL (Extract, Transform, Load) використовують для вилучення даних із різних джерел, перетворення цих даних у потрібний формат і завантаження їх у базу даних або засобів для подальшої обробки та аналізу. Це може бути корисно, коли дані зібрані з різних джерел або в різних форматах.

Популярні інструменти для ETL: Apache Nifi, Talend, Microsoft SSIS.

2. Програмне забезпечення для аналізу даних:

- Аналітика та візуалізація:

Програмне забезпечення для аналітики допоможе обробляти великі масиви даних та робити висновки на основі статистичного аналізу. наприклад, використання машинного навчання для аномалій або прогнозування майбутніх тенденцій.

Інструменти для аналітики:

- Apache Spark: Фреймворк для обробки великих даних, який підтримує паралельну обробку та машинне навчання.
- Hadoop: Рамкова платформа для обробки великих даних у розподіленому середовищі.
- Tableau, Power BI: Для створення інтерактивних табло та візуалізації даних.
- Python (бібліотеки pandas, numpy, scikit-learn): Для проведення статистичних аналізів, побудови моделей машинного навчання, візуалізації графіків.

- Моделі машинного навчання та прогнозування:

Програмне забезпечення для аналізу може використовувати машинне навчання для побудови моделей, які допомагають у прогнозуванні, виявлені аномалій або процесів оптимізації. зазвичай це включає:

- Навчання на історичних даних для побудови моделей прогнозування.
- Виявлення аномалії для автоматичного виявлення непередбачуваних подій (наприклад, злом, поломка обладнання).

Популярні бібліотеки для машинного навчання:

- TensorFlow, Keras, PyTorch: Для побудови нейронних мереж.
- Scikit-learn: Для класичних методів машинного навчання, таких як класифікація, регресія.
- XGBoost: Для підвищення точності прогнозів на основі дерев рішень.

3. Системи зберігання великих обсягів даних:

- Розподілені системи зберігання:

Для зберігання великих обсягів даних, які генеруються системами моніторингу, розширені файлові системи або сховища даних, які можуть обробляти паралельний доступ і високу пропускну здатність. Це може бути корисно для зберігання журналів, відео чи інших великих даних.

Приклади:

- Розподілена файлова система Hadoop (HDFS): Для обробки і зберігання великих даних у розподіленому середовищі.
- Apache HBase: Розподілена база даних NoSQL, що забезпечує високу доступність і масштабованість.

- Інфраструктура на основі хмари:

Для зберігання даних можна використовувати хмарні платформи, які пропонують гнучкість у масштабуванні, високий рівень доступності та безпеки. Це дозволяє швидко зберегти і обробляти величезні обсяги даних без необхідності інвестувати в інфраструктуру.

Приклади хмарних платформ:

- Amazon Web Services (AWS): Для зберігання даних у S3, обробки через EC2 або AWS Lambda, бази даних RDS.
- Google Cloud Platform (GCP): Для зберігання даних через Google Cloud Storage, обробки через Google BigQuery.

4. Безпека та управління доступом:

- Шифрування та захист даних:

Програмне забезпечення має забезпечити шифрування даних під час зберігання та передачі для запобігання несанкціонованому доступу.

Це можуть бути алгоритми шифрування, такі як AES для збереження даних, а також протоколи SSL/TLS для захисту переданих даних.

- Управління доступом і аутентифікація:

Використовуйте систему автентифікації та авторизації, наприклад OAuth, LDAP або Active Directory , для контролю доступу до даних та програмного забезпечення.

Ролі користувачів та управління доступом до певних функцій або даних у системі моніторингу.

5. Автоматизація та моніторинг процесів:

- Інструменти для автоматизації процесів:

Використання програмних інструментів для автоматизації обробки даних або створення звітів. Наприклад, автоматичне оновлення даних, виконання аналітики в реальному часі, генерація сповіщень або повідомлень про аномалії.

Для унаочнення відобразимо інформацію у вигляді таблиці 3.1.

Таблиця 3.1.

Хмарні платформи та процеси

Категорія	**Приклад/Опис**
Хмарні платформи	Amazon Web Services (AWS): Зберігання даних у S3, обробка через EC2 або AWS Lambda, бази даних RDS.
Хмарні платформи	Google Cloud Platform (GCP): Зберігання даних через Google Cloud Storage, обробка через Google BigQuery.
Безпека та управління доступом	Шифрування та захист даних: Алгоритми AES для збереження даних, протоколи SSL/TLS для захисту переданих даних.
Безпека та управління доступом	Управління доступом і аутентифікація: OAuth, LDAP, Active Directory для контролю доступу до даних.
Автоматизація та моніторинг процесів	Інструменти для автоматизації процесів: Apache Airflow для автоматизації робочих процесів.
Автоматизація та моніторинг процесів	Інструменти для автоматизації процесів: Cron jobs для запуску завдань за розкладом у Unix-подібних системах.

Другий рівень передбачає формування сповіщень на основі налаштованих правил. Користувачі зможуть визначати порогові значення для різних параметрів, таких як завантаженість мережі, кількість підключених пристроїв, кількість спроб

доступу до системи тощо. Якщо будь-який з цих параметрів перевищить встановлене порогове значення, система негайно сповістить відповідальних осіб.

Третій рівень передбачає використання інтеграцій з популярними месенджерами та системами комунікації. Система буде здатна надсилати повідомлення через SMS, електронну пошту або месенджери, такі як Telegram, що забезпечить швидке і зручне сповіщення.

Таким чином, реалізовані механізми попередження та оповіщення забезпечать оперативне реагування на інциденти та суттєво підвищать рівень безпеки мережі.

Основні компоненти системи попередження та оповіщення

1. Моніторинг даних та подій:

Для початку важливо встановити параметри, які потребують моніторингу. Це може бути:

Система може відслідковувати стан сервісів, програм, процесів.

Дані з сенсорів або пристроїв (температура, вологість, рівень забруднення, інші фізичні або хімічні параметри).

Статистичні показники або тенденції, такі як завантаження серверів, мережевих збоїв, помилок у програмному забезпеченні тощо.

2. Установка порогових значень:

Для того, щоб застосувати, коли відбувається інцидент, необхідно встановити пороги тривоги наприклад:

- Максимальне або мінімальне значення температури.
- Пороги навантаження на сервери чи мережу.
- Деякі системи вибір динамічні пороги , які адаптуються у залежності від нормальної варіативності процесу (наприклад, за допомогою методів машинного навчання).

3. Обробка подій та аномалій:

Виявлення інцидентів може відбуватися на основі певних подій або аномалій, що створюються в даних. Це може бути:

- Шаблон виявлення: якщо певна подія завершена встановлений поріг.

- Аномальне виявлення: Використовуються методи машинного навчання або статистичні моделі для виявлення подій, що є відхиленнями від звичайної системи поведінки.

4. Алгоритми обробки інцидентів:

Після виявлення інциденту система може використовувати певні правила або алгоритми для класифікації інциденту, встановлення його пріоритету та визначення кроків для реагування.

3.3. Механізми оповіщення

1. Сповіщення в реальному часі:

Після виявлення інциденту система повинна надіслати сповіщення користувача або відповідного для реагування персоналу.

Сповіщення може бути додатково за формою:

- Email: Це один із найбільш розширених способів оповіщення про інциденти.
- SMS: Для сповіщення на мобільних пристроях у випадках, коли необхідна термінова реакція.
- Push-сповіщення: Використовуються в мобільних додатках або спеціалізованих системах, наприклад, у додатках для моніторингу серверів.
- Телефонні дзвінки або IVR: Автоматичні дзвінки або голосові сповіщення про інциденти.

2. Інтерфейс для користувача:

Користувачі можуть отримувати інформацію про інциденти через графічні інтерфейси (дашборди), на яких у реальному часі відображаються статуси та звіти про події.

Візуалізація може включати:

- Графіки та діаграми: для швидкої оцінки стануть різні параметри (наприклад, графік завантаження на сервері).

- Списки подій або інцидентів: системи можуть автоматично категоризувати інциденти за рівнем важливості (наприклад, «низький», «середній», «високий») і видавати їх в інтерактивних списках для подальшої обробки.

3. Інтеграція з іншими системами:

Сповіщення може бути інтегровано з іншими корпоративними системами або інструментами для автоматизації управлінських та операційних процесів:

- CRM-системи (Customer Relationship Management): Для оповіщення менеджерів.
- Системи управління подіями (SIEM): Для аналізу й моніторингу безпеки.
- Інструменти для управління інцидентами (ITIL, ServiceNow): Для реєстрації та моніторингу інцидентів в рамках управління IT-послугами.

4. Реакція на інцидент:

Для кожного типу інциденту можуть бути передбачені певні дії реагування :

Наприклад, автоматичні дії: система може автоматично виконувати певну команду для виправлення сервера (відновлення сервісу, перезапуск програми тощо).

Сповіщення та ескалація: Якщо інцидент не було усунуто, сповіщення може бути ескальовано до вищого рівня адміністрації або технічної підтримки.

5. Інтерфейс для адміністраторів та технічної підтримки:

Адміністратори мають доступ до розширених журналів подій та зведених звітів про інциденти, що дозволяє не лише реагувати на поточні проблеми, а й аналізувати тенденції для попередження майбутніх інцидентів.

Інтерфейси включають часті функції:

- Фільтрація подій за типами, критичністю або часом.
- Пошук за ключовими словами чи подіями для виявлення закономірностей.
- Документація інцидентів: Для реєстрації дій, які були виконані, і результатів.

Приклад реалізації механізмів оповіщення

Уявимо, що система моніторингу IT-інфраструктури виявляє перевищення порогу завантаження на сервері. Порядок сповіщення та реагування може виглядати так:

1. Виявлення інциденту: Система фіксує, що завантаження на сервер досягло 90%.
2. Оповіщення: спочатку система надсилає сповіщення на електронну пошту та SMS адміністратора.
3. Аналіз та реагування: Адміністратор вивчає деталі інциденту через веб-інтерфейс, показує графік завантаження на сервері.
4. Автоматичне реагування: у випадку, якщо завантаження продовжує зростати, система автоматично запускає скрипт для перезапуску певних процесів або навіть переміщує завантаження на інший сервер.
5. Ескалація: якщо проблема не вирішена протягом 30 хвилин, інцидент ескалується до вищого рівня технічної підтримки.

Реалізація ефективних механізмів попередження та оповіщення учасників не лише випадково виявити інциденти, але й автоматизувати процеси реагування та мінімізувати час простої або збитків від нещатних ситуацій. Відповідно до системності, механізми можуть включати прості порогові сполучення або складні системи з автоматизованими діями та інтеграцією з іншими інструментами.

3.4. Тестування та оцінка ефективності системи

Тестування та оцінка ефективності системи є важливими етапами у процесі розробки, оскільки дозволяють визначити, наскільки система відповідає вимогам та очікуванням користувачів. Для тестування системи моніторингу буде використано декілька методів (рис.3.2).

Першим етапом тестування є функціональне тестування, яке дозволить перевірити, чи всі компоненти системи працюють відповідно до технічних вимог.

Це включає перевірку збору даних, обробки інформації, зберігання даних, а також механізмів оповіщення.

Другим етапом буде навантажувальне тестування, яке дозволить оцінити, як система реагує на збільшення обсягу даних та кількість одночасних запитів. Це важливо для виявлення можливих проблем з продуктивністю і забезпечення стабільної роботи системи в умовах високих навантажень.

Третім етапом є тестування на безпеку, яке включає перевірку вразливостей системи та оцінку її стійкості до зовнішніх загроз. Це дозволить виявити слабкі місця в системі та своєчасно вжити заходів для їх усунення.

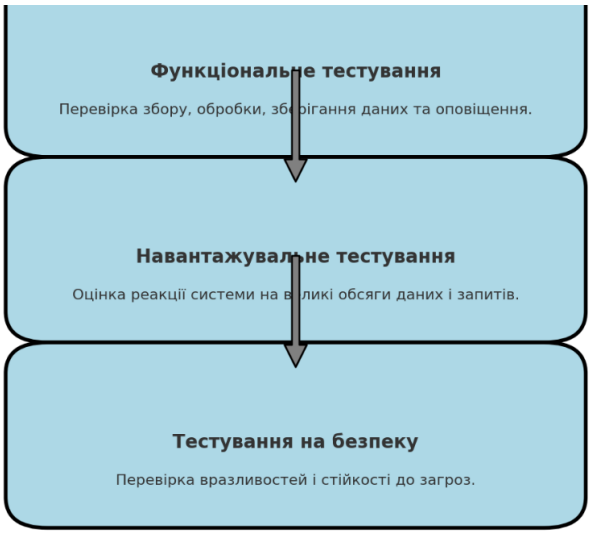


Рис. 3.2. Етапи тестування та оцінки ефективності системи моніторингу

Оцінка ефективності системи буде базуватися на результатах тестування, а також на відгуках користувачів. Основними критеріями оцінки будуть швидкість збору та обробки даних, точність виявлення загроз, час реагування на інциденти та задоволеність користувачів. На основі цих даних буде сформульовано план подальшого вдосконалення системи.

1. Тестування системи моніторингу

Тестування є необхідним для перевірки функціональності та надійності системи моніторингу в різних умовах. Тестування можна розділити на кілька типів:

- Функціональне тестування:
  - Перевіряється, чи працюють усі компоненти системи моніторингу відповідно до вимог. Наприклад, чи правильно збираються дані, чи правильно налаштовані пороги для сповіщення.
  - Тестується, чи правильно система реагує на події, розповідає про інциденти, чи правильно зберігаються і обробляються дані.
- Навантажувальне тестування (Stress Testing):
  - Це системи тестування при сильному навантаженні для перевірки її здатності працювати при великих обсягах даних або високих швидкостях обробки.
  - Наприклад, система повинна бути здатна обробляти великий обсяг запитів у піксельних умовах навантаження без втрати точності або своєчасного реагування.
- Тестування на відмову (Failure Testing):
  - Тестується, як система виникає в разі відмови одного з її компонентів або зовнішніх систем (наприклад, несправність датчика або відключення мережі).
  - Важливо перевірити, чи система може відновити свою роботу після відмови, чи є механізм аварійного відновлення та чи не втрачаються критичні дані.
- Тестування на масштабованість:
  - Перевірка здатності системи обробляти додаткові джерела даних або нові пристрої без значного зниження продуктивності.
  - Важливо оцінити, як система моніторингу масштабується в умовах збільшення кількості об'єктів моніторингу.
- Тестування безпеки:
  - Перевірка системи на вразливість до різних типів атак (наприклад, DoS-атаки, атаки з підробленими даними, несанкціонований доступ).
  - Оцінка правильності налаштування політики безпеки (шифрування даних, автентифікація користувачів, логування подій).

2. Оцінка ефективності системи

Після тестування важливо оцінити ефективність системи моніторингу. Оцінка ефективності включає в себе вимірювання ключових показників, які гарантують якість роботи системи.

- Точність та надійність збору даних:
  - Оцінка того, наскільки точно і коректно система збирає дані, порівнюючи їх з реальними значеннями або іншими джерелами.
  - Перевірка, яка втрачає дані або некоректні значення.
- Час перегляду системи (Latency):
  - Час, який потрібен системі для виникнення інциденту після того, як він стався. Це критично важливо для забезпечення швидкого реагування.
  - Оцінка часу затримки між підцією та спільним використанням користувача чи адміністратора.
- Продуктивність системи (Throughput):
  - Оцінка того, скільки даних система може обробити за одиницю часу. Це важливо для визначення того, як система справляється з великими обсягами даних або великою кількістю пристроїв.
- Актуальність даних:
  - Оцінка того, чи дані, зібрані системою моніторингу, є актуальними, що означає, що вони реально стануть об’єктами моніторингу на момент їх збору.
- Інтервал сповіщення та точність інцидентів:
  - Оцінка того, наскільки швидко система розповідає про інцидент і чисельно ці сповіщення точні.
- Важливо, щоб система не надсилала зайві, помилкові сповіщення (false positives) і не пропускала важливі інциденти (false negatives).

3. Надійність та доступність системи:

- Оцінка того, надійною є система, тобто вона працює без збоїв протягом тривалого часу.
- Перевірка доступності системи в різних умовах, наприклад, для наявності високого завантаження або часткових збоїв в інфраструктурі.

3. Інструменти та методи оцінки ефективності

- Аналіз логів:

➢ Аналіз журналів подій, які генерують систему моніторингу. Цей процес виявляє помилки, спроби зломів, збої в системі роботи та комп'ютері з причин інцидентів.

- Використання метрики та KPI (ключових показників ефективності):

➢ Визначення набору метрик (наприклад, середній час відгуку, кількість пропущених подій, середній час рішення інциденту), які будуть використовуватися для оцінки ефективності системи.

- Тестові сценарії:

➢ Використання сценаріїв, які моделюють реальні умови роботи системи. Наприклад, симуляція підвищеного навантаження або непередбачених ситуацій, щоб оцінити, як система реагує на них.

- Моніторинг в реальному часі:

➢ Використання системи моніторингу для оцінки роботи самої системи моніторингу (наприклад, час перегляду, точність даних, перевірка коректності перевірки в реальному часі).

4. Ітеративне вдосконалення системи

Тестування та оцінка ефективності повинні бути безперервним процесом. Ось кілька підходів для покращення системи після тестування:

- Аналіз отриманих результатів тестування дозволяє зменшити слабкі місця в системі роботи та вдосконалити її.
- Внесення корективу в налаштування системи , на основі отриманих даних про ефективність (наприклад, коригування порогових значень, зменшення латентності).
- Вдосконалення механізмів оповіщення та обробки інцидентів з нарахуванням мінімізації помилок у визначені інциденти та скорочення часу реагування.

Тестування та оцінка ефективності системи моніторингу є певними етапами для забезпечення її належної роботи в умовах реального навантаження. Завдяки остаточному тестуванню можна винести та усунути проблеми на ранніх етапах,

що дозволяє значно підвищити ефективність системи, зменшити кількість помилок та підвищити швидкість.

РОЗДІЛ 4. АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Аналіз результатів дослідження передбачає детальну оцінку розробленої системи моніторингу в порівнянні з існуючими рішеннями, економічною ефективністю впровадження, а також надійністю і масштабованістю системи.

4.1. Порівняння розробленої системи з існуючими рішеннями

Аналіз результатів дослідження передбачає порівняння розробленої системи моніторингу з існуючими рішеннями на ринку. Це дозволяє оцінити, наскільки нова система перевершує або поступається вже наявним системам за різними критеріями, такими як функціональність, продуктивність, безпека та зручність використання.

У порівнянні з традиційними системами моніторингу, розроблена система має ряд переваг, зокрема, використання сучасних технологій машинного навчання для виявлення аномалій, що дозволяє підвищити точність моніторингу та зменшити кількість хибних спрацьовувань. Крім того, система інтегрує хмарні технології, що забезпечує масштабованість та доступність даних з будь-якої точки.

Також, на відміну від більшості традиційних рішень, наша система реалізує гнучкі механізми оповіщення, що дозволяють налаштовувати канали зв’язку відповідно до вимог користувачів. Це суттєво покращує оперативність реагування на інциденти та зменшує ризики (табл.4.1)

Таблиця 4.1.

Порівняння критеріїв розробленої системи та існуючих рішень.

Критерії	Розроблена система	Існуючі рішення
Функціональність	Інноваційні можливості, ML, адаптація	Стандартні функції, обмежена інтеграція
Масштабованість	Горизонтальне масштабування	Обмеження при великому обсязі
Інтерфейс та зручність	Гнучкий, налаштований інтерфейс	Стандартний інтерфейс
Інтеграція	Потужні API та гнучкість	Готові інтеграції, обмежена адаптація
Вартість	Високі початкові витрати, низькі підтримки	Регулярні витрати на ліцензії
Надійність та безпека	Адаптивна безпека, налаштування	Перевірені засоби безпеки

Основні критерії порівняння:

1. Функціональність

Розроблена система : Має особливі функціональні можливості, які можуть включати налаштування порогів, автоматичне реагування на інциденти, інтеграцію з іншими системами та детальну візуалізацію даних. Може також підтримувати динамічні пороги та виявлення аномалій на основі машинного навчання.

Існуючі рішення : Більшість комерційних або готових рішень пропонують стандартний набір функцій, таких як моніторинг стану системи, виявлення простих порушень та сповіщення користувачів. Однак деякі більш складні механізми, як аномалія або інтеграція з іншими корпоративними системами, можуть бути або обмежені, або доступні тільки в преміум-версіях.

Порівняння :

- Якщо розроблена система включає інноваційні можливості (наприклад, застосування штучного інтелекту для аналізу даних, адаптивні алгоритми реагування), вона може мати перевагу над стандартними рішеннями.
- Існуючі рішення можуть бути простішими в налаштуваннях та використанні, але менш гнучкими та потужними.

2. Масштабованість

Розроблена система : Масштабованість залежить від її архітектури. Якщо система була спроектована з урахуванням можливостей розширення, вона може підтримувати збільшення кількості об’єктів моніторингу без значних витрат на ресурси.

Існуючі рішення : Багато готових рішень мають вбудовану масштабованість, однак можуть виникати проблеми з ефективністю при обробці великого обсягу даних або великої кількості пристроїв, особливо в недорогих або базових версіях.

Порівняння :

- Якщо розроблена система має чітко сплановану та чітко сплановану архітектуру для роботи з великими даними та підтримує горизонтальне масштабування (розширення без значних змін внутрішньої структури), це може бути її значною перевагою.

- Існуючі рішення можуть мати обмеження, які знижують ефективність при більшій кількості пристроїв або інцидентів.

3. Інтерфейс та зручність використання

Розроблена система : Інтерфейс залежить від вимог та специфікацій проекту, і може бути налаштований під конкретні потреби користувачів. Гнучкість у дизайні та функціональності інтерфейсу дозволяє створити більш комфортний та інтуїтивно зрозумілий продукт.

Існуючі рішення : Більшість готових рішень мають стандартні інтерфейси, які можуть бути менш гнучкими, але вони, як правило, добре документовані, з досвідченими командами, що підтримуються та навчальними матеріалами.

Порівняння :

- Розроблена система може мати перевагу, якщо її інтерфейс налаштований саме під потреби користувачів (наприклад, для технічних спеціалістів або адміністраторів), що робить її більш зручною в експлуатації.
- Існуючі рішення часто мають перевірену базову користувальницьку та стандартні функціональні можливості, що можуть бути перевагою для компаній, які шукають просто рішення без необхідності в налаштуваннях.

4. Інтеграція з іншими системами

Розроблена система : Якщо система була спроектована з урахуванням інтеграції, вона може безпроблемно взаємодіяти з іншими корпоративними інструментами, такими як CRM-системи, системи управління інцидентами, бізнес-аналізу або автоматизації.

Існуючі рішення : Високоякісні комерційні рішення часто мають добре розвинену інтеграційну здатність, проте не всі з них підтримують відкриті інтерфейси для додаткових налаштувань чи спеціальних програмних платформ.

Порівняння :

- Якщо розроблена система включає потужні API та інші інструменти для інтеграції, вона може бути більш адаптованою до конкретних потреб організації.

- Існуючі рішення, як правило, мають відмінний документ для інтеграції з популярними інструментами, проте можуть мати обмежену гнучкість при інтеграції з нестандартними або менш популярними платформами.

5. Вартість

Розроблена система : Першочергові витрати на розробку можуть бути великими, однак у довгостроковій перспективі система може бути більш вигідною, особливо якщо компанія вже має ресурси для її підтримки та адаптації.

Існуючі рішення : Комерційні рішення часто вимагають регулярних витрат на ліцензії, обслуговування, оновлення та навчання персоналу. Вартість може залежати від кількості користувачів, масштабів організації та функціональності.

Порівняння :

- Розроблена система може бути більш вигідною в разі масштабних чи спеціальних потреб, витрати на підтримку та оновлення можуть бути мінімальними після початкової розробки.
- Існуючі рішення можуть бути швидкими для впровадження та підтримки, але вимагають регулярних витрат, які з часом можуть виявитися дорожчими.

6. Надійність та безпека

Розроблена система : Можливість створення власних механізмів безпеки, включаючи шифрування даних, контроль доступу, моніторинг вразливостей. Однак, для забезпечення високого рівня безпеки потрібен додатковий зусиль.

Існуючі рішення : Як правило, комерційні системи мають механізми безпеки, що відповідають галузевим стандартам. Однак вони можуть бути невразливими до нових типів загроз або потребувати регулярного оновлення для підтримки актуальності.

Порівняння :

- Розроблена система може мати певні переваги в безпеці, потім вона може бути адаптована до конкретних вимог безпеки, але її підтримка може вимагати додаткових ресурсів.

➢ Існуючі рішення часто мають вбудовані та вже перевірені засоби безпеки, але можуть бути менш гнучкими у разі необхідності інтеграції з новими стандартами безпеки.

Переваги розробленої системи :

- Може мати інноваційні функції, зокрема адаптивні алгоритми, інтеграцію з іншими корпоративними системами та високу гнучкість.
- Можна оптимізувати під спеціальні вимоги організації.
- Може бути більш вигідною довготривалою перспективою, якщо є внутрішні ресурси для її підтримки та адаптації (рис.4.1).

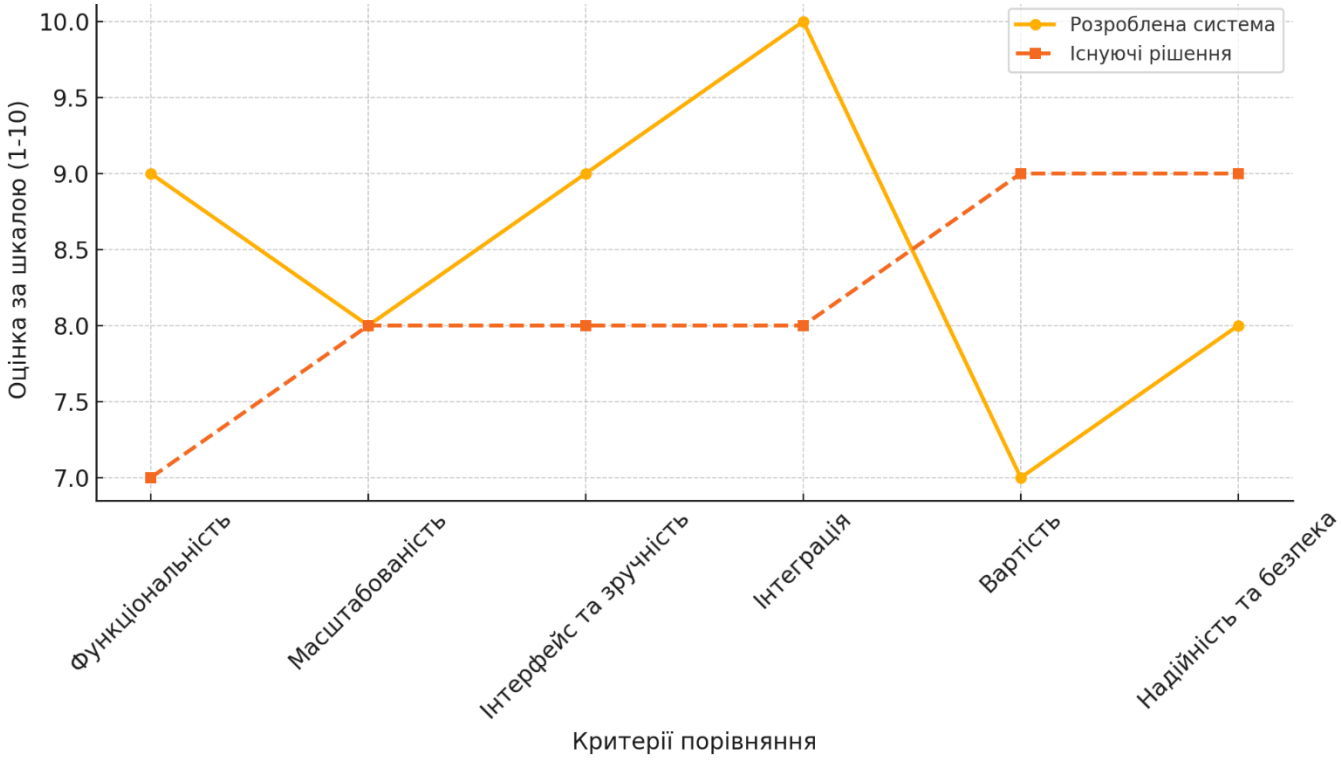


Рис. 4.1. Графічна структура переваг розробленої системи

Переваги існуючих рішень :

- Швидке впровадження та використання з мінімальними налаштуваннями.
- Добре розвинена підтримка, документація та готові рішення для інтеграції з популярними системами.
- Надійність і безпека на високому рівні перевіреним стандартам.

Вибір між розробленою та існуючою системою залежить від певних потреб організації, бюджету та наявності внутрішніх ресурсів для підтримки розробки та системи моніторингу.

4.2. Економічна ефективність впровадження системи

Економічна ефективність впровадження системи моніторингу є ключовим аспектом для бізнесу та організацій, які планують інвестувати у нові технології. Для оцінки економічної ефективності ми розглянемо витрати на розробку та впровадження системи, а також потенційні вигоди, які вона може принести.

Витрати включають закупівлю обладнання, програмного забезпечення, витрати на навчання персоналу, а також витрати на обслуговування та оновлення системи. Однак ці витрати компенсуються зниженням ризиків, пов’язаних з кібератаками, зменшенням витрат на реагування на інциденти, а також підвищенням продуктивності роботи співробітників.

Крім того, розроблена система моніторингу може значно скоротити час, необхідний для виявлення та усунення загроз, що безпосередньо вплине на економічні показники компанії. Впровадження автоматизованих механізмів моніторингу та оповіщення дозволяє зменшити навантаження на IT-персонал, що також призводить до економії ресурсів.

З урахуванням усіх цих факторів можна стверджувати, що впровадження системи моніторингу забезпечить суттєві економічні вигоди для організації.

Ключові елементи економічної ефективності:

1. Первісні витрати на впровадження

Витрати на впровадження системи моніторингу включити:

- Розробка або придбання системи : Вартість розробки індивідуальної системи або ліцензій на комерційне програмне забезпечення. У випадку розробки власної системи враховуються витрати на команду розробників, тестувальників, адміністраторів.

- Інтеграція з існуючими системами : Необхідно врахувати витрати на інтеграцію нової системи з іншими корпоративними системами (наприклад, ERP, CRM), налаштування API, адаптованих існуючих бізнес-процесів.
- Навчання персоналу : Витрати на навчання співробітників для використання нової системи. Це може включати тренінги, створення документації, підтримку на етапі впровадження.
- Інфраструктурні витрати : Витрати на сервери, бази даних, мережеві рішення, програмне забезпечення для адміністрування та резервного копіювання даних.

2. Постійні витрати на експлуатацію

- Підтримка та обслуговування систем : Витрати на технічну підтримку та оновлення програмного забезпечення, усунення помилок, оновлення функцій. Це може включати як внутрішні ресурси, так і оплату послуг зовнішніх постачальників.
- Операційні витрати : Витрати на енергію для роботи серверів та інших компонентів інфраструктури, витрати на зберігання даних.
- Заробітна плата персоналу : Витрати на утримання персоналу, відповідного за управління та моніторинг системи роботи.

3. Очікувані вигоди від впровадження

- Зниження витрат на обслуговування та інциденти : Завдяки щасливому виявленню проблеми системи моніторингу можуть швидше відновитися на збої в роботі, що знижує час простоїв та витрати на відновлення.
- Покращення продуктивності : Моніторинг дозволяє автоматизувати процеси, які раніше вимагали ручного втручання, наприклад, перевірка стану обладнання чи мережі. Це дозволяє порушити завантаження на персонал і підвищити ефективність роботи.
- Зниження ризиків та збитків від інцидентів : Проблеми в інфраструктурі можуть привести до значних фінансових втрат. Система моніторингу дозволяє мінімізувати час реакції та швидко локалізувати проблему, що зменшує кількість збитків.

- Покращення якості обслуговування клієнтів : Моніторинг дозволяє своєчасно виявляти проблеми в наданні послуг (наприклад, затримки в обробці запитів клієнтів), що може підвищити рівень задоволення клієнтів та погіршити ризик їх відтоку.
- Покращення прийняття управлінських рішень : Завдяки зібраним даним система моніторингу надає точні аналітичні дані, які можуть бути використані для прийняття стратегічних рішень щодо розвитку інфраструктури або змін у процесах.

4. Оцінка ефективності: економічні показники

Для оцінки економічної ефективності впровадження системи відповідають різним фінансовим показникам, які можуть бути кілька варіантів застосування від інвестицій:

- ROI (Return on Investment) : Оцінка разом між отриманими вигодами та витратами на впровадження.
- TCO (Total Cost of Ownership) : Загальна вартість володіння системою протягом її життєвого циклу. Враховуються не лише початкові витрати на впровадження, а й постійні витрати на підтримку та обслуговування.
- NPV (Net Present Value) : Чиста поточна вартість, яку порівняти оцінити, чи є інвестиція вигідною в довгостроковій перспективі, враховуючи дисконтовані грошові потоки.
- Payback Period : Період окупності — час, необхідний для того, щоб витрати на впровадження системи були покриті збереженими витратами чи збільшеними доходами.

5. Аналіз ризиків та непрямих вигод

- Ризики : Невизначеність, пов'язана з технічними проблемами при інтеграції систем, можливими збоєм у її роботі чи неефективністю при несподіваних обсягах даних.
- Непрямі вигоди : Поліпшення репутації компанії через стабільність і надійність роботи її інфраструктури, підвищення рівня довіри з боку клієнтів та партнерів (рис.4.2).

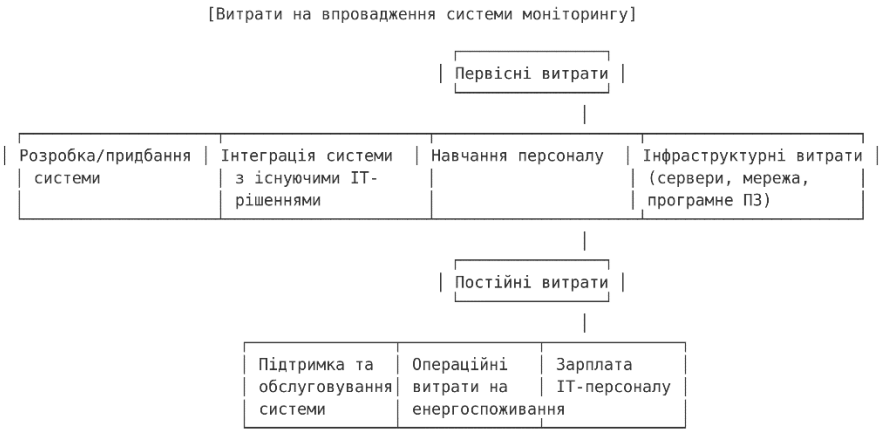


Рис.4.2. Економічна ефективність впровадження системи моніторингу

Економічна ефективність впровадження системи моніторингу збільшення поєднань початкових інвестицій, операційних витрат і майбутніх вигод. Система моніторингу може призвести до значних заощаджень на обслуговуванні інфраструктури, зниження ризиків інцидентів, підвищення продуктивності та покращення якості обслуговування клієнтів. Однак для точного аналізу ефективності необхідно оцінити всі витрати та вигоди з урахуванням специфіки компанії та її потреб.

Тому економічна ефективність проекту може бути позитивною, якщо система дозволить знизити загальні витрати, підвищити рівень безпеки та стабільність роботи, а також збільшити доходи через рік.

4.3. Оцінка надійності та масштабованості системи

Надійність та масштабованість системи є критичними показниками для її успішної роботи. Надійність системи визначається її здатністю безвідмовно виконувати функції в умовах різних навантажень та потенційних загроз. Для оцінки надійності буде проведено ряд тестів, включаючи стресове тестування та моделювання різних сценаріїв, які можуть вплинути на роботу системи.

Масштабованість системи передбачає її здатність адаптуватися до змін у навантаженні, а також до збільшення обсягу даних та кількості користувачів. Це є

важливим аспектом, особливо для організацій, які планують розширення або мають високий рівень динамічності.

Наша система буде побудована на основі мікросервісної архітектури, що забезпечує гнучкість у масштабуванні окремих компонентів. Це дозволить з легкістю адаптувати систему під змінювані вимоги бізнесу без значних витрат на перепроектування.

Також ми будемо використовувати автоматизовані механізми резервного копіювання і відновлення, що забезпечить високу надійність системи у разі виникнення збоїв. Завдяки цим підходам, ми можемо забезпечити не тільки високу продуктивність системи, але й її здатність без проблем обробляти великі обсяги даних.

1. Оцінка надійності системи

Надійність системи моніторингу розвитку її здатності функціонувати без збоїв протягом тривалого часу, а також швидко відновлюватися у разі несправностей. Для оцінки надійності розглядаються такі аспекти:

1.1. Доступність системи (Availability)

- Показники :

➢ SLA (Service Level Agreement) : Договірна угода, яка визначає рівень доступності системи, наприклад, 99,9% або 99,99%.

➢ Час безвідмовної роботи : Оцінка того, скільки годин система може працювати без збоїв протягом певного періоду (наприклад, кількість годин безвідмовної роботи за рік).

➢ Час відновлення (MTTR - Mean Time to Repair) : Середній час, необхідний для відновлення системи після збоїв.

➢ Час між відмовами (MTBF - Mean Time Between Failures) : Середній час між неполадками системи.

Як оцінюється доступність :

- Важливо відмітити, чи передбачена система резервування, відновлення автоматичних процесів та швидке реагування на інциденти.

- Найнадійніша система моніторингу повинна мати низький час відновлення та забезпечити високу доступність, навіть при виникненні збоїв в окремих компонентах.

1.2. Безпека та стійкість до атаки

- Аналіз загроз : Оцінка наявних загроз, таких як DDoS-атаки, спроби несанкціонованого доступу до системи моніторингу або витоків даних.
- Механізми захисту : Оцінка наявності шифрування, автентифікації, механізмів контролю доступу, моніторингу безпеки.
- Резервне копіювання та відновлення : Наявність надійних стратегій резервного копіювання та відновлення даних у разі критичних відмов.

Як оцінюється безпека :

- Важливим критерієм є здатність системи автоматично виявляти та реагувати на аномалії, а також забезпечувати безперервну роботу при навіть атаках або несанкціонованому доступі.

1.3. Тестування надійності

- Стрес-тестування : Оцінка системи роботи під високими навантаженнями для виявлення слабких місць, які можуть призвести до збою.
- Тестування на відмовостійкість : Симуляція відмови окремих компонентів для перевірки здатності системи до самовідновлення та забезпечення безперебійної роботи.

Як оцінюється надійність :

- Надійність системи повинна бути підтверджена результатами тестування, а також історією її роботи в реальних умовах. Враховуються можливості проблем, які можуть виникнути під час масштабування або зміни навантаження.

2. Оцінка масштабованості системи

Масштабованість системи моніторингу оцінюється за її здатність ефективно працювати при зростанні кількості об'єктів моніторингу, обсягу даних і вимог до обробки інформації.

2.1. Типи масштабованості

- Горизонтальна масштабованість : Це здатність системи додавати нові ресурси, наприклад, сервери, без значних змін в архітектурі. Горизонтальна масштабованість важлива для системи, яка обробляє велику кількість даних.
- Вертикальна масштабованість : збільшення потужності окремих компонентів системи, наприклад, підвищення потужності серверів або додавання процесорів для обробки більших обсягів даних.

2.2. Масштабованість архітектури

- Мікросервісна архітектура : Якщо система розроблена на базі мікросервісів, кожен компонент можна масштабувати незалежно, що значно спрощує адаптацію до зростаючих потреб.
- Розподілена обробка : Система, що використовує розподілену обробку даних (наприклад, за допомогою технологій Hadoop, Spark або іншої платформи), здатна ефективно працювати з великими обсягами даних.
- Обробка в реальному часі : Для великих обсягів даних необхідно забезпечити обробку в реальному часі, що вимагає відповідної архітектури, наприклад, використання черг повідомлень або потокових платформ.

2.3. Масштабованість у плані підтримки кількості пристроїв та об'єктів моніторингу

- Кількість пристроїв : Оцінка того, скільки пристроїв, серверів або точок моніторингу може підтримувати систему без значного падіння продуктивності.
- Обсяг даних : Оцінка здатності системи працювати з великими обсягами даних, які знаходяться в реальному часі, і забезпечувати їх зберігання та аналіз.

2.4. Гнучкість до вимог зміни

- Підтримка нових протоколів і стандартів : Масштабована система повинна безперешкодно інтегрувати нові типи пристроїв, протоколів або технологій, які використовуються в процесі розвитку бізнесу чи технологій.

- Легка адаптація до змін бізнес-вимог : Гнучкість у налаштуваннях порогових значень, алгоритмів виявлення аномалій або підтримка нових сценаріїв моніторингу.

2.5. Тестування масштабованості

- Тестування навантажень : Перевірка здатності системи справлятися з високими навантаженнями, наприклад, кількість об'єктів моніторингу або даних різко зростає.
- Моделювання завантажень : Оцінка системи роботи при збільшенні кількості пристроїв або обсягів даних, щоб зрозуміти, як система змінює завантаження.

3. Оцінка ефективності надійності та масштабованості

Надійність :

- Високий рівень надійності забезпечує стабільність роботи системи навіть при виникненні непередбачуваних ситуацій.
- Важливі фактори: відновлення часу, відмовостійкість, підтримка безпеки та моніторинг в реальному часі.

Масштабованість :

- Масштабована система може адаптуватися до збільшення вимог без значного впливу на продуктивність.
- Важливою характеристикою є здатність обробляти великі обсяги даних, підтримувати велику кількість пристроїв та адаптацію до нових технологій.

Отже, можна зробити висновки:

1. Надійність : Система повинна забезпечувати високий рівень доступності, безпеки та відмовостійкості. Регулярне тестування та використання стратегій резервного копіювання є необхідними для підтримки високої надійності.
2. Масштабованість : Архітектурні системи мають бути гнучкою, щоб підтримувати збільшення кількості об'єктів моніторингу та даних без зниження продуктивності. Підтримка горизонтального масштабування та адаптації до змін є ключовими критеріями для забезпечення ефективності роботи системи в майбутньому.

ВИСНОВКИ

Проведене дослідження показало, що розробка системи моніторингу бездротових мереж може суттєво підвищити рівень безпеки та ефективності управління мережами. З використанням сучасних технологій, таких як машинне навчання, хмарні рішення та протоколи моніторингу, система здатна швидко виявляти аномалії, автоматично реагувати на інциденти та знижувати ризики.

Архітектура системи, яка включає різні рівні збору, обробки, зберігання та оповіщення, забезпечує комплексний підхід до моніторингу, що дозволяє ефективно управляти ресурсами та даними. Оцінка економічної ефективності впровадження системи свідчить про значні вигоди, які можуть бути отримані внаслідок її використання.

Перспективи подальших досліджень у сфері моніторингу бездротових мереж охоплюють вдосконалення алгоритмів аналізу даних, інтеграцію нових технологій, таких як блокчейн для підвищення безпеки, а також розвиток методів виявлення та реагування на нові загрози.

Крім того, важливо продовжити дослідження у сфері економічної ефективності та ROI (повернення інвестицій) для підприємств, які впроваджують подібні системи. Подальші дослідження також можуть зосередитися на дослідженні взаємодії між різними компонентами системи та вдосконаленні механізмів оповіщення, щоб підвищити зручність користування для адміністраторів та забезпечити максимально ефективну реакцію на інциденти.

Таким чином, розвиток та вдосконалення систем моніторингу бездротових мереж є надзвичайно актуальними завданнями, які потребують подальшого дослідження та реалізації інноваційних рішень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network anomaly detection: Methods, systems, and tools. ACM Computing Surveys. 2018. Vol. 50(6). P. 1–36.

2. Chakraborty S., Jang D., Ramakrishnan N., Das S. R. Anomaly detection in cyber-physical systems: A survey. ACM Computing Surveys. 2016. Vol. 49(3). P. 1–37.

3. Computer Networks: A Systems Approach / Larry L. Peterson, Bruce S. Davie. URL: https://book.systemsapproach.org/ (дата звернення: 21.10.2024).

4. Dhawan M., Sood S. K., Sharma A. Anomaly detection in network traffic: A comprehensive survey. Journal of Network and Computer Applications. 2018. Vol. 103. P. 95–122.

5. Di Martino B., Esposito M., Rak M. Network monitoring in the cloud computing era: The state of the art and research challenges. IEEE Communications Surveys & Tutorials. 2018. Vol. 15(1). P. 262–293.

6. Jiang J., Li W., Wang G. A comprehensive survey on network anomaly detection techniques: Taxonomy, benchmarks, and future directions. Mathematical Problems in Engineering. 2018.

7. Kaur K., Verma A. K. Intrusion detection system: A comprehensive review. Procedia Computer Science. 2016. Vol. 89. P. 17–23.

8. Mahmood S., Shafique M., Qayyum U., Javaid N., Alrajeh N. Anomaly detection techniques in wired and wireless networks: A survey. Computers & Security. 2019. Vol. 83. P. 131–153.

9. Python Crash Course / Eric Matthes. 2020. URL: https://l-p.ua/wp-content/uploads/2021/10/metiz.-izuchaem-python.pdf (дата звернення: 21.10.2024).

10. Rajabzadeh A., Ghorbani A. A. Network anomaly detection methods: Systems, challenges and future directions. Journal of Network and Computer Applications. 2016. Vol. 50. P. 24–45.

11. Ray A., Varna A. L. Distributed network anomaly detection: A survey. ACM Computing Surveys. 2020. Vol. 53(1). P. 1–43.

12. SNMP: розуміння простого протоколу управління мережею. URL: https://www.kaseya.com/blog/2020/09/14/snmp-simple-network-managementprotocol/ (дата звернення: 21.11.2024).

13. Verma A., Kaushal R. A comprehensive survey on anomaly detection using machine learning techniques. IET Networks. 2019. Vol. 8(6). P. 326–340.

14. Wang Z., Lu J. Deep learning for network anomaly detection: A review. IEEE Communications Surveys & Tutorials. 2020. Vol. 22(3). P. 1516–1539.

15. Абакумова А.О. Методи моніторингу та підвищення якості надання послуг у мережах стільникового зв'язку: дисертація на здобуття наукового ступеня кандидата технічних наук. Національний авіаційний університет, 2021. URL: https://vchenarada.nau.edu.ua/wp-content/uploads/2021/12/Anotatsiya-disertatsiyi-Abakumovoyi-A.O..pdf (дата звернення: 11.12.2024).

16. Аналіз існуючих систем моніторингу. URL: https://documentbase.net/744175/ (дата звернення: 21.11.2024).

17. Використання засобів дистанційної освіти для підвищення ефективності навчального процесу. Матеріали конференції ТНТУ, 2016. URL: https://elartu.tntu.edu.ua/bitstream/123456789/17337/1/konferencija_.pdf (дата звернення: 04.11.2024).

18. Віддалений моніторинг: можливості та особливості впровадження. URL: https://worldvision.com.ua/articles/udalenniy-monitoring-vozmozhnosti-i-osobennosti-vnedreniya (дата звернення: 21.11.2024).

19. Грішнова О.А. Чинники, що впливають на ефективність роботи в умовах дистанційної зайнятості. Журнал "Теоретичні та прикладні питання економіки", 2022, вип. 44, с. 45-56. URL: https://tppe.econom.univ.kiev.ua/data/2022_44/zb44_04.pdf (дата звернення: 18.11.2024).

20. Загальна характеристика роботи. Український державний університет залізничного транспорту, 2020. URL: https://kart.edu.ua/wp-content/uploads/2020/12/aref-nikitin.pdf (дата звернення: 11.08.2024).

21. Засоби моніторингу IT-інфраструктури. URL: https://www.osp.ru/os/2015/04/13047967 (дата звернення: 15.11.2024).

22. Кардаш І.А. Методи підвищення ефективності та моніторингу роботи локальної комп'ютерної мережі: кваліфікаційна робота магістра. Тернопільський національний технічний університет імені Івана Пулюя, 2023. URL: https://elartu.tntu.edu.ua/bitstream/lib/43292/2/Ivan%20Anatoliyovych_Kardash.pdf (дата звернення: 03.10.2024).

23. Класифікація засобів моніторингу та аналізу. URL: https://wiki.cuspu.edu.ua/index.php/Класифікація_засобів_моніторингу_та_аналізу (дата звернення: 17.11.2024).

24. Ковшуненко Є. Дослідження протоколів бездротових мереж та їх масштабованості: кваліфікаційна робота бакалавра. Державний університет інформаційно-комунікаційних технологій, 2024. URL: https://duikt.edu.ua/repozitorii/ki/2024/бак/Ковшуненко_КІД_42_Кваліфікаційна_робота.pdf (дата звернення: 07.10.2024).

25. Марнерідес А., Пезарос Д., Хатчісон Д. Огляд інструментів моніторингу. IEEE Communications Surveys & Tutorials. 2014. Vol. 16(4). P. 2029–2055.

26. Мейдан Ю., Матов Ю., Богадана М., Шабтай А., Очоа М., Гварнізо Х. К. Виявлення атак на пристрої Інтернету. IEEE Transactions on Information Forensics and Security. 2017. Vol. 12(3). P. 528–539.

27. Методи підвищення ефективності протоколів маршрутизації для бездротових мереж автомобільного транспорту. Державний університет інформаційно-комунікаційних технологій, 2021. URL: https://duikt.edu.ua/uploads/p_2101_48039809.pdf (дата звернення: 18.11.2024).

28. Мороз Є. С. Моніторинг мереж. Ukrainian Information Security Research Journal. 2007. URL: https://doi.org/10.18372/2410-7840.9.4151 (дата звернення: 21.10.2024).

29. Нікітін С.О. Методи підвищення якості надання інфокомунікаційних послуг у безпроводових телекомунікаційних мережах: дисертація на здобуття наукового ступеня кандидата технічних наук. Український державний університет залізничного транспорту, 2020. URL: https://lib.kart.edu.ua/bitstream/123456789/3362/1/dis_Nikitin.pdf (дата звернення: 03.10.2024).

30. Поплавський Д.В. Дослідження методів оптимізації гібридних мереж: кваліфікаційна робота магістра. Державний університет інформаційно-комунікаційних технологій, 2024. URL: https://duikt.edu.ua/repozitorii/ki/2024/Диплом%20магістр%20Поплавський%20Д.В..pdf (дата звернення: 11.09.2024).

31. Простий протокол управління мережею (SNMP). URL: https://searchnetworking.techtarget.com/definition/SNMP (дата звернення: 21.11.2024).

32. Сагайдак В.А. Методи підвищення ефективності виявлення шахрайства на основі аналізу мережевого трафіку: дисертація на здобуття наукового ступеня кандидата технічних наук. Харківський національний університет радіоелектроніки, 2018. URL: https://www.uacademic.info/ua/document/0824U002803 (дата звернення: 18.04.2024).

33. Система моніторингу IT-інфраструктури. URL: https://cutt.ly/9kcnQc5 (дата звернення: 21.10.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДУІКТ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ



Презентація по кваліфікаційній роботі

на тему: «Метод підвищення ефективності моніторингу процесу дистанційної роботи на основі безпроводових мереж»

Виконав: Олексій МАРТИНЮК

Керівник: Назарій БЛАЖЕННИЙ
доктор філософії

Мета роботи

Метою кваліфікаційної роботи розробка та впровадження методів підвищення ефективності моніторингу процесу дистанційної роботи на основі бездротових мереж.

Об'єктом дослідження є процес моніторингу бездротових мереж, що забезпечують дистанційну роботу.

Предметом дослідження методи та технології підвищення ефективності моніторингу процесу дистанційної роботи на основі бездротових мереж.

Існуючі системи моніторингу дистанційної роботи

Категорія систем	Опис	Популярні рішення
1. Трекери часу та продуктивності	Фіксують час роботи, аналізують продуктивність завдань.	Toggl Track - ручне вимкнення/вимкнення таймера, аналітичні звіти. RescueTime - автоматичний аналіз дій. Clockify - трекінг часу з практично налаштуваннями.
2. Програмне забезпечення моніторингу активності	Відстежують активність, веб-сайти, використані програми та рівень роботи.	Time Doctor - фіксація сайтів та скриншоти. Hubstaff - активність та візуальними звітами. ActivTrak - аналітика активності та візуалізація робочих процесів.
3. Інструменти для комунікації та управління завданнями	Спрямовують розподіл завдань, контролю виконання та прозорості робочих процесів.	Asana - розподіл та відстеження завдань. Trello - візуальне управління завданнями. Jira - контроль проектів, популярний серед IT-команд.
4. Програмне забезпечення для автоматичного збору звітів	Генерують автоматизовані звіти та аналізують продуктивність на основі даних.	Workpuls - реальний час моніторингу та звіти. Teramind - аналітика ресурсів та виявлення порушень політики.
5. Системи на основі штучного інтелекту	Використовують алгоритми для аналізу даних та оптимізації робочого процесу.	SentryPC - машинне навчання для аналізу активності. Controlio - AI-аналіз поведінки та оптимізація роботи.

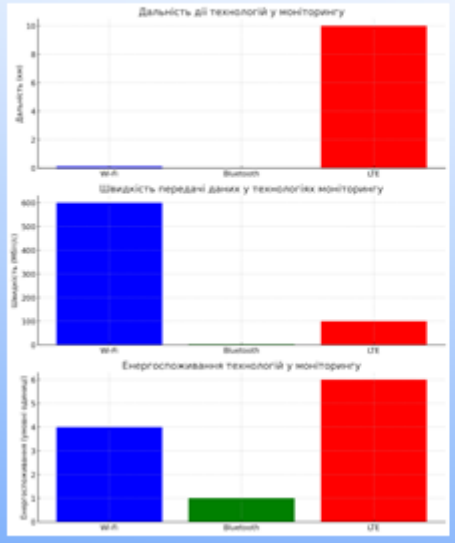
Основні елементи моніторингу бездротових мереж



Моніторинг віддалених процесів

Категорія	Проблема	Деталі
Безпека та конфіденційність	Ризик кібератак і витоку даних	Використання VPN, шифрування даних, двофакторна аутентифікація
	Конфіденційність працівників	Чітке визначення, що саме моніториться, та як використовуються дані
Технічні обмеження	Проблеми з доступом до інтернету	Нестабільне з'єднання впливає на продуктивність та точність даних
	Обмеження програмного забезпечення	Деякі програми мають обмеження на віддалене використання
Складність оцінки продуктивності	Неможливість повної об'єктивності	Потрібні додаткові показники, як-от виконані завдання та якість роботи
	Невизначеність ефективності моніторингу	Мікроменеджмент знижує мотивацію працівників
Комунікація та координація	Відсутність особистого контакту	Брак комунікації ускладнює координацію завдань та обмін інформацією
	Різниця в часових поясах	Узгодження робочого часу для глобальних команд
Висока вартість та інструменти	Фінансові витрати на програмне забезпечення	Вартість впровадження та обслуговування програмного забезпечення
	Навчання працівників	Витрати на навчання персоналу для роботи з інструментами
Психологічні аспекти	Виникнення стресу та тривоги	Надмірний контроль викликає стрес та тривогу
	Зниження рівня довіри	Моніторинг створює відчуття недовіри та знижує мотивацію
Дотримання законодавства	Відповідність законодавству про конфіденційність	Дотримання законів, як-от GDPR, щодо захисту персональних даних
	Врахування прав працівників	Дотримання прав працівників у різних юрисдикціях

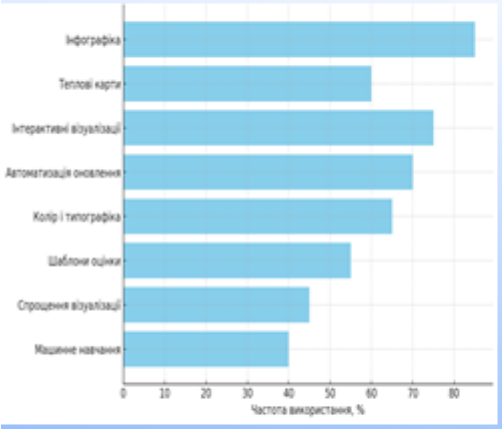
Енергоспоживання технологій у моніторингу



Порівняльна таблиця використання технологій у моніторингу

Технологія	Зона покриття	Швидкість передачі даних	Енергоспоживання	Вартість	Основні сценарії використання
Wi-Fi	Коротка - середня	Висока	Середнє	Низька (зі межами мереж)	В офісах, для пристроїв IoT
Bluetooth	Коротка	Низька	Низьке	Низька	Носимі гаджети, внутрішній моніторинг
LTE (4G/5G)	Велика (місто, регіон)	Висока (особливо 5G)	Високе	Висока	Віддалений моніторинг, GPS-трекінг

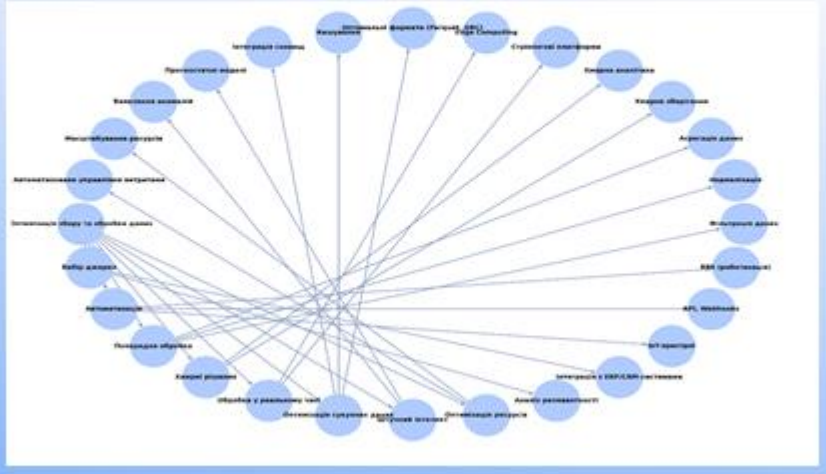
Методи підвищення моніторингу



№	Метод	Основні інструменти та підходи
1	Вибір джерел даних	Аналіз релевантності, інтеграція з CRM, ERP-системами
2	Автоматизація збору даних	IoT-пристрої, сенсори, API, Webhooks, RPA
3	Хмарні рішення	Хмарне зберігання (AWS, Google Cloud), аналітичні платформи
4	Попередня обробка даних	Фільтрація, очищення, нормалізація, агрегування
5	Обробка даних у реальному часі	Стрімінгові платформи (Apache Kafka, Flink), Edge Computing
6	Оптимізація сукупних даних	Формати (Parquet, ORC), інтеграція сховищ, кешування
7	Штучний інтелект і машинне навчання	Аналітика, прогностичні моделі, автоматичне виявлення аномалій
8	Оптимізація витрат і ресурсів	Масштабування ресурсів, автоматизоване управління ресурсами

Ключові методи оптимізації збору та обробки даних

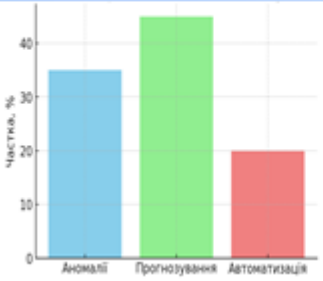
Оптимізація збору та обробки даних



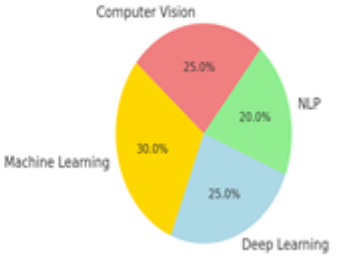
Ключові аспекти використання хмарних технологій для Big Data

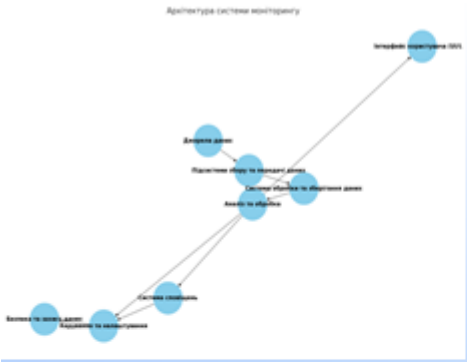
Категорія	Опис	Інструменти/Рішення
Переваги хмарних технологій	Масштабованість, зниження витрат, доступність, інтеграція інструментів	Amazon AWS, Google Cloud Platform, Microsoft Azure
Хмарні платформи	Надають послуги для зберігання, обробки та аналітики великих даних	Amazon S3, Google BigQuery, Azure Synapse Analytics
Процес інтеграції Big Data	Міграція даних, налаштування сховищ, автоматизація процесів	Apache Airflow, Amazon Snowball, Data Lake
Обробка потоків даних	Обробка в реальному часі для моніторингу та аналітики	Apache Kafka, Amazon Kinesis, Edge Computing
Машинне навчання та аналітика	Впровадження ML/AI для прогнозування, аналізу трендів та автоматичного виявлення аномалій	Amazon SageMaker, Google AI Platform, Azure ML
Безпека даних	Шифрування, контроль доступу, резервне копіювання	Керування доступом, резервне копіювання на хмарних платформах
Оптимізація витрат	Масштабування ресурсів на вимогу, контроль споживання ресурсів	Моніторинг витрат на AWS Cost Explorer, Google Cloud Billing

Розподіл використання ШІ для аналізу даних моніторингу



Інструменти ШІ для аналізу даних моніторингу





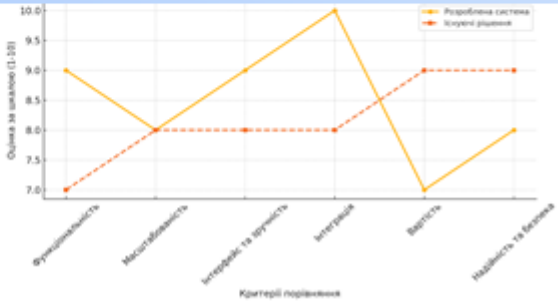
Хмарні платформи та процеси

Категорія	Приклад/Опис
Хмарні платформи	Amazon Web Services (AWS): Зберігання даних у S3, обробка через EC2 або AWS Lambda, бази даних RDS.
Хмарні платформи	Google Cloud Platform (GCP): Зберігання даних через Google Cloud Storage, обробка через Google BigQuery.
Безпека та управління доступом	Шифрування та захист даних: Алгоритми AES для збереження даних, протоколи SSL/TLS для захисту переданих даних.
Безпека та управління доступом	Управління доступом і аутентифікація: OAuth, LDAP, Active Directory для контролю доступу до даних.
Автоматизація та моніторинг процесів	Інструменти для автоматизації процесів: Apache Airflow для автоматизації робочих процесів.
Автоматизація та моніторинг процесів	Інструменти для автоматизації процесів: Cron Jobs для запуску завдань за розкладом у Unix-подібних системах.

Етапи тестування та оцінки ефективності системи моніторингу



Графічна структура переваг розробленої системи



Висновки

Проведене дослідження показало, що розробка системи моніторингу бездротових мереж може суттєво підвищити рівень безпеки та ефективності управління мережами. З використанням сучасних технологій, таких як машинне навчання, хмарні рішення та протоколи моніторингу, система здатна швидко виявляти аномалії, автоматично реагувати на інциденти та знижувати ризики.

Архітектура системи, яка включає різні рівні збору, обробки, зберігання та оповіщення, забезпечує комплексний підхід до моніторингу, що дозволяє ефективно управляти ресурсами та даними. Оцінка економічної ефективності впровадження системи свідчить про значні вигоди, які можуть бути отримані внаслідок її використання.

Перспективи подальших досліджень у сфері моніторингу бездротових мереж охоплюють вдосконалення алгоритмів аналізу даних, інтеграцію нових технологій, таких як блокчейн для підвищення безпеки, а також розвиток методів виявлення та реагування на нові загрози.
Крім того, важливо продовжити дослідження у сфері економічної ефективності та ROI (повернення інвестицій) для підприємств, які впроваджують подібні системи. Подальші дослідження також можуть зосередитися на дослідженні взаємодії між різними компонентами системи та вдосконаленні механізмів оповіщення, щоб підвищити зручність користування для адміністраторів та забезпечити максимально ефективну реакцію на інциденти.

Таким чином, розвиток та вдосконалення систем моніторингу бездротових мереж є надзвичайно актуальними завданнями, які потребують подальшого дослідження та реалізації інноваційних рішень.

Дякую за увагу!

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Олексій Мартинюк

Назва: Методи підвищення ефективності моніторингу процесу дистанційної роботи на основі бездротових мереж

Координатор: Назарій Блаженний

Підрозділ: ННІТ

Коефіцієнт подібності 1:1.2

Коефіцієнт подібності 2:0

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*