

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ

**КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ**

**КВАЛІФІКАЦІЙНА РОБОТА
на тему: «СИСТЕМНИЙ МОНІТОРИНГ КОМП'ЮТЕРА»**

Здобувача вищої освіти другого (магістерського) рівня, II курсу, групи КМІ-23-1,
спеціальності 122 «Комп'ютерні науки»
освітньо-професійна програма «Інформаційні управляючі системи і технології в економіці»


(підпис)

Терещенка Олександра Павловича
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Погореловська Ірина Дем'янівна
(прізвище, ім'я, по батькові)

Керівник освітньо-професійної програми


(підпис)

Горбовий Артур Юліанович,
д.т.н., професор
(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

Допущено до захисту за рішенням кафедри
теорії та історії держави і права протокол від «10» січня 2025 №11


(підпис)

Завідувач кафедри

Філоненко Михайло Миколайович,
к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене
звання)

Ірпінь – 2025

Ресстрація № 18

27.01.2025
(дата)


(підпис відповідальної особи)

Результати перевірки

до захисту
(до захисту, на доопрацювання)

24.01.2025
(дата)


(підпис)

Результати захисту

4 (добре)
(оцінка)

06.02.2025
(дата)


(підпис)

Голова комісії:


(підпис)

В.М. Франчук
(ініціали прізвище)

Члени комісії:


(підпис)

А.Ю. Горбовий
(ініціали прізвище)

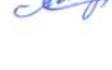

(підпис)

М.М. Філоненко
(ініціали прізвище)


(підпис)

І.Д. Погореловська
(ініціали прізвище)

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст кваліфікаційної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	25		<div style="text-align: right;">06.02.2025</div> <div>Франчук В.М. </div> <div>Горбовий А.Ю. </div> <div>Філоненко М.М. </div> <div>Погорєловська І.Д. </div> <div>Суховерхівка Л.П. </div>
2. Дотримання вимог щодо оформлення	від 0 до 10	7		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	40		

Оцінювання кваліфікаційної роботи науковим керівником - 40 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
80	B	4 (добре)	06.02.2025	<div>Франчук В.М. </div> <div>Горбовий А.Ю. </div> <div>Філоненко М.М. </div> <div>Погорєловська І.Д. </div> <div>Суховерхівка Л.П. </div>

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій

Кафедра комп'ютерних та інформаційних технологій і систем

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітня програма: «Інформаційні управляючі системи та технології в економіці»

Затверджую
Завідувача кафедри
Філоненко М. М.
«23» грудня 2023р.

**Завдання на кваліфікаційну роботу
здобувачу вищої освіти**

Терещенко Олександр Павловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи : **«Системний моніторинг комп'ютера»**

Затверджена наказом ректора від «20» грудня 2023 р. № 1701

2. Строк здачі закінченої роботи: «07» січня 2025р.

3. Мета роботи: визначення ефективних способів та засобів здійснення системного моніторингу стану функціонування комп'ютера.

Об'єкт дослідження: процеси моніторингу комп'ютерних систем, як явище, що визначає проблеми ефективності, своєчасності виявлення збоїв та оптимізації ресурсів.

Предмет дослідження: функціональність програмно-технічних засобів, що забезпечують моніторинг комп'ютерних систем.

4. Вихідні дані до роботи: програмно-технічні засоби моніторингу комп'ютерних систем та критерії їх оцінювання

5. Перелік графічного матеріалу: рисунки та таблиці в тексті роботи.

6. Зміст випускної кваліфікаційної (дипломної) роботи (перелік питань за кожним розділом): Розділ 1. Загальний аналіз систем та методів моніторингу.

1.1. Системи моніторингу та їх компоненти. 1.2. Класифікація систем моніторингу. Архітектура систем моніторингу. 1.3. Методи збору, аналізу та візуалізації даних моніторингу. 1.4. Проблеми, обмеження та безпекові виклики систем моніторингу. Розділ 2. Моніторинг комп'ютерних систем: практичний аспект, критерії оцінки ефективності. 2.1. Огляд провідних систем моніторингу. 2.2. Критерії оцінки ефективності систем моніторингу. 2.3. Порівняльний аналіз систем моніторингу. Розділ 3. Пропозиції щодо удосконалення та перспективи розвитку.

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури ДР	До 16.11.2023 р.	« 08 » 12 2023
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26.03. 2024 р.	« 26 » 03 2024
3	II розділ (аналіз експериментальної частини про і методики досліджень)	20. 06.2024 р.	« 20 » 06 2024
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проєктні рішення)	15.10.2024 р.	« 15 » 10 2024
5	Висновки	20.11.2024 р.	« 20 » 11 2024
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	20.01.2025 р.	« 20 » 01 2025
7	Отримання відгуку керівника	25.01.2025 р.	« 25 » 01 2025
8	Отримання зовнішньої рецензії	27.01.2025р.	« 27 » 01 2025

Дата видачі завдання «23» грудня 2023 р.

Керівник дипломної роботи


(підпис)

Погореловська І.Д.

Керівник освітньо-професійної програми


(підпис)

Горбовий А. Ю.

Завдання до виконання отримав
здобувач
вищої освіти


(підпис)

Терещенко О.П.

АНОТАЦІЯ

на тему: «СИСТЕМНИЙ МОНІТОРИНГ КОМП'ЮТЕРА»

Мета роботи: визначення ефективних способів та засобів здійснення системного моніторингу стану функціонування комп'ютера.

Завдання роботи:

- 1) дослідити компоненти систем моніторингу, їх взаємодію та функції;
- 2) проаналізувати архітектуру систем моніторингу, порівняти їх переваги та недоліки;
- 3) виконати порівняльний аналіз функціональності систем моніторингу (Zabbix, Nagios, RTG Network Monitor, SolarWinds.);
- 4) дослідити перспективи розвитку систем моніторингу з урахуванням сучасних тенденцій розвитку інформаційних технологій.

Предмет дослідження: функціональність програмно-технічних засобів, що забезпечують моніторинг комп'ютерних систем.

Об'єкт дослідження: процеси моніторингу комп'ютерних систем, як явище, що визначає проблеми ефективності, своєчасності виявлення збоїв та оптимізації ресурсів.

База для проведення дослідження: Товариство з обмеженою відповідальністю «ГРІН ЮКРЕЙН»

За результатами дослідження сформульовані висновки щодо важливості системного моніторингу для забезпечення стабільної, ефективної та безпечної роботи комп'ютерних систем та мереж; підтверджено, що системи моніторингу є критично важливими для забезпечення ефективної, безпечної та надійної роботи сучасних ІТ-інфраструктур.

Одержані результати можуть бути використані при визначенні оптимального програмного забезпечення для здійснення системного моніторингу комп'ютерів та/або комп'ютерних систем.

Дипломна робота містить: 56 сторінок, 7 таблиць, 6 рисунків, список використаних джерел складається з 49 найменувань.

Ключові слова: комп'ютер, системи моніторингу, класифікація систем моніторингу, архітектура систем моніторингу, ефективність, критерії оцінки ефективності.

Рік виконання кваліфікаційної роботи: 2023-2024 роки.

Рік захисту роботи: 2024 рік.

ANNOTATION

QUALIFICATION WORK on the topic: "SYSTEM MONITORING OF A COMPUTER"

Objective of the Study: Determining effective methods and tools for conducting systematic monitoring of computer operation.

Tasks of the Study:

- 1) To research the components of monitoring systems, their interactions, and functions.
- 2) To analyze the architecture of monitoring systems and compare their advantages and disadvantages.
- 3) To perform a comparative analysis of the functionality of monitoring systems (Zabbix, Nagios, RTG Network Monitor, SolarWinds).
- 4) To explore the prospects for the development of monitoring systems considering modern trends in information technology development.

Subject of the Study: Functionality of software and hardware tools that ensure the monitoring of computer systems.

Object of the Study: Processes of monitoring computer systems as a phenomenon that determines issues of efficiency, timely failure detection, and resource optimization.

Research Base: Limited Liability Company "GREEN UKRAINE."

Findings: The study formulated conclusions regarding the importance of systematic monitoring for ensuring stable, efficient, and secure operation of computer systems and networks. It confirmed that monitoring systems are critically important for ensuring the effective, secure, and reliable operation of modern IT infrastructures.

The obtained results can be used for determining optimal software solutions for performing systematic monitoring of computers and/or computer systems.

Thesis Composition: 56 pages, 7 tables, 6 figures, and a list of references consisting of 49 sources.

Keywords: Computer, monitoring systems, classification of monitoring systems, architecture of monitoring systems, efficiency, criteria for efficiency assessment.

Year of completion of the qualification work: 2023-2024.

Year of defense: 2024.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ЗАГАЛЬНИЙ АНАЛІЗ СИСТЕМ ТА МЕТОДІВ МОНІТОРИНГУ ...	6
1.1. Системи моніторингу та їх компоненти.	6
1.2. Класифікація систем моніторингу. Архітектура систем моніторингу.	9
1.3. Методи збору, аналізу та візуалізації даних моніторингу.	12
1.4. Проблеми, обмеження та безпекові виклики систем моніторингу.	18
РОЗДІЛ 2. МОНІТОРИНГ КОМП'ЮТЕРНИХ СИСТЕМ: ПРАКТИЧНИЙ АСПЕКТ, КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ.	22
2.1. Огляд провідних систем моніторингу.	22
2.2. Критерії оцінки ефективності систем моніторингу.	37
2.3. Порівняльний аналіз систем моніторингу.	39
РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ.	45
ВИСНОВКИ.	51
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.	53

ВСТУП

Актуальність теми кваліфікаційної роботи зумовлена кількома факторами:

- Зростання складності IT-інфраструктур, для яких є характерним складні розподілені архітектури, віртуалізація та використання хмарних технологій. Це ускладнює контроль за їх станом та вимагає використання ефективних систем моніторингу.

- Збільшення обсягів даних, які обробляються та передаються комп'ютерними системами, що створює додаткове навантаження та підвищує ризик виникнення збоїв.

- Зростання вимог бізнесових структур до продуктивності IT-систем, оскільки будь-які збої чи простої можуть призвести до значних фінансових втрат.

- Загрози інформаційній безпеці стають все більш складними та різноманітними. Системи моніторингу відіграють важливу роль у виявленні та запобіганні цим загрозам.

Отже, необхідність моніторингу стану функціонування комп'ютерних систем зумовлює пошук та дослідження методів, програмно-технічних засобів для його здійснення, що є актуальним у сучасних умовах розвитку та застосування інформаційних технологій.

Стан і ступінь розробки в науковій літературі. Питанням системного моніторингу присвячено значну кількість наукових досліджень в цій області, які охоплюють різні аспекти, включаючи методи збору та аналізу даних моніторингу, розробку архітектур систем моніторингу, використання штучного інтелекту для аналізу даних моніторингу, моніторинг окремих типів систем та додатків.

Американський дослідник та консультант у галузі DevOps Джин Кім у книзі "Фенікс Проект" підкреслює, що ефективний моніторинг є невід'ємною частиною успішної реалізації DevOps та забезпечення стабільної роботи IT-систем. Моніторинг дозволяє оперативно виявляти проблеми, запобігати збоям

та оптимізувати продуктивність, що є критично важливим для сучасного бізнесу [1]. Праці таких авторів, як А. Могіуддін (A.Mohyuddin) [2], М. Аббасі. (M. Abbasi) [3], та Бойкович З.. (Z. Bojkovic) [4], присвячені окремим протоколам та системам моніторингу. Питання використання машинного навчання для аналізу даних моніторингу розглядаються в роботах, опублікованих на конференціях з машинного навчання та аналізу даних (наприклад, ICML, KDD).

Однак, незважаючи на значний обсяг досліджень, питання удосконалення існуючих систем моніторингу та розробки нових методів моніторингу залишаються актуальними.

Мета дослідження: визначення ефективних способів та засобів здійснення системного моніторингу стану функціонування комп'ютера.

Для досягнення поставленої мети були визначені наступні завдання:

- дослідити компоненти систем моніторингу, їх взаємодію та функції;
- проаналізувати архітектуру систем моніторингу, порівняти їх переваги та недоліки;
- виконати порівняльний аналіз функціональності систем моніторингу (Zabbix, Nagios, RTG Network Monitor, SolarWinds);
- дослідити перспективи розвитку систем моніторингу з урахуванням сучасних тенденцій розвитку інформаційних технологій.

Об'єкт дослідження: процеси моніторингу комп'ютерних систем, як явище, що визначає проблеми ефективності, своєчасності виявлення збоїв та оптимізації ресурсів.

Предмет дослідження: функціональність програмно-технічних засобів, що забезпечують моніторинг комп'ютерних систем.

Методи дослідження: системний аналіз літератури за визначеною темою, що дозволив систематизувати існуючі знання щодо моніторингу комп'ютерних систем та їх застосування в контексті сонячних електростанцій. Порівняльний аналіз платформ проводився на основі визначених критеріїв, що охоплюють ключові аспекти моніторингу, такі як деталізація збору даних, аналітичні

можливості, інтеграція з обладнанням та інші. Емпіричні методи дослідження включали аналіз практичного досвіду використання систем моніторингу на реальних об'єктах енергетики - сонячних електростанціях різної потужності та конфігурації. Було проведено збір та аналіз даних про роботу систем моніторингу в умовах реальної експлуатації, що дозволило оцінити їхню ефективність та виявити особливості застосування. Для систематизації та візуалізації результатів дослідження використовувалися методи табличного представлення даних, що забезпечило наочність та зручність аналізу отриманих результатів. Комплексне застосування зазначених методів дозволило досягти об'єктивності та достовірності отриманих результатів, а також сформулювати обґрунтовані висновки щодо ефективності використання різних підходів до моніторингу комп'ютерних систем у контексті сонячних електростанцій.

База дослідження. Базою для проведення дослідження виступало Товариство з обмеженою відповідальністю «ГРІН ЮКРЕЙН» (ідентифікаційний код юридичної особи: 41029136), на якому проходила переддипломна практика автора роботи.

Науково-практична значимість одержаних результатів. Результати дослідження можуть бути використані при формуванні системи моніторингу комп'ютерних систем, в освітньому процесі при підготовці фахівців у галузі інформаційних технологій. Крім того, проведене теоретичне дослідження визначило напрями для подальшого вдосконалення існуючих підходів до моніторингу комп'ютерних систем.

Апробація результатів роботи. Результати роботи апробовано при проходженні практики у Товаристві з обмеженою відповідальністю «ГРІН ЮКРЕЙН» (ідентифікаційний код юридичної особи: 41029136) та на IV міжнародній науково-практичній Інтернет-конференції „Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції” (Дубляни, 16.05.2024), тези доповіді “Основні напрями здійснення моніторингу комп'ютерних систем” опубліковані у збірнику тез конференції [5].

РОЗДІЛ 1. ЗАГАЛЬНИЙ АНАЛІЗ СИСТЕМ ТА МЕТОДІВ МОНІТОРИНГУ

1.1. Системи моніторингу та їх компоненти.

Система моніторингу комп'ютера або комп'ютерної мережі – це комплекс апаратних та/або програмних засобів, призначений для безперервного спостереження за станом та працездатністю окремого комп'ютера, групи комп'ютерів або цілої мережі. Її головна мета полягає у своєчасному виявленні відхилень від нормального функціонування, збоїв, перевантажень, потенційних загроз безпеці та інших проблем, що можуть негативно вплинути на продуктивність, доступність та безпеку інформаційної системи. Моніторинг дозволяє не тільки оперативно реагувати на вже існуючі проблеми, але й прогнозувати їх виникнення, запобігаючи можливим збоям та простоям [2].

Функціональність системи моніторингу охоплює широкий спектр завдань. Вона збирає різноманітні дані про роботу системи, включаючи використання процесора, оперативної пам'яті, дискового простору, мережевий трафік, стан служб та процесів, журнали подій (логи) та багато іншого. Зібрана інформація аналізується для виявлення аномалій, порушень встановлених параметрів та інших відхилень від норми. Результати аналізу відображаються у зручному для користувача вигляді, наприклад, у вигляді графіків, діаграм, таблиць та дашбордів, що дозволяє швидко оцінити стан системи та виявити проблемні ділянки. У разі виявлення критичних подій система моніторингу генерує сповіщення (алерти) та інформує адміністраторів або відповідальних осіб за допомогою різних каналів зв'язку, таких як електронна пошта, SMS, повідомлення в месенджерах або спеціалізовані додатки [3].

Залежно від масштабу та призначення, системи моніторингу можуть відрізнятися за своєю складністю та функціональністю. Прості системи можуть обмежуватися моніторингом основних параметрів окремого комп'ютера, тоді як складні системи корпоративного рівня здатні контролювати великі розподілені мережі, що складаються з тисяч пристроїв. Вони можуть включати в себе

засоби для моніторингу продуктивності додатків, баз даних, веб-серверів, мережевого обладнання та інших компонентів IT-інфраструктури [4].

Важливою складовою сучасних систем моніторингу є інтеграція з іншими системами управління IT-інфраструктурою, такими як системи управління конфігураціями, системи управління інцидентами та системи управління безпекою. Це дозволяє створити єдиний центр управління IT-інфраструктурою та забезпечити комплексну автоматизацію процесів управління, моніторингу та реагування на інциденти [4].

Крім того, сучасні системи моніторингу все частіше використовують технології штучного інтелекту (ШІ) та машинного навчання (ML) для аналізу даних, прогнозування проблем та автоматизації процесів. Алгоритми ML дозволяють виявляти складні залежності в даних, прогнозувати пікові навантаження та інші потенційні проблеми, що дозволяє завчасно вживати заходів для їх запобігання. ШІ також може бути використаний для автоматичної кореляції подій з різних джерел, що спрощує діагностику складних проблем та скорочує час на їх вирішення [6].

Основними компонентами типової система моніторингу є агенти моніторингу, сервер моніторингу, база даних моніторингу та інтерфейс користувача. Агенти моніторингу – це програмні компоненти, що встановлюються безпосередньо на об'єкти моніторингу (сервери, мережеві пристрої, віртуальні машини, додатки тощо) та відповідають за збір даних про їхній стан. Існують різні типи агентів, що відрізняються за функціональністю та методами збору даних. Деякі агенти збирають базові метрики, такі як завантаження ЦП, використання пам'яті та дискового простору, тоді як інші можуть збирати більш специфічні дані, наприклад, метрики продуктивності баз даних або веб-серверів. Методи збору даних також можуть різнитися: агенти можуть періодично опитувати об'єкти моніторингу (polling), отримувати дані у вигляді подій або логів (trapping/logging), або використовувати комбінацію обох методів. Важливим аспектом є поділ на агентний та безагентний моніторинг. Агентний моніторинг передбачає встановлення спеціального програмного

забезпечення (агента) на кожний об'єкт, що підлягає моніторингу. Безагентний моніторинг, навпаки, використовує існуючі протоколи та служби (наприклад, SNMP, WMI, SSH) для збору інформації без встановлення додаткового програмного забезпечення на цільових системах [5].

Сервер моніторингу є центральним компонентом системи, який отримує дані від агентів, обробляє їх, зберігає в базі даних та надає інтерфейс для користувачів. Функції сервера включають:

- збір даних – тримання даних від агентів за допомогою різних протоколів (наприклад, HTTP, SNMP, TCP);
- обробка даних – агрегація, фільтрація, нормалізація та аналіз отриманих даних;
- зберігання даних – запис даних у базу даних моніторингу;
- генерація сповіщень – відправлення повідомлень про події, що вимагають уваги (наприклад, перевищення порогових значень метрик);
- надання інтерфейсу користувача – забезпечення доступу до даних моніторингу через веб-інтерфейс, API або інші методи [7].

Методи обробки даних на сервері можуть включати статистичний аналіз, аналіз трендів, кореляційний аналіз та методи машинного навчання. Для зберігання даних можуть використовуватись різні бази даних, як реляційні (наприклад, MySQL, PostgreSQL), так і NoSQL (наприклад, TimeScaleDB, InfluxDB) [8].

База даних моніторингу призначена для зберігання великих обсягів даних, що збираються системою моніторингу. Вибір моделі даних та вимоги до зберігання даних залежать від специфіки системи та типу даних, що збираються. Зазвичай використовуються часові ряди (time series), оскільки дані моніторингу мають часову прив'язку. Важливими вимогами до бази даних є:

- Висока швидкість запису. Дані моніторингу генеруються постійно та у великих обсягах, тому база даних повинна забезпечувати швидкий запис даних.
- Масштабованість. База даних повинна мати можливість масштабуватися для зберігання зростаючих обсягів даних.

- Надійність. Забезпечення збереження даних та запобігання їх втраті.

Інтерфейс користувача надає доступ до даних моніторингу та інструменти для їх візуалізації та аналізу. Існують різні типи інтерфейсів, такі як веб-інтерфейси, консольні інтерфейси та API. Веб-інтерфейси є найбільш поширеними та надають графічне відображення даних у вигляді графіків, діаграм та дашбордів. API дозволяють інтегрувати систему моніторингу з іншими системами. Детальніше питання візуалізації даних моніторингу розглянута у наступному підрозділі [9].

1.2. Класифікація систем моніторингу. Архітектура систем моніторингу.

Системи моніторингу комп'ютерів відіграють ключову роль у забезпеченні стабільної та ефективної роботи ІТ-інфраструктури. Для кращого розуміння їх різноманітності та можливостей, системи моніторингу розмежовані за кількома критеріями: функціональністю, рівнем моніторингу та архітектурою.

За функціональністю системи моніторингу розподілені на кілька основних типів:

- Моніторинг продуктивності: фокусується на зборі та аналізі показників продуктивності комп'ютерної системи, таких як завантаження ЦП, використання пам'яті, дисковий ввід-вивід, мережевий трафік. Він дозволяє виявляти вузькі місця в системі та оптимізувати її роботу. (Наприклад, Zabbix, Nagios).

- Моніторинг доступності: перевіряє доступність сервісів та додатків, таких як веб-сервери, бази даних, поштові сервери. Він дозволяє своєчасно виявляти збої та відновлювати роботу сервісів. (Наприклад, Pingdom, Uptime Robot).

- Моніторинг безпеки: відстежує події безпеки, такі як спроби несанкціонованого доступу, вірусні атаки, вторгнення. Він дозволяє своєчасно реагувати на загрози та захищати систему від атак. Наприклад, Security Onion, OSSEC.

- Моніторинг журналів (логів): забезпечує збір та аналіз журналу подій операційної системи та додатків. Він дозволяє виявляти проблеми, аналізувати причини збоїв та проводити аудит безпеки. Наприклад, ELK stack (Elasticsearch, Logstash, Kibana), Splunk.

- Моніторинг користувацької активності: відстежує дії користувачів на комп'ютері, такі як запуск програм, відвідування веб-сайтів, використання файлів. Він може використовуватися для контролю за роботою співробітників, виявлення інсайдерських загроз та аналізу поведінки користувачів. Наприклад, Teramind, ActivTrak [10].

За рівнем моніторингу системи розподілені на:

- Моніторинг на рівні хоста: відстежує ресурси та процеси на окремому комп'ютері (хості). Наприклад, вбудовані засоби Windows Performance Monitor або Linux top.

- Моніторинг на рівні мережі: відстежує трафік, доступність мережевих пристроїв та сервісів. Наприклад, Zabbix, Nagios, PRTG.

- Моніторинг на рівні додатків: фокусується на окремих додатках та відстежує їх продуктивність, доступність та помилки. Наприклад, New Relic, AppDynamics.

- Моніторинг на рівні бізнес-процесів: відстежує виконання бізнес-процесів, які залежать від роботи кількох комп'ютерних систем та додатків. Він дозволяє оцінити вплив IT-інфраструктури на бізнес [11].

Архітектура системи моніторингу визначає структуру та взаємодію її компонентів, впливаючи на ефективність, масштабованість та відмовостійкість.

Централізована архітектура передбачає збір та обробку всіх даних моніторингу на одному центральному сервері. Агенти, встановлені на об'єктах моніторингу, надсилають дані безпосередньо на цей сервер. Така архітектура відрізняється простотою розгортання та адміністрування, забезпечуючи централізоване управління та консолідований збір даних для спрощеного аналізу. Однак, централізована архітектура є вразливою до єдиної точки відмови: вихід з ладу центрального сервера призводить до зупинки всієї

системи моніторингу. Крім того, масштабування такої системи обмежене: зі збільшенням кількості об'єктів моніторингу навантаження на центральний сервер зростає, що може призвести до зниження продуктивності. Також, значні обсяги даних, що передаються на центральний сервер, можуть перевантажувати мережу. Прикладом централізованої архітектури може слугувати базова конфігурація Nagios Core або Zabbix з одним сервером [12].

У децентралізованій архітектурі збір та обробка даних здійснюються на кількох незалежних серверах моніторингу, кожен з яких відповідає за певну частину інфраструктури. Ці сервери можуть обмінюватися даними між собою, але центральний координуючий вузол відсутній. Децентралізація забезпечує підвищену відмовостійкість: вихід з ладу одного сервера не призводить до зупинки всієї системи. Також, навантаження розподіляється між кількома серверами, покращуючи масштабованість, а локальна обробка даних зменшує навантаження на мережу. Однак, адміністрування децентралізованої системи складніше, оскільки потрібно керувати кількома серверами. Консолідація даних, що зберігаються на різних серверах, також ускладнюється, а для забезпечення узгодженості інформації необхідна синхронізація даних між серверами. Прикладом децентралізованої архітектури є використання проксі-серверів або розподілених колекторів даних в системах моніторингу, зокрема Zabbix з використанням проксі [13].

Розподілена архітектура поєднує елементи централізованої та децентралізованої, забезпечуючи збір та обробку даних на кількох серверах, які працюють як єдина система під управлінням центрального координуючого вузла. Цей вузол керує роботою серверів та забезпечує консолідацію даних. Така архітектура характеризується високою відмовостійкістю: вихід з ладу окремих серверів не зупиняє роботу всієї системи. Вона також відмінно масштабується шляхом додавання нових серверів та ефективно обробляє великі обсяги даних завдяки їх розподілу між серверами для паралельної обробки. Розподілена архітектура поєднує централізоване управління з розподіленою обробкою. Однак, розгортання та адміністрування розподіленої системи є

найбільш складним, вимагаючи ретельного налаштування та підтримки. Для ефективної роботи потрібна надійна та швидка мережева інфраструктура. Прикладами розподілених архітектур є Prometheus з використанням federated setup та деякі конфігурації Elasticsearch для моніторингу логів [14].

Результати порівняння архітектур систем моніторингу зведено у табл.1.1.

Таблиця 1.1.

Порівняння архітектур систем моніторингу

Характеристика	Централізована	Децентралізована	Розподілена
Простота розгортання	Проста	Середня	Складна
Простота адміністрування	Найпростіша	Складна	Складна
Відмовостійкість	Низька (єдина точка відмови)	Середня	Висока
Масштабованість	Низька	Середня	Висока
Навантаження на мережу	Високе (особливо при великій кількості даних)	Середнє	Низьке (завдяки розподіленій обробці)
Вартість	Низька (один сервер)	Середня (кілька серверів)	Висока (багато серверів, складна інфраструктура)
Консолідація даних	Проста	Складна	Проста (завдяки центральній координації)

Джерело: виконано автором самостійно на основі [12], [13], [14].

Вибір архітектури залежить від багатьох факторів, включаючи розмір інфраструктури, вимоги до відмовостійкості та масштабованості, бюджет та доступні ресурси. Для невеликих інфраструктур з невеликою кількістю об'єктів моніторингу достатньо централізованої архітектури. Для великих та складних інфраструктур, що вимагають високої відмовостійкості та масштабованості, краще підходять децентралізовані або розподілені архітектури [15].

1.3. Методи збору, аналізу та візуалізації даних моніторингу.

Збір даних є фундаментальним етапом у роботі будь-якої системи моніторингу. Існує два основних підходи до збору даних: активний (polling) та пасивний (trapping/logging). Кожен з цих методів має свої особливості, переваги

та недоліки, які визначають його застосування в різних ситуаціях. Крім того, важливим аспектом є спосіб реалізації збору даних – з використанням агентів (агентний моніторинг) або без них (безагентний моніторинг).

Активний моніторинг, також відомий як polling, передбачає періодичне опитування об'єктів моніторингу з метою отримання інформації про їхній стан. Сервер моніторингу або спеціальний інструмент надсилає запит на об'єкт моніторингу, який у відповідь повертає необхідні дані. Частота опитування визначається налаштуваннями системи моніторингу. Активний моніторинг забезпечує контроль над частотою збору даних та дозволяє отримувати інформацію за запитом. Однак, він створює додаткове навантаження на мережу та об'єкти моніторингу, особливо при високій частоті опитування або великій кількості об'єктів. Прикладами протоколів, що використовуються для активного моніторингу, є SNMP (Simple Network Management Protocol) та WMI (Windows Management Instrumentation). SNMP широко використовується для моніторингу мережевих пристроїв (маршрутизатори, комутатори, сервери), дозволяючи отримувати інформацію про стан інтерфейсів, завантаження ЦП, використання пам'яті тощо. WMI є технологією Microsoft, яка дозволяє отримувати інформацію про стан операційної системи Windows та встановленого на ній програмного забезпечення [16].

Пасивний моніторинг, також відомий як trapping або logging, передбачає отримання даних у вигляді подій або логів, що генеруються об'єктами моніторингу. Об'єкт моніторингу самостійно генерує та відправляє повідомлення про певні події або зміни стану. Пасивний моніторинг мінімізує навантаження на мережу та об'єкти моніторингу, оскільки дані відправляються лише при виникненні подій. Однак, він залежить від налаштувань об'єктів моніторингу та не дозволяє отримувати інформацію за запитом. Прикладами технологій, що використовуються для пасивного моніторингу, є Syslog та Event Logs. Syslog є стандартом для передачі повідомлень про системні події в мережах TCP/IP. Він дозволяє збирати логи з різних джерел (сервери, мережеві пристрої, додатки) на центральному сервері. Event Logs є системою

журналювання подій в операційних системах Windows. Вони містять інформацію про системні події, події безпеки та події додатків [17].

Агентний моніторинг передбачає встановлення спеціального програмного забезпечення (агента) на кожний об'єкт, що підлягає моніторингу. Агент збирає дані локально та передає їх на сервер моніторингу. Безагентний моніторинг, навпаки, використовує існуючі протоколи та служби (наприклад, SNMP, WMI, SSH) для збору інформації без встановлення додаткового програмного забезпечення на цільових системах [18]. Інформація про відмінності між ними, наведена у порівняльній таблиці 1.2.

Таблиця 1.2.

Моніторинг: агентний та безагентний

Характеристика	Агентний моніторинг	Безагентний моніторинг
Встановлення ПЗ	Потрібне встановлення агента на кожний об'єкт моніторингу.	Не потребує встановлення додаткового ПЗ на об'єкти моніторингу.
Використання ресурсів	Може споживати ресурси об'єкта моніторингу (ЦП, пам'ять).	Менше навантаження на об'єкти моніторингу.
Збір даних	Можливість збору більш детальних та специфічних даних, недоступних через стандартні протоколи.	Обмежений збір даних стандартними протоколами.
Безпека	Потенційні ризики безпеки, пов'язані з встановленням та управлінням агентами. Потребує належного захисту з'єднання між агентом та сервером.	Менше ризиків, пов'язаних з встановленням додаткового ПЗ. Проте, потребує належної конфігурації та захисту використовуваних протоколів (SNMP, WMI, SSH).
Складність налаштування	Може бути складнішим у налаштуванні, особливо при великій кількості об'єктів моніторингу. Потребує управління версіями агентів.	Зазвичай простіше у налаштуванні.
Масштабованість	Може створювати додаткові складнощі при масштабуванні, пов'язані з управлінням агентами на великій кількості об'єктів.	Зазвичай краще масштабується, оскільки не потребує встановлення та управління агентами.
Приклади	Zabbix agent, Nagios NRPE, Datadog agent.	SNMP, WMI, SSH моніторинг.

Джерело: виконано автором самостійно на основі [16],[17],[18].

Вибір методу збору даних та підходу до моніторингу залежить від конкретних потреб та вимог. Активний моніторинг підходить для ситуацій, коли потрібен контроль над частотою збору даних та отримання інформації за запитом. Пасивний моніторинг є кращим вибором, коли необхідно мінімізувати навантаження на мережу та об'єкти моніторингу. Агентний моніторинг дозволяє збирати більш детальні дані, але може бути складнішим у налаштуванні та управлінні. Безагентний моніторинг простіший у налаштуванні, але має обмежені можливості збору даних. Часто в реальних системах моніторингу використовуються комбінації різних методів та підходів для досягнення оптимального результату.

Після розгляду методів збору даних, які дозволяють отримати первинну інформацію про стан системи, наступним важливим етапом є аналіз цих даних. Аналіз даних моніторингу є ключовим етапом, що дозволяє отримати корисну інформацію зі зібраних метрик та використовувати її для оптимізації роботи системи, виявлення проблем та прогнозування майбутніх тенденцій.

Застосування статистичного аналізу дозволяє отримати кількісні характеристики даних, такі як середнє значення, медіана, мода, стандартне відхилення, дисперсія, квартилі та інші. Ці показники дозволяють зрозуміти розподіл даних, їхню мінливість та центральну тенденцію. Наприклад, середнє значення завантаження ЦП за певний період часу може показати середній рівень використання процесора, а стандартне відхилення – ступінь його коливань. Статистичний аналіз також включає методи перевірки статистичних гіпотез, які дозволяють робити висновки про достовірність отриманих результатів. Наприклад, можна перевірити гіпотезу про те, чи є різниця між середнім часом відгуку сервера в різні дні тижня статистично значущою [19].

Кореляційний аналіз дозволяє визначити наявність та силу взаємозв'язку між різними метриками [20]. Наприклад, кореляційний аналіз може показати, чи існує зв'язок між завантаженням ЦП та часом відгуку сервера.

Аналіз трендів спрямований на виявлення та прогнозування змін у даних з часом. Для виявлення трендів використовуються різні методи, такі як

графічне відображення даних, методи згладжування (ковзна середня, експоненціальне згладжування) та методи регресійного аналізу. Методи згладжування усувають випадкові коливання даних, дозволяючи краще побачити основну тенденцію. [21].

Методи машинного навчання (ML) надають потужні інструменти для аналізу даних моніторингу, дозволяючи вирішувати складні завдання, такі як виявлення аномалій, прогнозування, класифікація та кластеризація.

- Виявлення аномалій. Методи ML, такі як One-Class SVM, Isolation Forest, Local Outlier Factor, дозволяють виявляти нетипові значення метрик, які можуть свідчити про проблеми в системі. Наприклад, раптове зростання трафіку або нетипове використання ресурсів може бути ідентифіковано як аномалія.

- Прогнозування. Методи ML, такі як лінійна регресія, часові ряди (ARIMA, Prophet), нейронні мережі, дозволяють прогнозувати майбутні значення метрик на основі історичних даних. Наприклад, можна спрогнозувати завантаження ЦП на наступний день або кількість запитів до веб-сервера на наступний тиждень.

- Класифікація. Методи ML, такі як дерева рішень, Random Forest, SVM, дозволяють класифікувати події або стани системи на основі набору ознак. Наприклад, можна класифікувати типи помилок, що виникають в додатку, на основі логів.

- Кластеризація. Методи ML, такі як k-means, DBSCAN, дозволяють групувати схожі об'єкти або події в кластери. Наприклад, можна виявити групи серверів зі схожими характеристиками продуктивності [22].

Використання ML для аналізу даних моніторингу дозволяє автоматизувати процес аналізу, виявляти складні залежності та робити більш точні прогнози. Застосування методів аналізу в задачах моніторингу наведені у табл. 1.3.

Таблиця 1.3.

Методи аналізу даних при моніторингу комп'ютерних систем

Метод аналізу	Завдання	Приклад застосування
Статистичний	Опис даних, перевірка гіпотез	Розрахунок середнього часу відгуку сервера, визначення відсотка помилок, порівняння продуктивності двох серверів.
Аналіз трендів	Виявлення та прогнозування змін з часом	Прогнозування завантаження мережі на наступний місяць, виявлення сезонних коливань трафіку.
Кореляційний	Визначення взаємозв'язків між метриками	Виявлення залежності між завантаженням ЦП та часом відгуку бази даних, визначення впливу кількості користувачів на завантаження веб-сервера.
Машинне навчання	Виявлення аномалій, прогнозування, класифікація	Виявлення нетипових запитів до веб-сервера, прогнозування кількості помилок в додатку, класифікація типів атак на мережу, кластеризація користувачів за поведінкою.

Джерело: виконано автором самостійно на основі [19], [20], [21], [22].

Застосування комбінації різних методів аналізу дозволяє отримати найбільш повну та об'єктивну картину стану системи та приймати обґрунтовані рішення щодо її оптимізації та розвитку.

Після того, як дані зібрано та проаналізовано, наступним критично важливим кроком є їх візуалізація. Аналіз, хоч і дозволяє виявити закономірності та тенденції, часто залишається складним для сприйняття без належного представлення. Візуалізація даних відіграє вирішальну роль у системах моніторингу, оскільки дозволяє швидко та ефективно сприймати великі обсяги інформації, виявляти тенденції, аномалії та інші важливі закономірності. Правильно підібрані методи візуалізації значно полегшують аналіз даних та прийняття обґрунтованих рішень [23].

Застосування різних методів візуалізації даних моніторингу дозволяє отримати повну та об'єктивну картину стану системи, швидко виявляти проблеми та приймати обґрунтовані рішення [24].

Ефективна система моніторингу потребує комплексного підходу до збору, аналізу та візуалізації даних. Правильний вибір методів на кожному етапі дозволяє отримати повну та об'єктивну картину стану системи, швидко

виявляти проблеми та приймати обґрунтовані рішення щодо її оптимізації та розвитку. Важливо враховувати специфіку системи, вимоги до точності та деталізації даних, а також доступні ресурси при виборі конкретних методів та інструментів.

1.4. Проблеми, обмеження та безпекові виклики систем моніторингу.

Незважаючи на значний прогрес у розвитку систем моніторингу, існуючі рішення все ще мають певні проблеми та обмеження, які необхідно враховувати при їх виборі та впровадженні.

Зі зростанням розміру IT-інфраструктури, кількість пристроїв та сервісів, що потребують моніторингу, також збільшується. Це може призвести до проблем з масштабуванням системи моніторингу. Централізовані системи можуть стати вузьким місцем, що призведе до зниження продуктивності та втрати даних. Розподілені системи, хоча й більш масштабовані, можуть бути складнішими у налаштуванні та управлінні. Що призводить до трьох основних проблем у даному напрямі:

- 1) збір та обробка великих обсягів даних з багатьох джерел може перевантажити сервери моніторингу;
- 2) збільшення кількості моніторингових агентів може призвести до збільшення мережевого трафіку;
- 3) складність координації та управління розподіленими компонентами системи моніторингу [25].

Деякі системи моніторингу, особливо ті, що пропонують широкий набір функцій, можуть бути складними у налаштуванні та конфігурації. Це може вимагати від адміністраторів значних знань та досвіду. Неправильне налаштування може призвести до неточних даних моніторингу або навіть до збоїв у роботі системи. Отже, за даним напрямом виділяються наступні проблеми:

- 1) велика кількість параметрів конфігурації;
- 2) недостатня документація або складність її розуміння;

Деякі системи моніторингу можуть не забезпечувати всі необхідні функції для моніторингу конкретних типів систем або додатків. Наприклад, система може не підтримувати моніторинг певних протоколів або технологій і як наслідок маємо проблеми з відсутністю підтримки необхідних метрик або методів збору даних; обмеженими можливостями візуалізації даних або створення звітів; відсутністю інтеграції з іншими системами управління IT-інфраструктурою [26].

У свою чергу, комерційні системи моніторингу можуть бути досить дорогими, особливо для великих організацій. Вартість може включати ліцензії на програмне забезпечення, вартість підтримки та навчання.

Окремо варто відзначити безпековий напрямок у питанні моніторингу комп'ютерних систем. Безпека є критично важливим аспектом для будь-якої системи, в тому числі системи моніторингу. Оскільки такі системи збирають та обробляють конфіденційну інформацію про стан інфраструктури, їх компрометація може призвести до серйозних наслідків, таких як витік даних, порушення роботи сервісів або навіть повний збій системи. Тому необхідно забезпечити належний рівень захисту даних моніторингу, захист від DoS-атак та ведення аудиту.

Захист даних моніторингу включає забезпечення конфіденційності, цілісності та доступності даних. Для цього застосовуються різні методи, зокрема шифрування та контроль доступу. Шифрування забезпечує конфіденційність даних шляхом перетворення їх у нечитабельний формат. Шифрування застосовується як під час передачі даних, так і під час їх зберігання. Для захисту даних під час передачі використовуються протоколи TLS/SSL, які шифрують з'єднання між агентами моніторингу та сервером, а також між сервером та клієнтами. Контроль доступу обмежує доступ до даних моніторингу лише авторизованим користувачам та системам. Він включає аутентифікацію, яка перевіряє ідентичність користувача (логін/пароль, багатофакторна аутентифікація), та авторизацію, яка визначає права доступу користувача до різних ресурсів системи моніторингу (перегляд даних, зміна

налаштувань, адміністрування). Для гнучкого управління правами доступу часто використовується рольова модель доступу (RBAC), яка призначає користувачам ролі з певними правами доступу [27].

DoS-атаки (Denial of Service) спрямовані на порушення доступності системи шляхом перевантаження її ресурсами (мережа, ЦП, пам'ять). Системи моніторингу, як і будь-які інші системи, можуть бути об'єктами DoS-атак. Для захисту від DoS-атак застосовуються різноманітні методи. Фільтрація трафіку, що реалізується за допомогою брандмауерів та систем виявлення/запобігання вторгненням (IDS/IPS), дозволяє відсіяти шкідливий трафік. Обмеження швидкості (Rate Limiting) обмежує кількість запитів з однієї IP-адреси або мережі, запобігаючи перевантаженню. Використання CDN (Content Delivery Network) розподіляє трафік між кількома серверами, зменшуючи навантаження на один сервер. Для захисту від DDoS-атак (Distributed Denial of Service) використовуються спеціалізовані сервіси, які здатні відфільтрувати великі обсяги шкідливого трафіку, що генерується з багатьох джерел. Моніторинг трафіку та виявлення аномалій дозволяє своєчасно ідентифікувати нетипову поведінку, яка може свідчити про DoS-атаку [28].

Аудит та журнали подій дозволяють відстежувати дії користувачів та системи, виявляти порушення безпеки та проводити розслідування інцидентів. Аудит передбачає реєстрацію всіх важливих подій в системі моніторингу, таких як вхід/вихід користувачів, зміна налаштувань системи, доступ до даних та генерування сповіщень. Інформація про ці події зберігається в журналах подій, які повинні бути захищені від несанкціонованого доступу та змін. Регулярний аналіз журналів дозволяє виявляти підозрілу активність та порушення безпеки. Для забезпечення цілісності журналів та запобігання їх підробці використовуються криптографічні методи. Взаємозв'язки між загрозами та заходами безпеки наведені у табл. 1.4.

Таблиця 1.4.

Загрози безпеки та заходи протидії

Загрози	Заходи безпеки
Несанкціонований доступ	Аутентифікація, авторизація, RBAC, шифрування даних на зберіганні та під час передачі.
Витік даних	Шифрування даних, контроль доступу, аудит.
DoS/DDoS-атаки	Фільтрація трафіку, обмеження швидкості, використання CDN, захист від DDoS-атак, моніторинг трафіку.
Підробка журналів подій	Криптографічні методи забезпечення цілісності журналів.
Компрометація агента	Шифрування з'єднання між агентом та сервером, автентифікація агента.

Джерело: виконано автором самостійно на основі [26],[27],[28].

Застосування цих методів та заходів безпеки дозволяє значно підвищити рівень захисту систем моніторингу та запобігти можливим негативним наслідкам. Важливо пам'ятати, що безпека – це безперервний процес, який потребує постійного моніторингу, аналізу та вдосконалення.

Наостанок зазначимо, що ці проблеми та обмеження не є універсальними для всіх систем моніторингу. Вибір конкретної системи повинен базуватися на ретельному аналізі потреб та вимог організації, а також на порівнянні доступних рішень.

РОЗДІЛ 2. МОНІТОРИНГ КОМП'ЮТЕРНИХ СИСТЕМ: ПРАКТИЧНИЙ АСПЕКТ, КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ

2.1. Огляд провідних систем моніторингу.

Засоби моніторингу за способом здійснення моніторингу прийнято розділяти на дві фундаментальні групи: засоби апаратного та засоби програмного моніторингу стану системи.

Апаратні в свою чергу поділяють на дві великі підгрупи: системні датчики (температури, напруги, освітленості та інші) та інструменти BIOS/UEFI. Останні включають інструменти системної діагностики – базові засоби моніторингу стану апаратних компонентів під час завантаження системи та «конфігуратори» – засоби налаштування параметрів роботи апаратного забезпечення для оптимальної продуктивності та стабільності.

Програмні засоби моніторингу, в свою чергу, поділяюся на вбудовані засоби операційних систем та спеціалізоване програмне забезпечення. До вбудованого відносяться такі засоби як: «Task Manager» для операційної системи «Windows»; «Activity Monitor» для пристроїв, що працюють на базі операційної системи «macOS»; «Linux» пропонує своїм користувачам інструмент під назвою «top, htop». Функціонал цих засобів подібний між собою та має спільну мету – забезпечення моніторингу стану комп'ютерної мережі та операційної системи, але дещо відрізняється між собою (табл. 2.1).

Таблиця 2.1.

Вбудовані програмні засоби моніторингу комп'ютерних мереж в популярних операційних система

Операційна система	Програмний засіб	Функціональні особливості
Windows	Task Manager	Відстеження використання ресурсів, процесів, продуктивності системи.
macOS	Activity Monitor	Моніторинг процесів, системної пам'яті, використання CPU та дискового простору.
Linux	top, htop	Інструменти командного рядка для моніторингу процесів і ресурсів у реальному часі.

Джерело: виконано автором самостійно.

Серед широкого спектру програмних рішень, призначених для моніторингу стану комп'ютерних систем та мереж, особливе місце займає система Zabbix. Цей програмний продукт являє собою потужний інструмент з відкритим вихідним кодом, що забезпечує комплексний моніторинг серверів, мережевих пристроїв, віртуальних машин та інших компонентів ІТ-інфраструктури в режимі реального часу (рис. 2.1.).

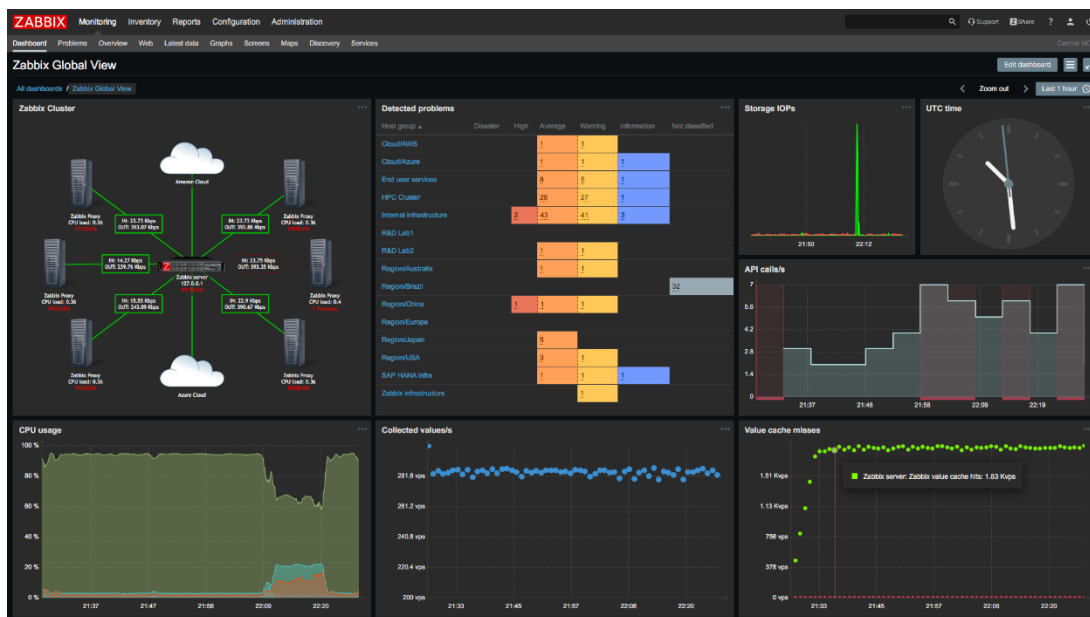


Рис. 2.1. Zabbix [29].

Функціональність Zabbix спрямована на забезпечення адміністраторів детальною інформацією щодо продуктивності та стану ІТ-ресурсів, що дозволяє здійснювати проактивне виявлення потенційних проблем до моменту їх негативного впливу на бізнес-процеси. Система надає можливість автоматичного сповіщення про критичні події, що сприяє оперативному реагуванню та мінімізації часу простою.

Zabbix характеризується підтримкою різноманітних методів збору даних, що забезпечує його інтеграцію з широким спектром обладнання та програмного забезпечення. Серед підтримуваних протоколів та технологій слід відзначити SNMP (Simple Network Management Protocol), IPMI (Intelligent Platform Management Interface), JMX (Java Management Extensions), а також

використання спеціалізованих агентів Zabbix, що встановлюються безпосередньо на цільових системах.

Однією з ключових переваг Zabbix є його висока гнучкість та масштабованість. Архітектура системи дозволяє ефективно використовувати її як у невеликих компаніях з обмеженою кількістю ІТ-ресурсів, так і у великих корпораціях з розгалуженою інфраструктурою, що нараховує тисячі пристроїв.

Окрім функцій безпосереднього моніторингу, Zabbix надає потужні засоби для аналізу історичних даних. Зібрана інформація може бути використана для виявлення тенденцій, прогнозування потенційних проблем та оптимізації роботи ІТ-систем. Інструменти для створення графіків та звітів забезпечують наочне представлення даних, що сприяє кращому розумінню стану системи та прийняттю обґрунтованих рішень.

Важливим елементом Zabbix є вбудована система тригерів. Тригери дозволяють визначати правила оповіщення та автоматичного реагування на події, що відбуваються в системі. Завдяки цьому досягається високий рівень автоматизації процесів моніторингу та управління, що значно зменшує час, необхідний для виявлення та усунення проблем, та мінімізує вплив інцидентів на роботу системи. Таким чином, Zabbix є комплексним та ефективним рішенням для моніторингу ІТ-інфраструктури, що поєднує в собі потужні функції збору, аналізу, візуалізації даних та автоматизації [29].

За підсумками моніторингу комп'ютера за період дослідження, Zabbix виявив такі результати:

Стан комп'ютера Office-PC-123 стабільний. Загальний час доступності системи (uptime) склав 99.9%, що відповідає високому рівню надійності. Виконано 6720 планових перевірок (кожні 60 секунд). Незначні збої у роботі були спричинені перезавантаженням системи після оновлення програмного забезпечення.

Середнє завантаження CPU протягом моніторингового періоду склало 23%, що є нормальним показником для офісних завдань.

Максимальне навантаження (88%) було зафіксовано під час роботи з великими Excel-таблицями. Проблем із продуктивністю процесора не зафіксовано.

Використання оперативної пам'яті в середньому становило 50% (8 GB із 16 GB). Максимальне навантаження (82%) було виявлено під час роботи із програмою Photoshop. У таких випадках рекомендується зменшувати кількість активних програм або збільшити обсяг оперативної пам'яті.

Середній рівень пінгу до шлюзу склав 2,5 мс, максимальна затримка: 320,0 мс. Максимальне навантаження на мережу зафіксовано під час оновлення програмного забезпечення: вхідний трафік: 45 Мбіт/с; вихідний трафік: 30 Мбіт/с.

Температура процесора коливалася в межах 45-70°C, що є нормою. Температура графічного адаптера залишалася стабільною на рівні 40-60°C. Жодних перегрівань не зафіксовано.

При проведенні моніторингу було зареєстровано два незначні попередження: 1) високе використання оперативної пам'яті (80%); 2) затримка доступу до мережевого ресурсу через високий пінг (320 мс). Обидва попередження не призвели до серйозних проблем і були вирішені автоматично.

Серед поширених інструментів, що застосовуються для моніторингу стану ІТ-інфраструктури, зокрема серверів, мереж та додатків, заслуговує на увагу програмний продукт **Nagios**. Ця система моніторингу з відкритим вихідним кодом зарекомендувала себе як ефективний засіб для забезпечення безперебійної роботи різноманітних ІТ-сервісів та компонентів інфраструктури (рис. 2.2).

Nagios забезпечує контроль доступності та продуктивності ключових елементів ІТ-середовища, дозволяючи оперативно виявляти потенційні проблеми та своєчасно інформувати адміністративний персонал за допомогою різноманітних каналів комунікації, таких як електронна пошта, SMS та інші.

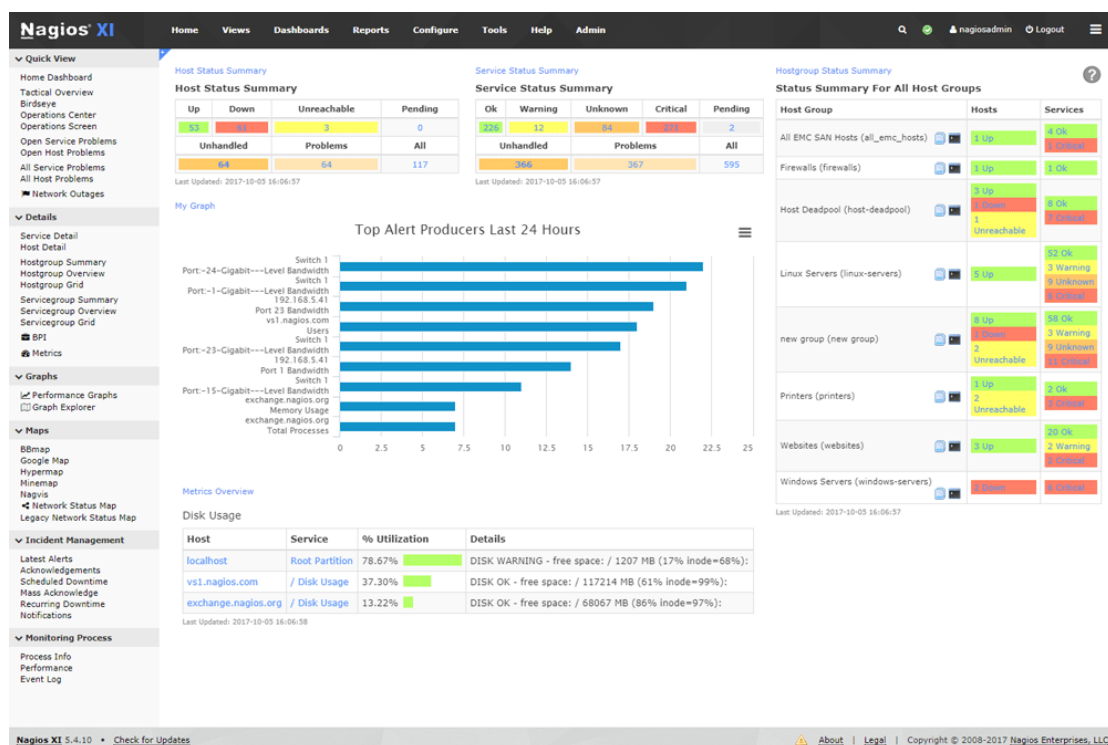


Рис. 2.2. Nagios [30]

Важливим аспектом функціональності Nagios є підтримка моніторингу на основі плагінів. Ця модульна архітектура надає можливість гнучкого налаштування та розширення системи для моніторингу специфічних сервісів, параметрів та показників, що відповідає потребам різних ІТ-інфраструктур.

Однією з фундаментальних переваг Nagios є його гнучкість та модульність. Ця особливість забезпечує інтеграцію з іншими системами та інструментами управління ІТ-інфраструктурою, а також дозволяє розширювати функціональні можливості за допомогою додаткових плагінів та модулів. Така **архітектура** робить Nagios придатним для використання в організаціях різного масштабу, від невеликих компаній до великих корпорацій, що потребують надійного та адаптованого інструменту для моніторингу своєї ІТ-інфраструктури [30].

Система Nagios також надає функціонал для створення детальних звітів та графічних відображень даних моніторингу. Ці інструменти дозволяють адміністраторам проводити аналіз продуктивності системи в динаміці, виявляти

тенденції та приймати обґрунтовані рішення щодо оптимізації використання ресурсів та забезпечення стабільної роботи критично важливих сервісів.

Загальний час роботи системи під час моніторингу системою Nagios склав 100% при виконанні 6720 планових перевірок (кожні 60 секунд), зброї не зафіксовані. Система працювала стабільно протягом усього періоду.

Середнє завантаження процесору за час моніторингу – 27%, максимальне завантаження 91%. Середнє використання оперативної пам'яті – 40% від загального обсягу; максимальне використання – 80%.

Середній пінг до шлюзу під час моніторингу складав 3,2. мс. Максимальний пінг. 15 мс. Середній вхідний трафік: 20 Мбіт/с, середній вихідний трафік: 12 Мбіт/с.

Температура процесора коливалася в межах 45–70°C, що є нормою. Температура графічного адаптера залишалася стабільною на рівні 40–60°C. Жодних перегрівань не зафіксовано.

Протягом періоду моніторингу було зафіксовано 2 попередження: 1) перевантаження CPU: 91% протягом 5 хвилин; 2) високе використання оперативної пам'яті: 12.9 GB. Жодних критичних інцидентів не виявлено.

Серед програмних продуктів, що забезпечують комплексний моніторинг ІТ-інфраструктури, зокрема мережевих пристроїв, серверів та баз даних, слід також виділити **PRTG Network Monitor**, розроблений компанією Paessler AG. Цей програмний комплекс являє собою інтегроване рішення, призначене для моніторингу стану та продуктивності різноманітних компонентів ІТ-середовища в режимі реального часу (рис. 2.3).

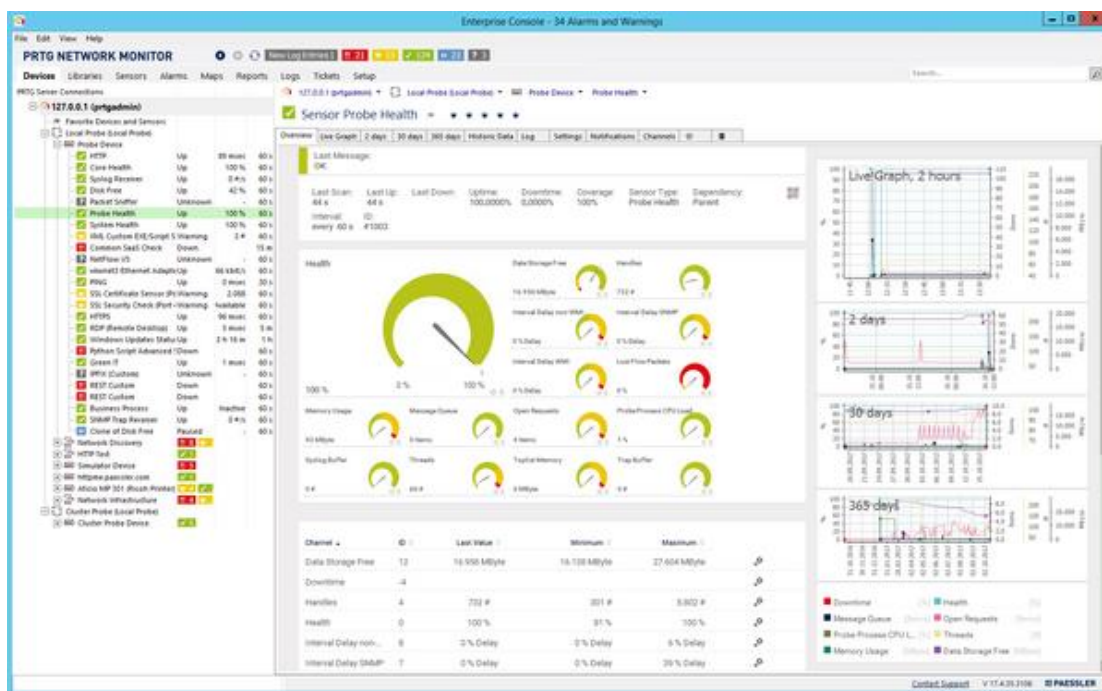


Рис. 2.3. PRTG Network Monitor [31]

PRTG Network Monitor забезпечує моніторинг широкого спектру елементів IT-інфраструктури, включаючи мережеві пристрої, сервери, додатки, мережевий трафік та інші критично важливі компоненти. Для збору даних використовуються різноманітні технології та протоколи, такі як SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation), NetFlow, sFlow та інші, що забезпечує сумісність з різними типами обладнання та програмного забезпечення. Особливістю PRTG є наявність інтуїтивно зрозумілого веб-інтерфейсу та мобільних додатків, що забезпечують доступ до інформації про стан мережі з різних пристроїв та платформ, підвищуючи оперативність реагування на інциденти [31].

Однією з ключових переваг PRTG Network Monitor є відносна простота встановлення та конфігурації. Система характеризується функцією автоматичного виявлення пристроїв у мережі та автоматичним налаштуванням сенсорів для моніторингу, що значно спрощує процес первинного розгортання та використання.

Крім того, PRTG надає розвинені інструменти для аналізу зібраних даних, включаючи інтерактивні інформаційні панелі (дашборди), генерування звітів та

систему оповіщень. Ці інструменти дозволяють оперативно виявляти та діагностувати проблеми, аналізувати тенденції та приймати обґрунтовані рішення щодо оптимізації роботи IT-інфраструктури. **Завдяки гнучким можливостям налаштування та масштабованості, PRTG Network Monitor є ефективним рішенням для організацій різного масштабу, що прагнуть забезпечити стабільну та безперебійну роботу своєї мережевої інфраструктури, незалежно від її розміру та складності [31].**

За час моніторингу з використанням засобу PRTG Network Monitor доступність системи складала 100%, кількість виконаних перевірок 10,080 (виконувалися кожні 30 секунд).

Середнє навантаження на систему за час моніторингу складало 25%, максимальне навантаження: 89%. Середнє використання оперативної пам'яті комп'ютером – 7,1 Гб (44% від загального обсягу 16 Гб), максимальне використання: 13.2 GB (82%).

Середня затримка (пінг) до шлюзу 3.5 мс., максимальна затримка: 17 мс. Середній вхідний трафік в мережі – 18 Мбіт/с, максимальний 90 Мбіт/с.

Температура процесора коливалася в межах 45–70°C, що є нормою. Температура графічного адаптера залишалася стабільною на рівні 40–60°C. Жодних перегрівань не зафіксовано.

За час проведення моніторингу зафіксовано два попередження: 1) завантаження процесора перевищило 80%; 2) використання оперативної пам'яті перевищило 80%. Попередження мали тимчасовий характер і не вплинули на загальну стабільність системи.

SolarWinds являє собою комплексну платформу, що об'єднує набір інструментів, призначених для моніторингу продуктивності систем, управління логами та адміністрування мережевої інфраструктури (рис. 2.4). Ця платформа розроблена компанією SolarWinds, відомим розробником програмного забезпечення для управління та моніторингу IT-інфраструктури. Продуктовий портфель компанії охоплює широкий спектр рішень, що забезпечують контроль

та оптимізацію різних аспектів ІТ-середовища, від моніторингу мереж та серверів до управління базами даних та віртуалізацією.



Рис. 2.4. SolarWinds [32]

Одним з найбільш відомих продуктів компанії є SolarWinds Network Performance Monitor (NPM), який надає потужні інструменти для моніторингу продуктивності мережі в режимі реального часу. NPM дозволяє здійснювати діагностику та усунення проблем, аналізувати мережевий трафік та отримувати детальну інформацію про стан мережевих пристроїв. Завдяки інтуїтивно зрозумілому інтерфейсу та розширеним функціональним можливостям, SolarWinds NPM забезпечує адміністраторам швидкий доступ до необхідної інформації та сприяє прийняттю обґрунтованих рішень щодо управління мережевою інфраструктурою.

Система SolarWinds має також інструменти, що забезпечують комплексний підхід до моніторингу та управління ІТ-інфраструктурою. Серед них - Server & Application Monitor, який дозволяє контролювати стан та продуктивність серверів та додатків, Database Performance Analyzer, призначений для аналізу продуктивності баз даних, та Virtualization Manager,

який забезпечує моніторинг та управління віртуалізованим середовищем. Зазначені продукти в сукупності забезпечують повну видимість та контроль на всіх рівнях IT-інфраструктури, сприяючи її ефективному функціонуванню.

SolarWinds відома своєю орієнтацією на потреби користувачів та прагненням до створення рішень, що легко інтегруються в існуючі системи та здатні масштабуватися відповідно до розвитку компанії. Завдяки своїй надійності, функціональності та ефективності, SolarWinds здобула широке визнання та стала вибором багатьох організацій по всьому світу для забезпечення стабільної та продуктивної роботи їх IT-середовища [32].

Під час моніторингу комп'ютера за допомогою системи SolarWinds доступність системи складала 100%, перевірки виконувались щохвилини.

Середнє завантаження процесора склало 26%, пікове навантаження – 90%. Середнє використання оперативної пам'яті – 6,8 Гб (42% від максимального об'єму, що складає 16 Гб); максимальне використання оперативної пам'яті – 13,1 Гб (82%).

Середня затримка (пінг) до шлюзу – 3,8 мс., максимальна затримка – 120 мс.; середній вхідний трафік у мережі – 20 Мбіт/с, максимальний – 55 Мбіт/с. Протягом всього часу моніторингу підключення залишалося стабільним.

Температура процесора коливалася в межах 45–70°C, що є нормою. Температура графічного адаптера залишалася стабільною на рівні 40–60°C. Жодних перегрівань не зафіксовано. За час проведення моніторингу зафіксовано два попередження: 1) завантаження процесора перевищило 85%; 2) використання оперативної пам'яті перевищило 80%. Попередження мали тимчасовий характер і не вплинули на загальну стабільність системи.

Окремої уваги заслуговують спеціалізовані засоби моніторингу, що враховують специфіку функціонування об'єктів енергетичної галузі, зокрема сонячних та гідроелектростанцій, підприємство з обслуговування яких було практичною базою даного дослідження. У контексті моніторингу сонячних електростанцій широко застосовуються спеціалізовані програмні рішення,

серед яких вагоме місце займає онлайн-платформа Sunny Portal, розроблена компанією SMA Solar Technology (рис. 2.5).

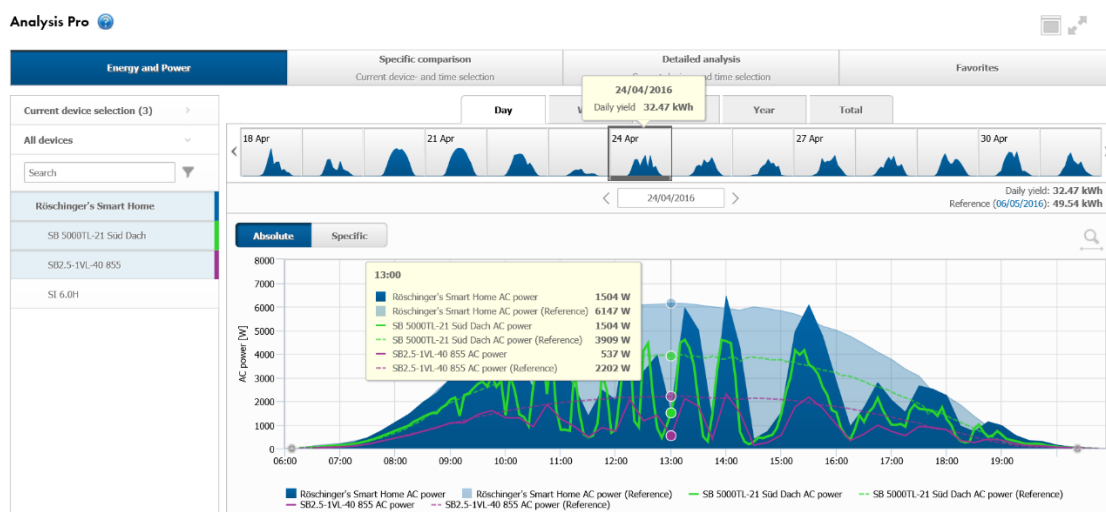


Рис. 2.5. Sunny Portal (SMA) [33].

Sunny Portal являє собою веб-платформу, що забезпечує користувачам можливість моніторингу та управління сонячними електростанціями. За допомогою цього інструменту власники сонячних установок отримують доступ до деталізованих даних щодо продуктивності їхніх систем, що дозволяє відстежувати рівень генерації електроенергії, аналізувати ефективність та оперативно виявляти потенційні проблеми в режимі реального часу.

Однією з ключових переваг Sunny Portal є можливість віддаленого доступу до даних з будь-якої локації, що значно підвищує рівень зручності та оперативності в управлінні сонячними системами.

Платформа підтримує інтеграцію з різноманітними пристроями SMA, включаючи інвертори та системи зберігання енергії. Ця інтеграція дозволяє створювати комплексні рішення для оптимізації енергоспоживання та ефективного управління всіма компонентами сонячної електростанції. Завдяки інтегрованому підходу, користувачі отримують повну інформацію про роботу системи та можуть оперативно реагувати на будь-які зміни в її стані.

Крім того, Sunny Portal пропонує функціонал спільного доступу, що дозволяє користувачам обмінюватися даними про продуктивність з іншими зацікавленими сторонами, такими як енергетичні консультанти або сервісні компанії. Ця функція сприяє підвищенню прозорості та ефективності

управління та обслуговування сонячних електростанцій, забезпечуючи можливість колективної роботи та обміну експертними знаннями. Таким чином, Sunny Portal є потужним інструментом для моніторингу та управління сонячними електростанціями, що забезпечує користувачам повний контроль над роботою їхніх систем та сприяє оптимізації виробництва електроенергії [33].

Протягом періоду моніторингу за допомогою Sunny Portal було проаналізовано роботу сонячної електростанції потужністю 1 МВт. За цей час станція виробила 4900 кВт·год електроенергії, що на 6% менше планового показника. Найвища добова генерація становила 820 кВт·год, тоді як мінімальна – 580 кВт·год (ймовірно через хмарну погоду). Незважаючи на незначне відхилення від плану, станція працювала стабільно.

Ефективність роботи станції була оцінена за середнім коефіцієнтом ефективності (Performance Ratio, PR), який склав 87%. Максимальне значення PR у звітному періоді досягло 92%, мінімальне – 81%, що було пов'язано з погодними умовами та накопиченням пилу на модулях. Усі інвертори, які входять до складу системи, працювали стабільно з середнім коефіцієнтом корисної дії 96%, без будь-яких збоїв чи помилок.

Передача енергії до мережі відбувалася без значних втрат, які в середньому склали лише 2%. Станція функціонувала без перепадів навантаження та аварійних відключень. Однак було виявлено зниження продуктивності на трьох модулях, які генерували лише 30-50% від номінальної потужності. Ймовірною причиною цього стали тінь від дерев або забруднення поверхні.

Протягом моніторингового періоду середня сонячна радіація становила 4.8 кВт·год/м², з максимальним показником у 6.2 кВт·год/м². На два дні припав високий рівень хмарності, що також вплинуло на генерацію. Жодних збоїв у роботі системи за цей час не було виявлено.

Ще один засіб – **SolarEdge Monitoring** який являє собою платформу, призначену для моніторингу та управління фотоелектричними системами, що

забезпечує користувачів детальними звітами та аналітичними інструментами (рис. 2.6). Розроблена компанією SolarEdge, ця платформа забезпечує комплексний контроль над продуктивністю сонячних електростанцій, надаючи в режимі реального часу детальну інформацію про виробництво електроенергії, ефективність сонячних панелей та стан обладнання [34].

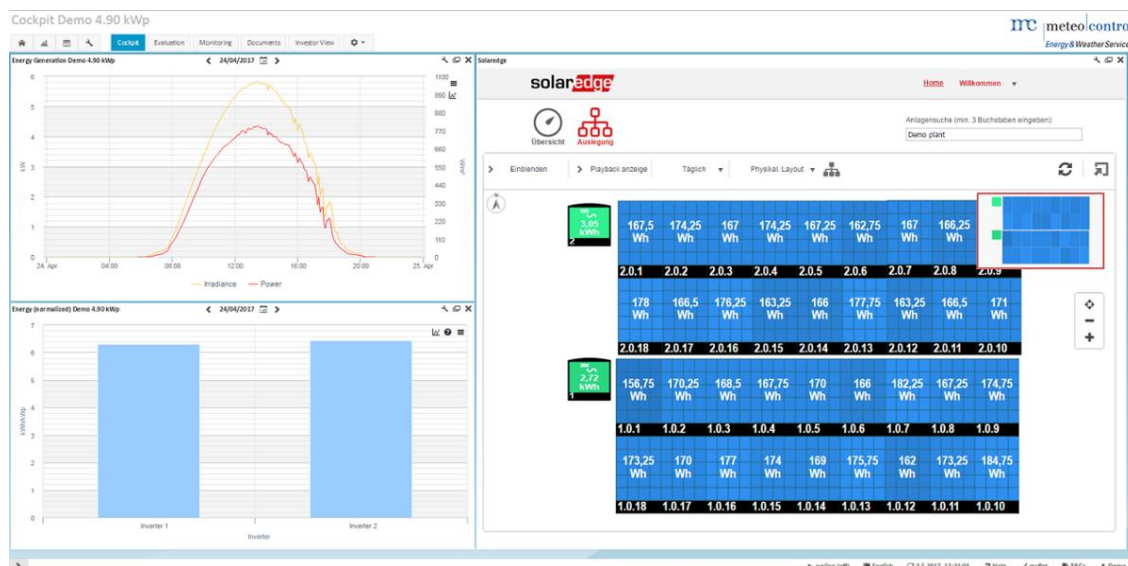


Рис. 2.6. SolarEdge Monitoring [34].

Однією з ключових особливостей SolarEdge Monitoring є можливість відстеження продуктивності кожного окремого фотоелектричного модуля. Ця функція дозволяє оперативно ідентифікувати та усувати проблеми на початкових стадіях їх виникнення, що сприяє мінімізації втрат енергії та підвищенню загальної ефективності системи.

Інтерфейс платформи SolarEdge Monitoring характеризується інтуїтивною зрозумілістю та надає різноманітні графіки, звіти та візуалізації даних. Це робить аналіз інформації доступним навіть для користувачів без спеціальної технічної підготовки, спрощуючи процес моніторингу та прийняття рішень. Візуалізація даних у зручному форматі сприяє швидкому розумінню стану системи та виявленню потенційних проблем.

Важливою перевагою SolarEdge Monitoring є можливість віддаленого доступу до даних через веб-браузер або спеціалізований мобільний додаток. Ця функція забезпечує високу зручність та гнучкість управління сонячною

електростанцією, дозволяючи користувачам контролювати роботу системи з будь-якого місця та в будь-який час. Віддалений доступ сприяє оперативному реагуванню на будь-які зміни в стані системи та мінімізує час простою.

Платформа інтегрована з іншими продуктами SolarEdge, такими як інвертори та системи зберігання енергії. Ця інтеграція дозволяє створювати комплексні рішення для ефективного управління енергією, оптимізуючи виробництво, споживання та зберігання електроенергії.

SolarEdge Monitoring також підтримує функцію спільного доступу до даних, що дозволяє користувачам ділитися інформацією про продуктивність системи з іншими зацікавленими сторонами, такими як енергетичні консультанти або сервісні компанії. Це сприяє покращенню обслуговування та оптимізації роботи сонячних електростанцій, забезпечуючи максимальну ефективність та надійність їх функціонування. Спільний доступ до даних покращує комунікацію між різними учасниками процесу та сприяє підвищенню якості обслуговування [34].

Протягом звітного періоду SolarEdge Monitoring забезпечив детальний моніторинг роботи сонячної електростанції потужністю 1 МВт.

Загальна генерація електроенергії склала 4950 кВт·год, що є дещо нижчим за планові показники через погодні умови. Найвищий добовий рівень складав 830 кВт·год, тоді як найнижчий – 570 кВт·год через хмарність.

Рівень продуктивності станції (Performance Ratio, PR) у середньому становив 88%, з максимумом у 93% та мінімумом у 82%. Зниження показників ефективності було пов'язане з впливом хмарності та можливим забрудненням панелей. Станція продемонструвала високу стабільність роботи, оскільки всі інвертори функціонували бездоганно, забезпечуючи середній коефіцієнт корисної дії на рівні 97%.

Мережеве з'єднання працювало без збоїв, а втрати при передачі електроенергії були мінімальними й не перевищували 2%. Жодних аварійних відключень чи серйозних відхилень у роботі обладнання зафіксовано не було. Водночас система ідентифікувала зниження продуктивності на двох модулях,

які працювали лише на 40-50% від номінальної потужності. Ця проблема, ймовірно, була викликана тінню від сторонніх об'єктів або забрудненням панелей.

Протягом моніторингового періоду середня сонячна радіація становила 4.9 кВт·год/м², що відповідало сезонним очікуванням. Жодних критичних проблем у роботі системи не було виявлено. SolarEdge Monitoring успішно забезпечив контроль усіх ключових параметрів, дозволив виявити відхилення у роботі окремих модулів.

Базовим завданням для будь-якого засобу моніторингу є збір даних. Галузева специфіка, обумовлена роботою з сонячними електростанціями, передбачає також збір даних про продуктивність сонячних панелей, що визначається шляхом вимірювання вихідної потужності для подальшої оцінки їхньої ефективності. Крім того, здійснюється збір даних про рівень заряду та зносу акумуляторів з метою забезпечення контролю стану зарядки та розрядки акумуляторних батарей, які забезпечують стабільне живлення мережі, накопичення надлишкової електроенергії та запобігання перевантаженню системи в періоди активної генерації. Функція збору інформації охоплює не лише збір первинних даних, але й накопичення так званих **"логів" – журналів подій**, що містять інформацію про зміни стану системи та використовуються для виявлення аномалій в роботі та діагностики проблем [35].

Характерною рисою комп'ютерних систем при роботі з сонячними електростанціями є наявність віддаленого моніторингу: оскільки база дослідження знаходиться в м. Київ, а об'єкти моніторингу – сонячні електростанції – розташовані у Київській, Хмельницькій та Миколаївській областях, забезпечення можливості відстеження стану сонячних панелей та інших компонентів електростанції дистанційно є критично необхідним для зручності управління. Також важливою функцією є можливість інтеграції програмного забезпечення з SCADA-системами (Supervisory Control and Data Acquisition) – системами управління та збору даних, які використовуються для контролю та моніторингу промислових процесів [34].

Нарешті, забезпечення кібербезпеки є універсальною функцією програмних засобів моніторингу стану системи. Виявлення та запобігання кібератакам на мережеву інфраструктуру електростанції, забезпечення безпечної передачі даних між компонентами системи та серверами моніторингу є невід'ємними та критично важливими функціями, виконання яких допомагає забезпечити економічну ефективність діяльності підприємства.

Підсумовуючи, функції засобів моніторингу комп'ютерних систем охоплюють широкий спектр завдань, спрямованих на забезпечення стабільної, безпечної та ефективної роботи цих систем. У випадку моніторингу мереж у роботі сонячних електростанцій, додаткову увагу слід приділяти віддаленому моніторингу, інтеграції з SCADA-системами та кібербезпеці, що дозволяє підвищити надійність та продуктивність таких об'єктів.

2.2. Критерії оцінки ефективності систем моніторингу.

Оцінка ефективності системи моніторингу є важливим етапом, що дозволяє визначити, наскільки добре система виконує свої функції та чи відповідає вона потребам організації. Зважаючи на суб'єктивність питання визначення «найкращого» програмного засобу моніторингу у даному підрозділі ми запропонуємо та розглянемо основні критерії, які на нашу думку доречно використовувати для оцінки ефективності систем моніторингу.

Точність та повнота даних. Обидва критерії є фундаментальними. Точність відображає ступінь відповідності даних моніторингу реальному стану системи. Неточні дані можуть призвести до неправильних висновків та помилкових дій. Повнота даних означає наявність всієї необхідної інформації для моніторингу та аналізу. Неповні дані можуть ускладнити виявлення проблем та призвести до пропуску важливих подій. Для оцінки точності можна порівнювати дані моніторингу з даними, отриманими з інших джерел, або з еталонними значеннями. Повнота даних оцінюється шляхом перевірки наявності **всіх необхідних метрик та подій**. Наприклад, якщо система

моніторингу не збирає дані про використання дискового простору, це свідчить про низьку повноту даних [37].

Час виявлення інцидентів (Mean Time To Detect, MTTD) – це середній час, необхідний для виявлення інциденту після його виникнення. Чим менший MTTD, тим швидше система реагує на проблеми та тим менші потенційні збитки від інциденту. MTTD залежить від багатьох факторів, таких як частота збору даних, налаштування сповіщень, ефективність методів аналізу даних та кваліфікація персоналу. Для покращення MTTD можна використовувати більш часті опитування, більш точні порогові значення для сповіщень, автоматизовані методи аналізу та системи кореляції подій. Наприклад, якщо система моніторингу налаштована на виявлення перевищення завантаження ЦП понад 90%, і це перевищення триває протягом 5 хвилин до моменту сповіщення, то MTTD становитиме 5 хвилин [38].

Час відновлення після інцидентів (Mean Time To Repair/Resolve/Restore, MTTR) – це середній час, необхідний для відновлення працездатності системи після виявлення інциденту. Чим менший MTTR, тим швидше система повертається до нормального стану та тим менші простої. MTTR залежить від складності інциденту, наявності планів відновлення, кваліфікації персоналу та доступності необхідних ресурсів. Для зменшення MTTR необхідно мати чіткі процедури реагування на інциденти, автоматизовані інструменти відновлення та добре навчений персонал. Наприклад, якщо після виявлення збою сервера знадобилося 30 хвилин для його перезавантаження та відновлення роботи, то MTTR становитиме 30 хвилин. Важливо зазначити, що існують різні варіації цього показника, такі як MTTR (Mean Time To Repair – середній час ремонту), MTTR (Mean Time To Resolve – середній час вирішення) та MTTR (Mean Time To Restore – середній час відновлення). Вони можуть дещо відрізнятися за змістом залежно від контексту [39].

Навантаження на систему моніторингу відображає використання ресурсів (ЦП, пам'ять, мережа) серверами та агентами моніторингу. Надмірне

навантаження на систему моніторингу може призвести до її нестабільної роботи та вплинути на точність та своєчасність збору даних. Для оцінки навантаження на систему моніторингу необхідно моніторити використання ресурсів серверами та агентами, а також аналізувати трафік, що генерується системою. Для зменшення навантаження можна оптимізувати конфігурацію системи, використовувати більш ефективні методи збору даних та масштабувати інфраструктуру моніторингу. Наприклад, якщо сервери моніторингу постійно перевантажені, це може призвести до затримок у зборі та обробці даних.

Вартість володіння системою моніторингу (Total Cost of Ownership, TCO) – це сукупність витрат, пов'язаних з придбанням, впровадженням, експлуатацією та підтримкою системи моніторингу протягом певного періоду часу. TCO включає витрати на обладнання, програмне забезпечення, ліцензії, навчання персоналу, підтримку та обслуговування [40]. При виборі системи моніторингу необхідно враховувати не тільки вартість придбання, але й загальну вартість володіння, яка може значно відрізнятися для різних систем. Наприклад, безкоштовна система моніторингу з відкритим кодом може вимагати значних витрат на налаштування та підтримку, що збільшить її TCO.

Вибір конкретних критеріїв та їхня пріоритетність залежить від специфічних потреб та вимог організації. Важливо враховувати всі аспекти роботи системи моніторингу, від точності даних до вартості володіння, для отримання об'єктивної та комплексної оцінки її ефективності.

2.3. Порівняльний аналіз систем моніторингу.

Розпочнімо з популярних систем моніторингу та порівняємо їх за визначеними раніше критеріями, а саме: точністю та повнотою даних, часом виявлення інцидентів, часом відновлення після інцидентів та вартістю володіння. Оцінка за такими критеріями як простота використання, масштабованість, візуалізація та підтримка спільноти базуватиметься на **суб'єктивних враженнях автора від використання.**

Для зручності порівняння представимо інформацію у вигляді таблиці (табл. 2.2.). Оцінка виставлено за шкалою від 1 до 5, де 5 – найкраща оцінка.

Таблиця 2.2.

Порівняння популярних систем моніторингу

Критерій	Zabbix	Nagios	PRTG Network Monitor	SolarWinds
Точність та повнота даних	4	4	4	4
Час виявлення інцидентів (MTTD)	4	4	4	4
Час відновлення (MTTR)	3	3	3	3
Навантаження на систему	3	3	4	3
Вартість володіння (TCO)	5	5	3	2
Простота використання	3	2	5	4
Масштабованість	5	4	4	4
Візуалізація/Звітність	4	3	4	4
Підтримка спільноти/Виробника	4	5	4	4
Середній показник	4	3.8	3.9	3.6

Джерело: виконано автором **самостійно на основі власних досліджень**.

Розглянемо більше детально дані системи за кожним з критеріїв окремо.

Точність та повнота даних. Усі чотири системи забезпечують достатню точність та повноту даних для більшості випадків використання. Zabbix та Nagios завдяки своїй гнучкості дозволяють збирати дані з різних джерел та налаштовувати збір даних під конкретні потреби. PRTG пропонує широкий набір готових сенсорів, що спрощує збір даних **для типових сценаріїв**. SolarWinds пропонує комплексні рішення для моніторингу різних аспектів ІТ-інфраструктури.

Час виявлення інцидентів (MTTD) та Час відновлення (MTTR). Усі системи надають механізми сповіщень про інциденти, що дозволяє оперативно реагувати на проблеми. Однак, жодна з цих систем не надає вбудованих інструментів для автоматичного відновлення. Для автоматизації відновлення необхідно використовувати інтеграції з іншими системами.

Навантаження на систему. Zabbix та Nagios можуть створювати значне навантаження на сервери моніторингу при великій кількості об'єктів

моніторингу та високій частоті збору даних. PRTG та SolarWinds, як правило, більш оптимізовані для роботи з великими обсягами даних.

Вартість володіння (TCO). Zabbix та Nagios є open-source рішеннями, що значно знижує витрати на ліцензії. PRTG пропонує безкоштовну версію з обмеженою кількістю сенсорів, а також платні ліцензії. SolarWinds є комерційною платформою з різними варіантами ліцензування.

Простота використання. PRTG вважається однією з найпростіших у використанні систем завдяки інтуїтивному веб-інтерфейсу та великій кількості готових сенсорів. Zabbix та Nagios вимагають більше зусиль для налаштування та адміністрування. SolarWinds пропонує зручний інтерфейс, але складність може зростати зі збільшенням кількості використовуваних продуктів.

Масштабованість. Zabbix відомий своєю високою масштабованістю та здатністю моніторити дуже великі інфраструктури. Nagios також може бути масштабований, але це може вимагати додаткових зусиль. PRTG та SolarWinds також підтримують масштабування, але їхня архітектура може мати певні обмеження.

Гнучкість/Розширюваність. Zabbix та Nagios є дуже гнучкими та розширюваними завдяки підтримці плагінів та скриптів. PRTG пропонує широкий набір вбудованих сенсорів, але можливості розширення можуть бути обмеженими. SolarWinds пропонує інтеграції з іншими продуктами SolarWinds, що забезпечує певну гнучкість.

Візуалізація/Звітність. Усі чотири системи надають можливості для візуалізації даних та створення звітів. Zabbix пропонує гнучкі можливості для налаштування графіків та дашбордів. PRTG має зручний веб-інтерфейс з готовими дашбордами та картами. SolarWinds пропонує потужні інструменти для створення звітів та аналізу даних.

Підтримка спільноти. Zabbix та Nagios мають великі та активні спільноти користувачів, які надають підтримку та діляться досвідом. PRTG та SolarWinds пропонують комерційну підтримку від виробника.

Отже, вибір конкретної системи залежить виключено від потреб та вимог організації, адже загалом їх функціонал та ефективність близькі одна до одної, а відмінність полягає в вузько-спеціалізованих функціях характерних для окремих систем. Узагальнюючи результати можна стверджувати, що Zabbix – підходить для організацій, яким потрібна гнучка, масштабована та безкоштовна система моніторингу з широким набором функцій; Nagios – підходить для організацій, які шукають потужне та розширюване open-source рішення з великою спільнотою користувачів; PRTG Network Monitor – підходить для організацій, яким потрібна проста у використанні та швидка у впровадженні система моніторингу з готовими сенсорами; SolarWinds – підходить для організацій, які шукають комплексну платформу для моніторингу та управління IT-інфраструктурою з комерційною підтримкою.

Також, проведемо порівняльний аналіз платформ Sunny Portal (SMA) та SolarEdge Monitoring, аналогічно до попередніх порівнянь систем моніторингу IT-інфраструктури. Обидві платформи призначені для моніторингу фотоелектричних систем, проте мають певні відмінності у функціональності та підході до збору та аналізу даних. Результати порівняння представимо у вигляді таблиці, після чого сформулюємо висновки (табл. 2.3).

Обидві платформи, Sunny Portal та SolarEdge Monitoring, є потужними інструментами для моніторингу сонячних електростанцій, проте вони мають різні підходи та орієнтовані на дещо різні типи систем.

Sunny Portal від SMA є комплексною платформою, яка забезпечує загальний моніторинг системи, включаючи інвертори, загальну генерацію та інші параметри. Платформа надає зручні інструменти для візуалізації даних та аналізу ефективності, що робить її привабливою для власників як житлових, так і комерційних сонячних установок. Акцент робиться на загальному огляді системи та зручному представленні інформації.

Таблиця 2.3.

Порівняння спеціалізованих засобів моніторингу

Критерій порівняння	Sunny Portal (SMA)	SolarEdge Monitoring
Основна функція	Моніторинг та управління сонячними електростанціями	Моніторинг та управління фотоелектричними системами
Деталізація моніторингу	Моніторинг на рівні системи (інвертори, загальна генерація)	Моніторинг на рівні окремого модуля (оптимізатори потужності)
Аналіз даних	Візуалізація даних у вигляді графіків та звітів, аналіз ефективності	Детальні звіти та аналітика, включаючи виявлення проблем на рівні модуля
Віддалений доступ	Веб-платформа, мобільний додаток	Веб-браузер, мобільний додаток
Інтеграція з іншим обладнанням	Інвертори SMA, системи зберігання енергії SMA	Інвертори SolarEdge, оптимізатори потужності SolarEdge, системи зберігання енергії SolarEdge
Спільний доступ до даних	Підтримується	Підтримується
Орієнтація	Житлові та комерційні установки	Системи з оптимізаторами потужності, комерційні та промислові установки
Акцент	Загальний моніторинг системи, візуалізація даних	Детальний аналіз продуктивності на рівні модуля, оптимізація енергоспоживання

Джерело: виконано автором самостійно на основі [33], [34].

SolarEdge Monitoring, з іншого боку, вирізняється можливістю моніторингу на рівні окремого модуля завдяки використанню оптимізаторів потужності. Це дозволяє отримувати детальну інформацію про продуктивність кожної сонячної панелі, виявляти та вирішувати проблеми на ранніх етапах, що сприяє максимізації виробництва електроенергії та оптимізації енергоспоживання. SolarEdge Monitoring орієнтована на системи з оптимізаторами потужності, які часто використовуються в комерційних та промислових установках, де важлива максимальна ефективність та детальний контроль.

Таким чином, вибір між Sunny Portal та SolarEdge Monitoring залежить від конкретних потреб та характеристик сонячної електростанції. Якщо потрібен загальний моніторинг системи та зручна візуалізація даних, Sunny Portal буде

хорошим вибором. Якщо ж важливий детальний аналіз продуктивності на рівні модуля та оптимізація енергоспоживання, SolarEdge Monitoring з її інтеграцією з оптимізаторами потужності буде більш підходящим рішенням. Важливо також враховувати сумісність платформи з встановленим обладнанням (інверторами, оптимізаторами, системами зберігання енергії) при виборі системи моніторингу.

Для великих підприємств з комплексними потребами, включаючи інтеграцію з SCADA та IoT, найбільш підходящим варіантом є SolarWinds. Для малих та середніх підприємств, які шукають просте у використанні рішення, оптимальним вибором є PRTG Network Monitor. Організаціям з обмеженим бюджетом та технічними ресурсами для налаштування можуть підійти Zabbix або Nagios.

Вибір оптимального засобу залежить від конкретних потреб організації, доступних ресурсів та специфіки роботи системи. Впровадження надійних засобів моніторингу сприяє підвищенню продуктивності, зниженню ризиків та забезпеченню безпеки операцій.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ.

Перспективи розвитку та удосконалення систем моніторингу комп'ютерних мереж є широкими та багатограними, відображаючи постійний розвиток технологій та зростаючі вимоги до надійності та ефективності IT-інфраструктур. Сучасні тенденції в галузі, такі як хмарні обчислення, віртуалізація, Інтернет речей (IoT), штучний інтелект (ШІ) та машинне навчання (ML), Big Data, безперервно генерують нові виклики та можливості для систем моніторингу.

Застосування алгоритмів машинного навчання дозволяє автоматизувати аналіз великих обсягів даних, виявляти складні залежності та прогнозувати потенційні проблеми ще до їх виникнення. Це значно підвищує проактивність моніторингу та дозволяє запобігати збоєм, а не реагувати на вже існуючі інциденти. Наприклад, алгоритми ML можуть аналізувати історичні дані про трафік мережі та прогнозувати пікові навантаження, що дозволяє завчасно оптимізувати ресурси та уникнути перевантаження. Також, ШІ може автоматично корелювати події з різних джерел, що спрощує діагностику складних проблем та скорочує час на їх вирішення.

З розвитком хмарних технологій та мікросервісної архітектури зростає складність моніторингу розподілених систем. Традиційні підходи до моніторингу часто виявляються неефективними в таких середовищах. Тому, перспективним напрямком є розвиток систем моніторингу, орієнтованих на хмарні середовища та контейнеризовані додатки. Такі системи повинні забезпечувати динамічне виявлення сервісів, автоматичне масштабування моніторингу та глибоку інтеграцію з хмарними платформами [41].

Зі зростанням кількості пристроїв IoT, моніторинг мереж стає ще більш складним завданням. Пристрої IoT часто мають обмежені ресурси та використовують різноманітні протоколи зв'язку. Тому, системи моніторингу повинні підтримувати широкий спектр протоколів та забезпечувати ефективний збір даних з великої кількості різнорідних пристроїв. Перспективним

напрямок є використання Edge Computing для попередньої обробки даних на периферії мережі, що дозволяє зменшити навантаження на центральні сервери моніторингу та покращити швидкість реагування на локальні події [42].

Важливим напрямком розвитку є також покращення візуалізації та аналізу даних. Сучасні системи моніторингу повинні надавати користувачам інтуїтивно зрозумілі дашборди та графіки, що дозволяють швидко отримувати інформацію про стан мережі та виявляти проблеми. Перспективним є використання інтерактивних візуалізацій, які дозволяють користувачам досліджувати дані та виявляти приховані залежності. Також, важливим є розвиток засобів для аналізу логів та подій, що дозволяє швидко діагностувати складні проблеми та визначати їх причини [43].

Зростаюча кількість кіберзагроз вимагає посилення функцій кібербезпеки в системах моніторингу. Системи моніторингу повинні не тільки виявляти аномалії в роботі мережі, але й ідентифікувати потенційні кібератаки та реагувати на них. Перспективним напрямком є інтеграція систем моніторингу з системами виявлення та запобігання вторгненням (IDS/IPS), що дозволяє створити комплексну систему захисту мережі. Також, важливим є використання аналізу поведінки користувачів та пристроїв для виявлення підозрілої активності.

Автоматизація процесів моніторингу та реагування на інциденти є ще однією важливою тенденцією. Застосування технологій автоматизації дозволяє зменшити ручну працю та підвищити ефективність управління мережею. Перспективним є використання playbook-ів та workflow-ів для автоматизації типових завдань, таких як перезавантаження сервісів, блокування IP-адрес та ізоляція заражених пристроїв. Також, важливим є інтеграція систем моніторингу з іншими системами управління IT-інфраструктурою, що дозволяє створити єдиний центр управління.

Нарешті, важливим аспектом є розвиток стандартів та протоколів для обміну даними між різними системами моніторингу. Це дозволить створити більш інтегровані та гнучкі рішення для моніторингу складних IT-

інфраструктур. Перспективним є використання відкритих стандартів та API, що дозволяє легко інтегрувати різні системи та отримувати комплексну картину стану мережі [44].

Таким чином, перспективи розвитку та удосконалення систем моніторингу комп'ютерних мереж пов'язані з інтеграцією новітніх технологій, таких як ШІ, ML, хмарні обчислення, IoT та автоматизація. Це дозволить створити більш проактивні, інтелектуальні та ефективні системи моніторингу, які здатні забезпечити надійну та безпечну роботу сучасних IT-інфраструктур.

Подальший розвиток систем моніторингу нерозривно пов'язаний з впровадженням концепції Observability (спостережуваність). Observability виходить за рамки традиційного моніторингу, який фокусується на зборі метрик, логів та трасування. Observability передбачає здатність системи надавати повне уявлення про свій внутрішній стан на основі зовнішніх вихідних даних. Це досягається шляхом інтеграції даних з різних джерел, таких як метрики, логи, трасування, події та інша телеметрія, та їх кореляції за допомогою аналітичних інструментів. Observability дозволяє не тільки виявляти проблеми, але й розуміти їх причини та прогнозувати потенційні ризики [45].

З розвитком технологій віртуалізації та контейнеризації, зокрема Docker та Kubernetes, виникає потреба в моніторингу динамічних середовищ. Традиційні системи моніторингу часто не справляються з швидкою зміною конфігурації таких середовищ. Тому, перспективним напрямком є розвиток систем, які автоматично виявляють нові контейнери та віртуальні машини, адаптуються до змін в їх конфігурації та забезпечують моніторинг на рівні окремих контейнерів та сервісів. Важливим аспектом є інтеграція з оркестраторами контейнерів, такими як Kubernetes, для отримання інформації про стан та ресурси кластера [46].

Зі збільшенням обсягів даних, що генеруються мережевими пристроями та додатками, зростає потреба в ефективних методах їх зберігання та аналізу. Технології Big Data, такі як Hadoop та Spark, можуть бути використані для зберігання та обробки великих обсягів даних моніторингу. Це дозволяє

проводити складний аналіз, виявляти тренди та прогнозувати майбутні проблеми. Також, важливим є використання технологій потокової обробки даних, таких як Kafka та Flink, для аналізу даних в реальному часі та оперативного реагування на інциденти [47].

Безпека залишається одним з найважливіших аспектів моніторингу комп'ютерних мереж. Системи моніторингу повинні не тільки виявляти аномалії в роботі мережі, але й ідентифікувати потенційні кібератаки, такі як DDoS-атаки, вторгнення та шкідливе програмне забезпечення. Перспективним напрямком є використання технологій Security Information and Event Management (SIEM) для збору та аналізу інформації про безпеку з різних джерел, включаючи логи, події та дані з систем виявлення вторгнень. Також, важливим є використання методів машинного навчання для виявлення складних та невідомих атак.

Автоматизація процесів моніторингу та реагування на інциденти залишається важливою тенденцією. Застосування технологій Infrastructure as Code (IaC) дозволяє автоматизувати розгортання та конфігурацію інфраструктури моніторингу. Також, важливим є використання інструментів автоматизації, таких як Ansible та Puppet, для автоматизації рутинних завдань, таких як перезавантаження сервісів, блокування IP-адрес та ізоляція заражених пристроїв. Це дозволяє зменшити час реагування на інциденти та підвищити ефективність роботи ІТ-персоналу.

З розвитком технологій Edge Computing, моніторинг переміщується ближче до джерела даних. Це дозволяє зменшити затримки при зборі та аналізі даних, а також зменшити навантаження на центральні сервери моніторингу. Перспективним є використання Edge Computing для попередньої обробки даних, фільтрації та агрегації, що дозволяє передавати на центральні сервери тільки важливу інформацію. Також, Edge Computing дозволяє забезпечити моніторинг в умовах обмеженої пропускної здатності каналу зв'язку [46].

Нарешті, важливим аспектом є розвиток інтероперабельності між різними системами моніторингу. Це дозволяє створити єдину систему моніторингу, яка

об'єднує дані з різних джерел та надає повну картину стану IT-інфраструктури. Перспективним є використання відкритих стандартів та API, таких як OpenTelemetry та Prometheus, для обміну даними між різними системами. Це дозволяє уникнути залежності від конкретного виробника та створити більш гнучкі та масштабовані рішення [48].

Враховуючи всі ці тенденції, можна стверджувати, що майбутні системи моніторингу будуть більш інтелектуальними, автоматизованими, розподіленими та орієнтованими на спостережуваність. Вони будуть здатні аналізувати великі обсяги даних в реальному часі, прогнозувати потенційні проблеми та автоматично реагувати на інциденти.

Висновки щодо перспектив розвитку та удосконалення систем моніторингу комп'ютерних мереж зводяться до кількох ключових тенденцій:

1) Ввідбувається активна інтеграція штучного інтелекту та машинного навчання, що дозволяє не тільки виявляти існуючі проблеми, але й прогнозувати їх виникнення, автоматизувати аналіз великих обсягів даних та корелювати події з різних джерел. Це значно підвищує проактивність моніторингу та скорочує час реагування на інциденти.

2) Розвиток хмарних технологій та мікросервісної архітектури зумовлює потребу в нових підходах до моніторингу розподілених систем. Системи майбутнього повинні забезпечувати автоматичне масштабування та глибоку інтеграцію з хмарними платформами, моніторинг на рівні окремих мікросервісів та їх взаємодії. Зі збільшенням кількості пристроїв IoT, системи моніторингу повинні підтримувати широкий спектр протоколів та ефективно збирати дані з різнорідних пристроїв, використовуючи Edge Computing для попередньої обробки даних на периферії мережі.

3) Важливим є покращення візуалізації та аналізу даних. Інтуїтивно зрозумілі дашборди, інтерактивні візуалізації та розвинені засоби аналізу логів дозволять користувачам швидко отримувати інформацію про стан мережі, виявляти приховані залежності та діагностувати складні проблеми. Зростання кількості кіберзагроз вимагає посилення функцій кібербезпеки в системах

моніторингу, зокрема інтеграції з IDS/IPS та аналізу поведінки користувачів і пристроїв.

4) Автоматизація процесів моніторингу та реагування на інциденти залишається ключовою тенденцією. Застосування технологій автоматизації, таких як playbook-и та workflow-и, дозволяє автоматизувати рутинні завдання та зменшити час реагування на інциденти. Інтеграція з іншими системами управління IT-інфраструктурою створює єдиний центр управління.

5) Концепція Observability виходить за рамки традиційного моніторингу, пропонуючи повне уявлення про внутрішній стан системи на основі зовнішніх даних. Це досягається шляхом інтеграції даних з різних джерел та їх кореляції. З розвитком віртуалізації та контейнеризації, системи моніторингу повинні автоматично виявляти нові контейнери та віртуальні машини.

Загалом, майбутні системи моніторингу будуть більш інтелектуальними, автоматизованими, розподіленими та орієнтованими на спостережуваність, здатними аналізувати великі обсяги даних в реальному часі, прогнозувати проблеми та автоматично реагувати на інциденти, забезпечуючи високу доступність, надійність та безпеку сучасних IT-інфраструктур.

ВИСНОВКИ

Кваліфікаційна робота підтвердила важливість та необхідність системного моніторингу для забезпечення стабільної, ефективної та безпечної роботи комп'ютерних систем та мереж. Сучасні тенденції розвитку ІТ-інфраструктур, такі як хмарні обчислення, віртуалізація, Інтернет речей (IoT), мікросервісна архітектура та зростання кіберзагроз, ставлять перед системами моніторингу нові, складні завдання, що вимагають впровадження інноваційних підходів та технологій.

Дослідження показало, що системи моніторингу еволюціонують від простих інструментів збору метрик до складних аналітичних платформ, здатних передбачати проблеми, автоматично реагувати на інциденти та надавати глибоке розуміння стану системи. Ключовими функціями таких систем є збір та аналіз даних, візуалізація, сповіщення, інтеграція з іншими системами та забезпечення кібербезпеки. Важливими аспектами є також віддалений моніторинг, інтеграція з SCADA-системами та забезпечення кібербезпеки.

Аналіз перспектив розвитку систем моніторингу виявив кілька ключових напрямків. Одним з найважливіших є інтеграція штучного інтелекту (ШІ) та машинного навчання (ML), що дозволяє автоматизувати аналіз даних, прогнозувати проблеми та оптимізувати роботу системи. Концепція Observability (спостережуваність) виходить за рамки традиційного моніторингу, пропонуючи повне уявлення про внутрішній стан системи на основі зовнішніх даних, що досягається шляхом інтеграції даних з різних джерел та їх кореляції.

З розвитком хмарних технологій та мікросервісів зростає потреба в моніторингу динамічних та розподілених середовищ. Системи моніторингу повинні автоматично адаптуватися до змін в конфігурації таких середовищ та забезпечувати моніторинг на рівні окремих контейнерів та сервісів. Зі збільшенням обсягів даних, що генеруються мережевими пристроями, зростає роль технологій Big Data та потокової обробки даних. Безпека залишається пріоритетним аспектом, з акцентом на використання SIEM-систем та методів машинного навчання для виявлення кібератак. Автоматизація процесів

моніторингу та реагування на інциденти дозволяє зменшити ручну працю та підвищити ефективність управління мережею. Розвиток Edge Computing дозволяє перенести частину обробки даних на периферію мережі, а розвиток інтероперабельності між різними системами моніторингу дозволяє створити більш гнучкі та інтегровані рішення.

Проведене порівняння різних засобів моніторингу, таких як Zabbix, Nagios, PRTG Network Monitor та SolarWinds, показало, що вибір оптимального рішення залежить від конкретних потреб та ресурсів організації. Для великих підприємств з комплексними вимогами, включаючи інтеграцію з SCADA та IoT, найбільш підходящим є SolarWinds. Для малих та середніх підприємств, які шукають просте у використанні рішення, оптимальним є PRTG Network Monitor. Zabbix та Nagios, як open-source рішення, підходять для організацій з обмеженим бюджетом та наявністю технічних фахівців для налаштування.

У результаті дослідження було підтверджено, що системи моніторингу є критично важливими для забезпечення ефективної, безпечної та надійної роботи сучасних IT-інфраструктур. Вони еволюціонують в складні, інтелектуальні та автоматизовані платформи, здатні аналізувати великі обсяги даних, прогнозувати проблеми та автоматично реагувати на інциденти. Вибір оптимального рішення залежить від конкретних потреб організації та специфіки її діяльності. Подальший розвиток систем моніторингу буде тісно пов'язаний з впровадженням новітніх технологій, таких як ШІ, ML, хмарні обчислення, IoT та автоматизація, що дозволить створити ще більш ефективні та інтелектуальні системи, здатні забезпечити високу доступність, надійність та безпеку сучасних IT-інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kim J. he Phoenix Project. A Novel About It, Devops, And Helping Your Business Win / Jin Kim., 2020.
2. A.Mohyuddin. The Art of Network Monitoring. URL:
<https://www.cscan.org/download/?id=394>.
3. Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey Author links open overlay panel Mahmoud Abbasi. URL:
<https://www.sciencedirect.com/science/article/pii/S0140366421000426>.
4. Bojkovic, Z. Integration of monitoring tools in IT management and cloud environments/ Bojkovic, Z., Bakmaz, A. // Journal of Cloud Computing: Advances, Systems and Applications. 2020. URL:
https://www.researchgate.net/publication/372443181_Tool_Integrations_for_Monitoring_Solutions_and_Associated_Performance_Analysis
5. Терещенко О. П. Основні напрями здійснення моніторингу комп'ютерних систем /Терещенко О. П., Погореловська І.Д. //Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції. Digital transformation of the financial system of Ukraine and V4 countries in the context of european integration. Збірник тез IV міжн. наук.-практ. Інтернет-конф. (Дубляни, 16 травня 2024 р.). Частина II. Дубляни: ЛНУП, 2024. с. 329-334.
6. Network Monitoring for SDN Virtual Networks. URL:
<https://ieeexplore.ieee.org/abstract/document/9155260>.
7. ECG Monitoring Systems: Review, Architecture, Processes, and Key Challenges. URL: <https://www.mdpi.com/1424-8220/20/6/1796>.
8. A Review on Data-Driven Condition Monitoring of Industrial Equipment URL:
<https://www.mdpi.com/1999-4893/16/1/9>.
9. Hemanth G. AI-Augmented Database Management Systems for Real-Time Data Analytics. Gadde Hemanth. URL:
<http://redcrevistas.com/index.php/Revista/article/view/152>.
10. Kyle Kingsbury. Monitoring Distributed Systems / Kyle Kingsbury . URL:
<https://www.google.com/url?sa=E&source=gmail&q=https://queue.acm.org/detail.cfm?id=2898444>.
11. Network Monitoring Explained. URL:
https://en.wikipedia.org/wiki/Network_monitoring .
12. Open Source Monitoring Tools: Nagios Core, Zabbix. URL:
<https://www.nagios.org/>.
13. Zabbix Proxy for Distributed Monitoring. URL:
<https://www.zabbix.com/documentation/7.2/en/manual/concepts/proxy?hl=Prox%2Cprox>

14. Prometheus Federated Setup Documentation. URL: <https://prometheus.io/docs>.
15. Julius Volz. System Monitoring with Prometheus. URL: <https://www.youtube.com/watch?v=9GMWvFcQjYI>.
16. SNMP-Based Network Mapping and Fault Management. URL: https://link.springer.com/chapter/10.1007/978-981-16-0878-0_62.
17. Gerhards, R. The Syslog protocol 15. Gerhards, R. // Internet Engineering Task Force. 2009. URL: <https://doi.org/10.17487/RFC5424>
18. Network Forensics: A Comprehensive Review of Tools and Techniques. URL: <https://www.semanticscholar.org/paper/Network-Forensics%3A-A-Comprehensive-Review-of-Tools-Qureshi-Tunio/c2ce749dedb9fe68586abf447384c49ecdef7548?p2d>
19. Montgomery, D. C. Applied Statistics and Probability for Engineers/ Montgomery, D. C., Runger, G. C. //John Wiley & Sons. 2014. URL: <https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/088-Applied-Statistics-and-Probability-for-Engineers-Douglas-C.-Montgomery-George-C.-Runger-Edisi-5-2011.pdf>.
20. Ferguson, G. A. Statistical Analysis in Psychology and Education/ Ferguson, G. A., Takane, Y. //McGraw-Hill. 1989. URL: <https://archive.org/details/statisticalanaly0000geor>.
21. Pearson Correlation Coefficient / Benesty, J., Chen, J., Huang, Y., Cohen, I. // Springer Topics in Signal Processing. 2009. URL: https://www.researchgate.net/publication/226642299_Pearson_Correlation_Coefficient.
22. Chandola, V. Anomaly detection: A survey. ACM Computing Surveys (CSUR) / Chandola, V., Banerjee, A., Kumar, V. URL: https://www.researchgate.net/publication/220565847_Anomaly_Detection_A_Survey.
23. Tufte, E. R. The Visual Display of Quantitative Information / Tufte, E. R. // Graphics Press. 2001. URL: <https://kyl.neocities.org/books/%5BTEC%20TUF%5D%20the%20visual%20display%20of%20quantitative%20information.pdf>.
24. Morrison, M. Effective Data Visualization: The Right Chart for the Right Data / Morrison, M. // SAGE Publications. 2012. URL: https://books.google.com.ua/books/about/Effective_Data_Visualization.html?id=iIWKDwAAQBAJ&redir_esc=y.
25. Spatial Data Visualization With Python: Techniques, Tools, and Real-World Applications URL: <https://www.igi-global.com/chapter/spatial-data-visualization-with-python/347436>.
26. Distributed Systems Observability URL: <https://unlimited.humio.com/rs/756-LMY-106/images/Distributed-Systems-Observability-eBook.pdf>.

27. Cryptography and Network Security: Principles and Practice URL:
[https://www.kufunda.net/publicdocs/Cryptography%20and%20Network%20Security%20Principles%20and%20Practice%20\(6th%20Edition\)%20\(William%20Stallings\).pdf](https://www.kufunda.net/publicdocs/Cryptography%20and%20Network%20Security%20Principles%20and%20Practice%20(6th%20Edition)%20(William%20Stallings).pdf).
28. Bauer, L. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems and Applications / Bauer, L., Livshits, B. // O'Reilly Media. – 2013. URL: <https://www.oreilly.com/library/view/building-secure-and/9781492083115/>.
29. Zabbix Documentation. URL: <https://www.zabbix.com/documentation/>.
30. Nagios Documentation. URL: <https://www.nagios.org/documentation/>.
31. PRTG Network Monitor. URL: <https://www.paessler.com/prtg>.
32. SolarWinds Overview. URL: <https://www.solarwinds.com/products>.
33. SMA Solar Technology. Sunny Portal Overview. URL: <https://www.sma-solar.com/en/home.html> .
34. SolarEdge Technologies. Monitoring Solutions. URL: <https://www.solaredge.com/us/products/monitoring> .
35. Ковальчук, В. О. Основи моніторингу та аналізу даних у комп'ютерних системах /Ковальчук, В. О. 2020. URL:
<https://learn.ztu.edu.ua/mod/resource/view.php?id=203224>.
36. Михайлов, В. І. Особливості моніторингу сонячних електростанцій та інтеграція з SCADA-системами /Михайлов, В. І. 2023. URL:
https://iate.kpi.ua/uploads/p_21_54785228.pdf
37. Garlan, D. An Introduction to Software ArchitectureAdvances in Software Engineering and Knowledge Engineering / Garlan, D., Shaw, M. // World Scientific. – 1993. URL: https://link.springer.com/chapter/10.1007/978-3-540-74343-9_1
38. Tomic, P. The evolution of monitoring techniques in computer systems: Accuracy, completeness, and incident detection time. / Tomic, P., Zeljko, J. // Journal of Network and Computer Applications. 2019. URL:
<https://www.sciencedirect.com/science/article/abs/pii/S1084804518303692?via%3Dihub>
39. What Is a System Monitor? URL:
<https://web.archive.org/web/20101207054610/https://www.wisegeek.com/what-is-a-system-monitor.htm>.
40. Jain, P. Cost of ownership in IT monitoring systems: Optimization and financial implications. /Jain, P., Arora, P. //Journal of Computer Science and Technology. 2018. URL: <https://link.springer.com/article/10.1007/s11390-018-1817-4>
41. Ding, Y. Future perspectives and advancements in network monitoring systems / Ding, Y., Liu, X. // International Journal of Network Management. – 2020. URL:
<https://onlinelibrary.wiley.com/doi/epdf/10.1002/nem.2156>

42. Integrating AI and Machine Learning into SIEM Systems URL:
<https://securetrust.io/blog/integrating-ai-and-machine-learning-into-siem-systems/>
43. Measuring the effect of monitoring on a cloud computing system by estimating the delay time of requests URL:
<https://www.sciencedirect.com/science/article/pii/S1319157821000409>.
44. Simran Baheti. Challenges and Innovations in Cybersecurity / Simran Baheti URL: https://www.researchgate.net/publication/348744351_Challenges_and_Innovations_in_Cybersecurity.
45. The Future of Observability: Trends and Innovations in Data and Application Monitoring URL: <https://www.insightsfromanalytics.com/post/the-future-of-observability-trends-and-innovations-in-data-and-application-monitoring>.
46. Bangar Raju Cherukuri. Containerization in cloud computing: comparing Docker and Kubernetes for scalable web applications / Bangar Raju C48.herukuri //2024 URL:
https://www.researchgate.net/publication/385481942_Containerization_in_cloud_computing_comparing_Docker_and_Kubernetes_for_scalable_web_applications.
47. Akbar Sharief Shaik. ADVANCEMENTS IN REAL-TIME STREAM PROCESSING: A COMPARATIVE STUDY OF APACHE FLINK, SPARK STREAMING, AND KAFKA STREAMS / Akbar Sharief Shaik URL:
https://iaeme.com/Home/article_id/IJCET_15_06_052.
48. Van-Hau Nguyen. Edge Computing for Real-Time Internet of Things Applications: Future Internet Revolution / Van-Hau Nguyen URL:
https://www.researchgate.net/publication/372654016_Edge_Computing_for_Real-Time_Internet_of_Things_Applications_Future_Internet_Revolution#:~:text=Edge%20computing%20enables%20data%20processing,capabilities%20%5B12%2C%2013%5D%20..
49. A Deep Dive into OpenTelemetry and Prometheus Metrics URL:
<https://betterstack.com/community/guides/observability/opentelemetry-metrics-vs-prometheus-metrics/>.