Міністерство освіти і науки України
Харківський національний університет
радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Другий (магістерський)
(рівень вищої освіти)

Розробка автоматизованого модуля моніторингу параметрів об'єктів критичної інфраструктури
(тема)

Виконав:
студент 2 курсу, групи КТРСм-22-1

Рак О.О.
(прізвище, ініціали)

Спеціальності 151 Автоматизація та комп'ютерно-інтегровані технології
(код і повна назва спеціальності)

Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма «Комп'ютеризовані та робототехнічні системи»
(повна назва освітньої програми)

Керівник доц. Максимова С.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри КІТАР _____ Невлюдов І. Ш.
(підпис) (прізвище, ініціали)

2024р.

Я, як студент ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

10.01.24  Рак О.О.

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Факультет АКТ

Кафедра КІТАР

Рівень вищої освіти другий (магістерський)

Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології

Тип програми Освітньо-професійна
Освітня програма «Комп'ютеризовані та робототехнічні системи»

(шифр і назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри КІТАР _____
(підпис)
« » 20_р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Раку Олексію Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка автоматизованого модуля моніторингу параметрівоб'єктів критичної інфраструктури»

Затверджена наказом по університету від 03.11.23 № 1288Ст

2. Термін подання студентом роботи до екзаменаційної комісії
3. Вихідні дані до роботи
3.1 Розробки системи моніторингу
3.2 Автоматизований моніторинг
3.3 Об'єкти критичної інфраструктури
3.4 Сучасні прилади та системи моніторингу

4. Перелік питань, що потрібно опрацювати в роботі
Вступ. Аналіз технічного завдання. Аналіз актуальності розробки автоматизованого модуля моніторингу параметрів об'єктів критичної інфраструктури. Визначити принципи створення модулю віддаленого керування параметрів об'єктів критичної інфраструктури. Розробка сценарію автоматизованого розгортання системи моніторингу параметрів об'єктів критичної інфраструктури. Висновки. Додатки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Демонстраційний матеріал, представлений у форматі презентації PowerPoint (*.ppt) – кіл. с. формату А4.: мета, актуальність, задачі роботи; актуальності розробки автоматизованого модуля моніторингу параметрів об'єктів критичної інфраструктури; розробка сценарію автоматизованого розгортання системи моніторингу; висновки.*

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз технічного завдання.	05.12.23	Виконано
2	Аналіз актуальності розробки автоматизованого модуля моніторингу параметрів об'єктів критичної інфраструктури	05.12.23	Виконано
3	Аналіз сучасних приладів та систем моніторингу	10.12.23	Виконано
4	Розробка структури та розробки автоматизованої системи моніторингу	18.12.23	Виконано
5	Проектування інфраструктури системи моніторингу	22.12.23	Виконано
6	Розробка сценарію автоматизованого розгортання системи моніторингу	25.12.23	Виконано
7	Оформлення пояснювальної записки	07.01.24	Виконано
8	Оформлення презентаційних матеріалів	10.01.24	Виконано
9	Подання кваліфікаційної роботи в ЕК	15.01.24	
11			

Дата видачі завдання 03.11.23

Студент _____ Рак О.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доц. Максимова С.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 68 с., 30 рис., 4 дод., 13 джерел.

МОНІТОРИНГ, КРИТИЧНІ СИТУАЦІЇ, КРИТИЧНІ ОБ’ЄКТИ, КРИТИЧНА ІНФРАСТРУКТУРА.

Метою роботи є підвищення ефективності керування параметрів об’єктів критичної інфраструктури.

Об’єктом дослідження є процес віддаленого керування параметрів об'єктівкритичної інфраструктури.

Предметом дослідження є модуль віддаленого керування параметрів об’єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз літератури за темою дослідження;

– провести аналіз існуючі розробки;

– визначити принципи створення модулю віддаленого керування параметрів об’єктів критичної інфраструктури;

– обрати необхідне обладнання для розробки модуля;

– розробити программу автоматизованого модуля моніторингу параметрів об’єктів критичної інфраструктури.

ABSTRACT

Explanatory note to revenge: 68 p., 30 pic., 4 app., 13 sources.

MONITORING, CRITICAL SITUATIONS, CRITICAL FACILITIES, CRITICAL INFRASTRUCTURE.

The aim of the study is to improve the efficiency of controlling the parameters of criticalinfrastructure facilities.

The object of study is the process of remote control of critical infrastructure parameters.

The subject of the study is a module for remote control of critical infrastructure parameters.

To achieve this goal, the following tasks need to be solved:

– analyze the literature on the research topic;

– analyze existing developments;

– to determine the principles of creating a module for remote control of critical infrastructure parameters;

– to select the necessary equipment for the development of the module;

– to develop a program for an automated module for monitoring the parameters of criticalinfrastructure facilities.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АСМ – автоматична система моніторингу; АСОД – автоматизована система обробки даних;

АТ – список АТ-команд з коротким описом;

ІТ – інформаційні технології;

КІТАР – кафедра комп’ютерно–інтегрованих технологій, автоматизації та робототехніки;

ПЗ – програмне забезпечення;

САПР - система автоматизованого проектування;

ХНУРЕ – харківський національний університет радіоелектроніки;

IoT – internet of things – інтернет речей.

ВСТУП

Забезпечення безпеки життя та діяльності людини – як окремого громадянина країни та як члена організованих колективів (виробничих, громадських, навчальних, спортивних колективів тощо) є пріоритетом держави, найважливішим завданням, гарантованим державними інституціями та Законом України. Це реалізується, зокрема, комплексом взаємопов’язаних процесів: моніторингу (динамічному контролю) поточної ситуації; попередження та (або) виявлення (ідентифікація) небезпечних і потенційно небезпечних подій (критичних ситуацій (КС)); планування й здійснення заходів протидії та ліквідації наслідків небезпечних подій; облік і ретроспективний аналіз КС та дій щодо їх ліквідації.

Критична інфраструктура сьогодні є в кожному місті. Вона складається з сукупності певних об'єктів, систем і засобів, що забезпечують життєдіяльність на різних рівнях: на рівні окремого міста, області, країни в цілому, і загалом впливають на стан і розвиток суспільства та економіки. До критичної інфраструктури відносять об'єкти енергетики та електропостачання, водопостачання, теплопостачання, транспорту, зв'язку, а також об'єкти, що забезпечують функціонування державних органів, фінансової системи, обороноздатності тощо.

Забезпечення безперебійної роботи критичної інфраструктури та захисту її від зовнішніх впливів є одним із найважливіших завдань державного рівня. Одним із способів забезпечення ефективної та безперебійної роботи критичної інфраструктури є автоматизований моніторинг її параметрів. У створенні системи моніторингу використовують інформаційні технології (ІТ), що удосконалюються з кожним роком. Сучасні ІТ та рішення використовуються на етапах проєктування, розробки та впровадження автоматизованого модуля моніторингу параметрів об’єктів критичної інфраструктури.

Автоматизований моніторинг параметрів об'єктів критичної інфраструктури – це комплекс заходів, спрямованих на отримання, обробку та аналіз інформації про стан об'єктів критичної інфраструктури в режимі реального часу.

Таким чином метою кваліфікаційної роботи є впровадження автоматизованого модуля моніторингу параметрів об’єктів критичної інфраструктури.

Об’єкт дослідження – процес віддаленого керування параметрами об'єктів критичної інфраструктури.

Предмет дослідження – модуль віддаленого керування параметрами об’єктів критичної інфраструктури.

Мета дослідження – підвищення ефективності керування параметрами об’єктів критичної інфраструктури шляхом розробки автоматизованої системи моніторингу.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– провести аналіз літератури за темою дослідження;

– провести аналіз розробок, що існують;

– визначити принципи створення модулю віддаленого керування параметрами об’єктів критичної інфраструктури;

– обрати необхідне обладнання для розробки модуля;

– розробити програму автоматизованого модуля моніторингу параметрів об’єктів критичної інфраструктури;

– показати додану наукову публікацію за темою роботи;

– оформити пояснювальну записку згідно з рекомендаціями [1], та вимогами ДСТУ 3008:2015 [2];

– результати даної кваліфікаційної роботи представлені у науковій статті, яку можна знайти в гугл-академії [3].

1 ОГЛЯД ТА АНАЛІЗ МАТЕРІАЛІВ ЗА ТЕМОЮ РОБОТИ

1.1 Актуальність розробки системи моніторингу

У сучасному світі всі потужні виробництва використовують системи автоматизації, регулярно перевіряють їх дію та удосконалюють. Системи автоматизації дозволяють контролювати всі етапи технологічного процесу на виробництві та стан апаратури в режимі реального часу. Саме автоматизація багатьох ланок виробництва підвищує ефективність роботи, сприяє вивільненню робітників від тяжкої чи монотонної фізичної праці, що в цілому забезпечує ефективну роботу підприємства, знижує ризик виникнення людських помилок і травматизації, оптимізує собівартість продукції.

Разом із тим періодично виникають проблеми, якщо обладнання підприємств застаріле або використовується тривало, та іноді вже не може підтримувати необхідні функції на потрібному високому рівні. У першу чергу це пов'язано з відсутністю певних складових, наприклад, необхідних датчиків, а також відповідного програмного забезпечення. Такі обмеження стають перешкодою для повноцінного впровадження систем автоматизації на підприємствах.

Одним із шляхів оптимізації виробництва є оновлення обладнання та програмного забезпечення. Повна заміна виробничого обладнання коштує дуже дорого, і тому актуальним завданням є створення нових або удосконалення окремих ланцюгів виробництва, одним із яких є система моніторингу. Ці системи повинні бути спроможними інтегруватися в необхідні частини виробничого процесу, а також бути доступними за ціною та зручними в роботі для людини. Використовуючи них, підприємства зможуть поступово запроваджувати нові технології на інших ланках без надмірних витрат.

Наша робота присвячена розробці системи моніторингу. Ми пропонуємо побудувати модель такої системи моніторингу й візуалізації в комплексі з програмним забезпеченням, які б забезпечували, з одного боку, адекватну роботу самої системи, а з другого – дозволяли користувачеві швидко отримувати необхідну інформацію та своєчасно реагувати на неї. Застосування такої системи моніторингу стане кроком у напрямку розвитку та модернізації підприємства. Саме такий підхід дозволить підприємствам поступово запроваджувати нові технології, підвищувати ефективність виробництва та забезпечувати якісний контроль над технологічним процесом і

продукцією. З іншого боку, саме такі загальні характеристики, як продуктивність, новітність, інноваційність і ефективність складають основу успішного бізнесу.

Система моніторингу в структурі управління інфраструктурою підприємства за мету має ретельне спостереження за параметрами робочого процесу, відстеження та аналіз змін, що відбуваються з ними. Отримання, збереження та аналіз інформації про стан елементів структури є основними завданнями систем моніторингу. Завдяки ним відбувається своєчасне виявлення проблем, які можуть виникнути під час роботи, збоїв та поломок якогось технологічного ланцюжка чи пристрою. Безпосередньо це і є основною метою функціонування системи моніторингу, що убезпечує від отримання бракованої та некондиційної продукції, шкоди для виробників і користувачів, від створення надзвичайних ситуацій і, відповідно, матеріальних втрат для підприємства та суспільства.

На будь-якому підприємстві сьогодні технологічний процес вимагає автоматизації систем управління й моніторингу. При цьому періодично виникає потреба в удосконаленні цих систем відповідно до нових завдань, з урахуванням сучасних тенденцій розвитку науки, отримання нових знань і впровадженні більш зручних інформаційно-комп’ютерних технологій. Як приклад інформаційно-технологічної системи можна навести промисловий інтернет речей (IoT), масштаби якого сьогодні вражають. Система IoT дозволяє збирати значні масиви інформації з різних куточків світу, обмінюватися інформацією, дистанційно керувати процесами виробництва, логістики й торгівлі.

Позитивним моментом з точки зору ефективності та рентабельності виробництва є впровадження автоматизованої системи з модулем обробки інформації, що дозволяє вивільнити людський персонал і знизити можливий ризик людської недбалості. Використання хмарного сервісу, такого як Microsoft Azure, забезпечує практично безстрокове зберігання та надійний захист інформації. Такий інструмент, як веб-додаток для моніторингу дозволяє керівникові оперативно реагувати на виникнення неполадок і проблем при роботі сервісів.

Отже, надійне функціонування системи моніторингу за ключовими параметрами під час робочого процесу забезпечує ефективність виробництва, безпеку для людини, та створює умови для подальшого розвитку підприємства та бізнесу. Тому виникла ідея створення подібної системи, яка буде автоматизованою системою моніторингу та управління параметрами об'єктів критичної інфраструктури. Автоматизований моніторинг параметрів об'єктів критичної інфраструктури має суттєві переваги порівняно з традиційним ручним моніторингом:

– підвищує оперативність отримання інформації про стан об'єктів

критичної інфраструктури;

– забезпечує більш точне та об'єктивне отримання інформації;

– дозволяє значно скоротити витрати на моніторинг;

– підвищує безпеку критичної інфраструктури;

– унеможливлює фактор людської недбалості при контролі за параметрами об'єктів критичної інфраструктури.

Таким чином, тема дослідження, що присвячена проблемі розробки автоматизованого модулю керування для об’єктів критичної інфраструктури є актуальною.

1.2 Об'єкти критичної інфраструктури

Об'єкти критичної інфраструктури в сучасному житті суспільства відіграють надзвичайно важливу роль. Вони забезпечують нормальне функціонування економіки в країні, забезпечують безпеку та комфорт громадян. Такі об'єкти забезпечують різні сторони життя людей. Вони включають різноманітні споруди та підприємства: електростанції та енергетичні споруди, системи водопостачання та водовідведення, транспортну інфраструктуру, телекомунікаційні мережі, інформаційні технології, системи охорони здоров'я та інші соціально-економічні сектори.

Електростанції та нафто-газопроводи є основними об’єктами енергетики, що забезпечують енергією всю країну. Вони забезпечують і побутову електрику, що дуже важливо для кожної людини, і необхідні ресурси для промисловості та господарства. Транспортна інфраструктура: аеропорти, залізниці, автовокзали, мости та тунелі, – є необхідною для забезпечення мобільності та перевезення людей та грузів. Системи водопостачання та водовідведення забезпечують населення водою для пиття та господарських потреб, а також відведення стічних вод. У промисловості вода необхідна для багатьох процесів, бо вона є розчинником, необхідна для хімічних процесів, потрібна для миття, для охолодження систем тощо.

Телекомунікаційні мережі та інформаційні технології забезпечують зв'язок та доступ до інформації. Системи охорони здоров'я, такі як лікарні та медичні центри, забезпечують медичну допомогу населенню. Інші соціально-економічні сектори, такі як фінансові установи, продуктові ринки та громадські служби, також відіграють важливу роль у житті суспільства.

Автоматизовані модулі моніторингу відповідають за безперервний нагляд за станом об'єктів критичної інфраструктури. Вони контролюють стан технічного обладнання, вимірюють і контролюють низку важливих параметрів, забезпечують

безпеку та доступність послуг. Це дозволяє забезпечити надійність та ефективність функціонування цих об'єктів для людини, суспільства та країни в цілому.

1.3 Автоматичний моніторинг

Відповідно до стандарту, автоматизована система управління (АСУ) призначена для забезпечення ефективної роботи об'єкта управління шляхом автоматизованого виконання управлінських функцій. АСУ складається з різних компонентів, таких як інформаційне, програмне, технічне, організаційне, метрологічне, правове та лінгвістичне забезпечення [1]. У цілому, основні функції АСУ включають такі елементи (дії):

- планування; та (або) прогнозування;
- облік, контроль, аналіз;
- координацію і (або) регулювання;
- прогнозування.

Вибір необхідних компонентів залежить від типу конкретної АСУ. Залежно від функцій та типу процесу, що контролюється, можна виділити такі типи АСУ: адміністративно-організаційні, технологічні (для управління технологічними процесами) та інтегровані [1].

Серед багатьох сучасних систем автоматизованого управління виробництвом (АСУВ) існують такі, які вимагають ручного введення даних оператором. Оскільки об'єкти управління розподілені, ефективне виконання функцій системи автоматизованого збору, введення і зберігання даних (АСУП) набуває великої ваги. Тому розробка засобів для організації ручного введення даних є важливою задачею в сучасних АСУП. Таким чином, область наших інтересів лежить в частині АСУП і їх підсистем, що забезпечують наступні функції:

- збір даних і контроль;
- приведення до потрібного формату, первинна обробка даних;
- організація зберігання і надання доступу до збережених даних;
- аналітична обробка даних моніторингу;
- генерація запитів;
- генерація звітних форм, візуалізація звітів.

Функціонал, що використовується, полягає у використанні автоматизованої системи обробки даних (АСОД). АСОД відповідає за збір інформації, її обробку, надання керуючих впливів на об'єкт управління, а також надання результатів обробки

інформації людині для прийняття управлінських рішень або для інших цілей [2]. Залежно від призначення автоматизованої системи обробки даних (АСОД), різні функції можуть бути реалізовані та використовуватися в різній мірі. Це призводить до існування різних типів АСОД. Проте, класифікація є неоднозначною, оскільки критерій віднесення системи до певного типу не є чітким, а набір функцій, які виконуються системами, перетинається. За сферою застосування автоматизовані системи обробки даних можна розділити на наступні групи.

Інформаційні системи організаційного управління [3] [4]. Призначені для автоматизації функцій управлінського персоналу [5].

Автоматизовані системи управління технологічними процесами (АСУ ТП). Це комплекс програмних і технічних засобів, призначений для автоматизації управління технологічним обладнанням на підприємствах [6].

Системи автоматизованого проектування (САПР). Ці системи призначені для автоматизації роботи інженерів-проектувальників, інженерів-конструкторів, архітекторів та дизайнерів у процесі створення нової техніки, виробів і продуктів. Основними функціями таких систем є проведення інженерних розрахунків, створення графічної документації (креслень, схем, планів), розробка проектної документації та моделювання проектованих об'єктів [7]. Інтегровані (корпоративні) інформаційні системи використовуються для автоматизації всіх функцій підприємства і охоплюють весь цикл робіт від проектування до збуту продукції [8] [9] [10] [11].

У пошукових системах немає можливості керувати об'єктом, тоді як у системах автоматизованого управління технологічним процесом це є ключовим аспектом. В АСУ ТП оброблені дані можуть бути використані для отримання інформації про стан системи або для цілеспрямованої зміни її стану.

Автоматизована система обробки даних (АСОД) інформаційного характеру використовується для пошуку та аналізу інформації. Вона призначена для задоволення потреб людини, яка є її користувачем. Зазвичай, такі системи працюють з невеликим обсягом вхідних даних, але мають великі постійні або повільно змінюються масиви даних. З іншого боку, АСОД керуючого типу використовується для цілеспрямованої зміни стану об'єкта управління або керування процесом його функціонування. Для успішного управління такою системою необхідно мати наступну інформацію:

– як поводиться об'єкт управління (його стану в задані моменти часу);
– які є некеровані зовнішні впливи на об'єкт (впливу зовнішнього середовища);
– яка мета управління;

– якими засобами впливу на об'єкт можна розташовувати (які ресурси є) [12].

Для реалізації складних законів управління потрібні складні алгоритми і реалізують їх програмні комплекси, що є характерною особливістю АСОД керуючого типу в порівнянні з інформаційними системами. Інша відмінність - наявність жорстких обмежень на час вирішення завдань управління, що обумовлено високою швидкістю зміни збурень, що діють на об'єкт.

Тим чином будь-яка АСОД тим чи іншим чином входить до складу автоматизованої системи управління. Це підтверджується, зокрема, схожістю наведених класифікацій АСУ і АСОД по виконуваних функцій і виду керованого процесу. Таким чином, і систему моніторингу, що реалізує ті чи інші функції збору, зберігання і обробки даних, можна вважати складовою частиною АСУ [13].

З наведених вище видів АСОД функції ручного введення даних складають істотну частину функціональності в інтегрованих (корпоративні) інформаційних системах та інформаційних системах організаційного управління. І ті й інші належать до класу автоматизованих систем управління виробництвом (АСУВ) [14]. У структурі АСУП прийнято виділяти функціональні і забезпечують підсистеми.

До групи функціональних підсистем входять такі підсистеми, як управління технічною підготовкою виробництва, основним та допоміжним виробництвом, матеріально-технічним постачанням, техніко-економічним плануванням, бухгалтерським обліком, збутом, кадрами, якістю продукції та фінансами. Залежно від складу та завдань основних функціональних відділів планування і управління, автоматизована система управління повинна забезпечувати автоматизацію відповідних функцій [15].

До складу АСУ входять технічне, інформаційне, математичне, програмне та організаційне забезпечення [1] [16].

Технічне забезпечення – це комплекс технічних засобів, що включає засоби обчислювальної техніки, обладнання для організації локальних мереж і підключення до глобальних мереж, пристрій реєстрації, накопичення та відтворення інформації.

Інформаційне забезпечення має дві частини: зовнішнє та внутрішнє. Зовнішнє забезпечення включає вхідні та вихідні дані, які використовуються для вирішення різних завдань. Внутрішнє забезпечення спрямоване на організацію бази даних підприємства.

Математичне забезпечення включає в себе різні математичні методи, моделі та алгоритми, які використовуються для вирішення управлінських завдань.

Програмне забезпечення включає системне програмне забезпечення, спеціальні

програми для управління, а також інші програми, які використовуються на підприємстві.

Організаційне забезпечення складається з набору правил, інструкцій, положень та інших документів, що регламентують функціонування АСУП.

Кожен тип забезпечення в різних формах визначає та реалізує вимоги до процедур збору інформації. Дані надходять на різних етапах роботи великою кількістю і регулярно. Однак, коли йдеться про управління, цих даних часто виявляється недостатньо. Кожне завдання має свої вимоги до складу та структури показників. Тому потрібна підсистема збору даних, яка зможе реєструвати дані, введені вручну, незалежно від їх предметної специфіки.

Для того, щоб продемонструвати функції збирання, зберігання та оброблення даних у системі моніторингу в АСУ, згадаймо класичний контур керування АСУ [17]. Коли вплив змінює стан об'єкта, він надходить на об'єкт управління. Отриманий стан об'єкта управління реєструється вимірювальним механізмом, який оцінює його і передає суб'єкту управління. Уся ця інформація є важливою складовою роботи системи моніторингу, яка забезпечує ефективне функціонування АСУ. Таким чином, система моніторингу відіграє важливу роль у забезпеченні надійності та ефективності роботи АСУ. Вона дає змогу здійснювати контроль та аналіз даних, що є необхідним для прийняття правильних управлінських рішень. Суб'єкт управління після аналізу отриманої оцінки стану видає вектор управління, який приймає і виконує регулятор. Виконання полягає в напрямку на об'єкт управління керуючого впливу (рисунок 1.1).

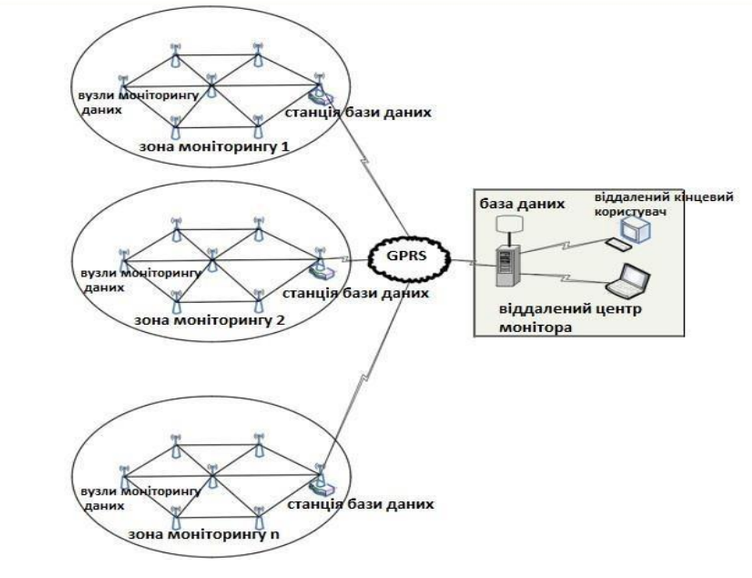

Рисунок 1.1 – Контур управління АСУ

Таким чином, місце системи моніторингу в АСУП схематично можна представити

у вигляді, наведеному на рисунку 1.2.

Рисунок 1.2 – Місце системи в контурі управління

Відстеження як сталих, так і динамічних, що змінюються за часом, характеристик об'єкта, безпосереднє спостереження за процесом управління є сутністю моніторингу відносно до об'єкту.

1.4 Аналіз сучасних приладів та систем моніторингу зовнішніх показників

Параметри, які характеризують середовище, в якому працює об’єкт критичної інфраструктури, називають зовнішніми показниками. До цих показників належать:

– метеорологічні показники (температура, тиск, вологість, вітер, освітленість тощо);

– геофізичні показники (сейсмічна активність, магнітні бурі тощо);

– екологічні показники (забруднення повітря, води, ґрунту тощо);

– інші показники (наприклад, рівень радіації, хімічного забруднення тощо).

Для безперебійної роботи важливих інфраструктур важливим є моніторинг зовнішніх показників. Він дозволяє швидко виявити зміни в навколишньому середовищі, які можуть мати негативний вплив на стан об’єкта.

Сучасні пристрої та системи моніторингу зовнішніх показників мають багато переваг перед традиційними методами:

– вони забезпечують більш точне та об'єктивне вимірювання параметрів;

– вони дозволяють здійснювати моніторинг в режимі реального часу;

– вони мають високу надійність і довговічність;

– вони є більш економічними у використанні.

Приклади використання сучасних приладів та систем моніторингу зовнішніх показників для критичної інфраструктури:

– метеорологічні показники. Для спостереження за погодними умовами, такими як температура, атмосферний тиск, вологість, швидкість вітру, рівень освітленості тощо, використовуються різноманітні прилади і системи, такі як термометри, барометри, гігрометри, анемометри, сонячні датчики тощо. Ці прилади і системи можуть бути розміщені на відкритих майданчиках або в спеціально обладнаних приміщеннях.

Наприклад, для контролю стану повітряних ліній електропередачі використовуються спеціальні пристрої, які здатні вимірювати різні параметри, такі як температура, вологість, тиск, швидкість вітру, рівень забрудненості повітря та інші. Отримана інформація дозволяє прогнозувати можливі пошкодження повітряних ліній та приймати необхідні заходи для їх попередження;

– геофізичні показники. Для моніторингу геофізичних показників, таких як сейсмічна активність, магнітні бурі тощо, використовуються спеціальні прилади та системи, такі як сейсмографи, магнітометри тощо. Ці прилади та системи встановлюються в місцях, де існує підвищений ризик виникнення природних явищ.

Наприклад, для моніторингу сейсмічної активності в районах, де розташовані об'єкти критичної інфраструктури, використовуються сейсмографи. Ці прилади дозволяють своєчасно виявляти землетруси та інші сейсмічні явища, що можуть призвести до пошкоджень об'єктів;

– екологічні показники. Для моніторингу екологічних показників, таких як ступінь забруднення атмосфери, води, грунту тощо, використовуються різноманітні пристрої та системи, такі як газоаналізатори, хімічно-аналітичні пристрої і т.д. Ці технічні засоби встановлюються на місцях, де виявлено джерела забруднення навколишнього середовища.

Відомо, що для оцінки й динамічного моніторингу рівня забруднення повітря в районах, де розташовані об'єкти критичної інфраструктури, використовуються газоаналізатори. Ці прилади дозволяють контролювати рівень концентрації шкідливих речовин у повітрі та забезпечувати безпеку працівників та населення.

При проектуванні та розробці систем моніторингу, що базуються на інформаційно-вимірювальних системах, одним із ключових аспектів є визначення множини діагностичних ознак. Обґрунтування вибору конкретних ознак здійснюється через побудову та аналіз математичних моделей об’єктів моніторингу та діагностики, або фізичних процесів, що супроводжують роботу цих об’єктів. Моніторинг, заснований на

аналізі випадкових процесів та полів, включаючи шумову діагностику, ґрунтується, перш за все, на належним чином побудованих математичних моделях. Ці моделі встановлюють зв’язок між фактичним технічним станом об’єкта та певними характеристиками та параметрами, отриманими в результаті обробки вимірювальної інформації. Математична модель може представляти собою випадковий процес або випадкове поле з певного класу, які мають конкретні властивості, що дозволяють оцінити їх за допомогою статистичних чи інших методів, ґрунтуючись на вимірюванні та обробці однієї чи кількох реалізацій процесу (поля). Під час розроблення ймовірнісних математичних моделей фізичних процесів у теплоенергетичному обладнанні найбільш зручними є лінійні випадкові процеси. Ці моделі мають структурований характер, де кожен параметр має певне фізичне значення. Крім того, властивості лінійних випадкових процесів дають змогу отримувати аналітичні вирази для моментів розподілу досліджуваного процесу, а також будувати його функції розподілу або характеристичні функції. Аналіз таких моделей дає змогу теоретично обґрунтовувати діагностичні ознаки, визначати допустимі межі їхньої зміни (діагностичні простори) і розробляти ефективні правила для виявлення та класифікації дефектів. Крім того, використання таких моделей дає змогу застосовувати методи комп'ютерного імітаційного моделювання, що допомагає скоротити витрати часу і грошей на фізичне моделювання процесів моніторингу або експериментальних досліджень на реальному обладнанні.

2 РОЗРОБКА СТРУКТУРИ АВТОМАТИЗОВАНОЇ СИСТЕМИ МОНІТОРИНГУ

2.1 Проектування інфраструктури системи моніторингу

Ключовим моментом нашої роботи стала розробка автоматизованої системи контролю за параметрами, що характеризують виробничий процес і дозволяють контролювати його на всіх послідовних етапах роботи. Одним з важливих складових цієї системи є, безперечно, інформаційно-комп'ютерні технології та сучасні датчики, привабливими є сенсорні датчики. Виробничий процес може відбуватися як на великому підприємстві, заводі, так і на підприємстві середнього чи малого рівня, і ефективне функціонування певного виробництва можна представити такою схемою: закупівля матеріалів, створення матеріального продукту, збут-реалізація продукту й отримання за це матеріальної винагороди – коштів, які не тільки «повертають» затрати, але й дають можливість удосконалення, розширення та навіть преміювання робітників. Використання автоматизованого моніторингу цих ланцюжків безпосередньо полегшує працю та стає чинником підвищення ефективності виробництва.

Для кожного виробництва дуже важливим є забезпечення конкретних фізичних складових умов: температурного режиму, вологості, світла, площі виробничої зони, напруги в електромережі тощо. Дотримання температурного режиму – вкрай необхідна умова на всіх виробництвах, з одного боку – для забезпечення безпосередньо етапів переробки матеріалів та створення продукту, з другого – для збереження здоров'я робітників. Наприклад, недотримання температурного режиму буде вкрай критичним у таких галузях, як металургійна та хімічна промисловість, харчова та фармацевтична. Відхилення від необхідних умов під час виробництва може стати причиною промислового браку або продукту низької якості. Для запобігання цього служать датчики вологості та температури, моніторинг показників яких доцільно налаштувати в робочих зонах, і дані передаватимуться до відповідного каталогу. Кількість таких датчиків може бути будь-якою, залежно від потреби в конкретному місці, і це визначається показниками, що впливають на якість виробленого продукту.

Однією з актуальних задач є створення автоматизованої системи моніторингу фізичних характеристик освітлення, температури, вологості, шуму та вібрації – важливих показників під час робочих процесів на виробництві. Ця система працюватиме за допомогою сенсорів та інформаційно-технічних технологій, з використанням AWS. Робочими процесами вважаються послідовні технологічні етапи

створення з матеріалів кінцевого продукту виробництва і продаж його, що прирівнює виробництво до певного роду бізнесу. Моніторинг при цьому є необхідним додатком для інтенсифікації та підвищення ефективності виробництва.

AWS є важливою частиною даної системи, оскільки саме в веб-хмарі буде розгортатися створений додаток. Завдяки можливостям AWS можна швидко нарощувати ресурси в міру потреби та використовувати різноманітні технології для ефективного впровадження інновацій. AWS також надає широкий спектр інструментів безпеки, і це надійно забезпечує конфіденційність і безпеку даних, і система моніторингу стає більш захищеною.

Забезпечення ефективного та якісного виробництва продукту відповідно технологічних норм досягається завдяки підтримки оптимальних параметрів і, звичайно, сталих факторів середовища. У даній роботі розглядається використання датчиків, що надаватимуть інформацію системі моніторингу, таких як датчик освітлення, температури, вологості, шуму та вібрації. Передбачено створення системи, у якій взаємодіятимуть мікроконтролер, датчики та програмне забезпечення через хмарний веб-сервіс і бездротові технології. Робота детально описує процес створення такої автоматизованої системи моніторингу на виробництві, що схематично представлена на рисунку 2.1.

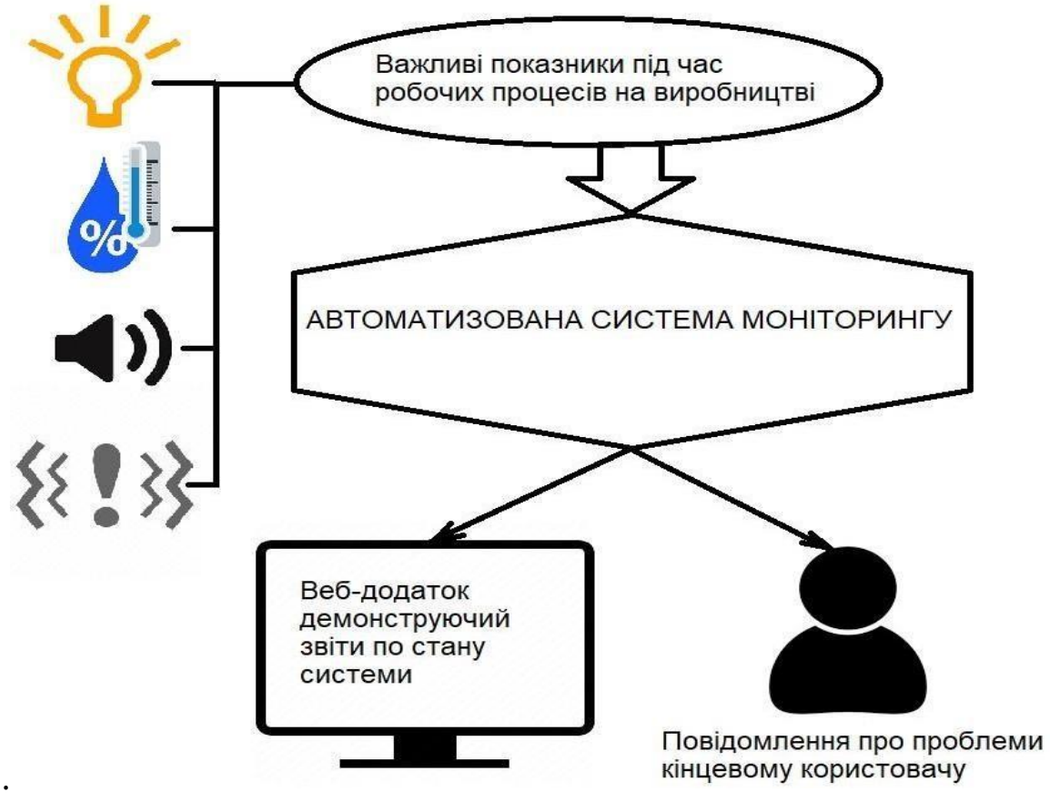

Рисунок 2.1 – Функції автоматизованої системи моніторингу

2.2 Послідовність і принцип дії автоматизованої системи

Для автоматизованої обробки даних з сенсорів шуму, освітлення, температури та вологості, а також вібрації, пропонується розробити систему, яка сприятиме підвищенню ефективності та враховуватиме недоліки сучасних популярних аналогів. Для досягнення цієї мети використовуються компоненти існуючих систем, але з удосконаленими можливостями [18].

Після аналізу технічних документів та відгуків щодо роботи датчиків, мікроконтролерних платформ і апаратно-програмних рішень для обробки інформації на виробництві, прийнято рішення включити до системи, що розробляється, для автоматизації контролю та обліку, такі елементи, які показано на рисунку 2.2.

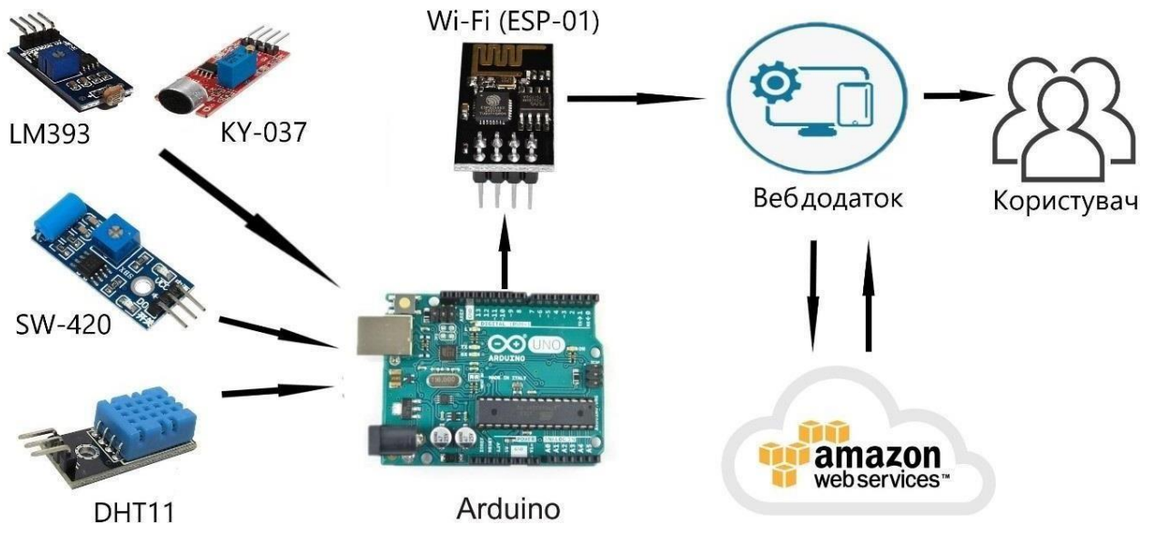

Рисунок 2.2 – Загальна схема роботи автоматизованої системи моніторингу

Wi-Fi модуль ESP-01 є найбільш поширеним серед модулів з серії ESP8266. Керуючий пристрій взаємодіє з ESP8266 через UART (серійний порт) за допомогою команд AT. Робота з передачею та прийомом даних схожа на взаємодію з TCP-сокетом або серійним портом комп'ютера. Програмування та завантаження прошивок можливе через Arduino IDE [19], подібно до взаємодії з Arduino. Реакція на AT-команди представляє собою функцію стандартної прошивки, яка встановлена на заводі.

У зв'язку з наявністю двох портів вводу/виводу на платі, після прошивки можна підключати периферійні пристрої безпосередньо до модуля без додаткового контролера. Для прошивки модуля використовується звичайний програматор, аналогічний тому, що використовується для деяких плат Arduino. Завдяки PCB-антені модуля забезпечується

дальність зв'язку до 400 м на відкритому просторі.

Wi-Fi модуль ESP-01 застосовується в стаціонарних і мобільних пристроях, таких як системи "розумний будинок", рухомі пристрої і компактні переносні пристрої. Завдяки ESP-01 сучасні побутові прилади стають частиною інтернету речей. Бездротовий зв'язок Wi-Fi разом з функцією економного електроспоживання особливо корисні в рухомих апаратах чи комплексах, які мають нестандартні системи живлення, наприклад, від хімічних джерел струму або сонячних батарей, можливо, біотоплива. Модуль ESP-01 якнайкраще підходить для обробки інформації від мікроконтролера до веб-додатку на основі хмарного веб-сервісу AWS.

Модуль датчика LM393 призначений для визначення рівня освітлення (в люксах), а також встановлення відстані до об'єктів і перешкод. Він містить: ІЧ-світлодіод із програмним драйвером, два фотодіоди для визначення загальної освітленості (Ch0) та освітленості в інфрачервоному (ІЧ) діапазоні (Ch1), підсилювачі з програмним коефіцієнтом посилення, мікроконтролер, АЛУ, АЦП, ОЗП, контролер шини I2C (контакти SDA і SCL). Функція датчику освітленості та наближення полягає в забезпеченні змін яскравості екрану залежно від освітленості або зміни відстані до об'єктів – наближення та віддалення від них, що може успішно використовуватися в проєктах Arduino.

Наступний модуль DHT11 є цифровим датчиком вологості та температури. Він має термістор та ємнісний датчик вологості, які забезпечують визначення й слідкування за змінами відповідних характеристик – температури та вологості повітря. Додатково він обладнаний аналого-цифровим перетворювачем (АЦП) для перетворення аналогових значень вологості та температури. Хоча DHT11 має обмежену швидкодію й точність, його простота та доступність забезпечили широке використання, він добре підходить як для контролю температурного режиму та вологості в приміщенні, так і для використання в навчальному процесі.

Задля автоматичного вимірювання та регулювання виробничих шумів доцільно використовувати датчик KY-037, який характеризується високою енергоефективністю в роботи (споживання від 3,1 мА до 6 мА). Особливою перевагою є його здатність автоматично регулювати рівень шумів, добре взаємодіючи з різними акустичними сигналами (збільшуючи тихі звуки та зменшуючи гучні). Вбудований електричний мікрофон чутливий до звуків у діапазоні частот від 22 Гц до 22 кГц. Стандартне підключення модуля до контролера, наприклад, до плати Arduino, здійснюється за допомогою трьох контактів: Vdd (“+”), GND (“-”), OUT (для аналогового входу). За допомогою контакту GAIN можна регулювати значення максимального посилення

гучності (40 дБ, 50 дБ або 60 дБ). Контакт AR використовується для налаштування часу спрацьовування.

Датчик вібрації SW-420 призначений для діагностики наявності та сили вібрацій у системах, що засновані на Arduino. Цей модуль широко застосовується, починаючи від розробки антикрадіжкових систем до створення детекторів прогнозування й фіксації землетрусів. Датчик вібрацій SW-420 чуйно реагує на удари будь-якої сили та вібрації. За допомогою підстроювального резистора налаштовується чутливість модуля. Датчик має невеликі розміри, він укомплектований двома світлодіодами: один з них контролює наявність живлення, а другий вмикається під час спрацьовування. На відміну від інших аналогів цей датчик більш чутливий, для його вмикання достатньо одного поштовху.

На основі зазначених датчиків буде вирішуватись завдання з автоматизації обробки обраних для цілей показників та створення системи. Ця система буде використовувати мікроконтролер Arduino для генерації інформативних графіків у реальному часі на основі вихідних даних [20]. Зображення буде відображатись у вікнах програмного забезпечення, яке, в свою чергу, буде розгорнуто через веб-сервіс AWS.

Моніторинг буде доступний через веб-версію в захищеному середовищі хмарного провайдера, при цьому відсутня необхідність встановлення системи на нові комп'ютери чи інші цифрові пристрої. Для зручного використання ефективної системи, яка допомагатиме підприємству стежити за важливими робочими процесами, достатньо мати доступ лише до веб-версії.

В останні роки широко впроваджуються хмарні обчислення, які забезпечують гнучкість і швидкість робочого процесу, не потребують додаткових людських або технічних ресурсів під час зростання ділової активності на підприємстві або в робочому колективі. Разом із тим створюються умови для миттєвого збільшення або зменшення цих ресурсів відповідно до зміни потреб. Управління базовою інфраструктурою спрощується завдяки контейнерним і оркестровим послугам AWS, що використовуються як локально, так і в хмарі. Це дозволяє фокусуватися на інноваційних розробках і потребах виробництва, установи чи бізнесу. Приблизно 80% усіх контейнерів у хмарі наразі працюють сьогодні на платформі AWS, і цей вибір обумовлений її безпекою, надійністю та масштабністю. Такі великі компанії, як Samsung, Expedia, GoDaddy і Snap, обирають AWS для запуску своїх контейнерів.

AWS IoT надає можливість вибору найбільш відповідних і сучасних технологій для реалізації вашого рішення. Для управління вашими пристроями IoT та їх підтримки в умовах експлуатації AWS IoT Core підтримує різноманітні протоколи:

– MQTT (черга повідомлень і транспортування телеметрії);

– MQTT через WSS (Websockets Secure);
– HTTPS (протокол передачі гіпертексту – безпечний);
– LoRaWAN (глобальна мережа дальнього дії).

На рисунку 2.3 представлена схема роботи мікроконтролера Arduino у хмарній системі обчислень за допомогою сервісів платформи AWS та стороннього сервісу моніторингу Grafana.

Grafana відіграє ключову роль у візуалізації метрик, які генерує система під час роботи. За допомогою цього сервісу можна зручно та ефективно оцінювати функціонування системи [21]. Його якісна інтеграція з платформою AWS робить використання Grafana ефективним засобом реалізації системи моніторингу.

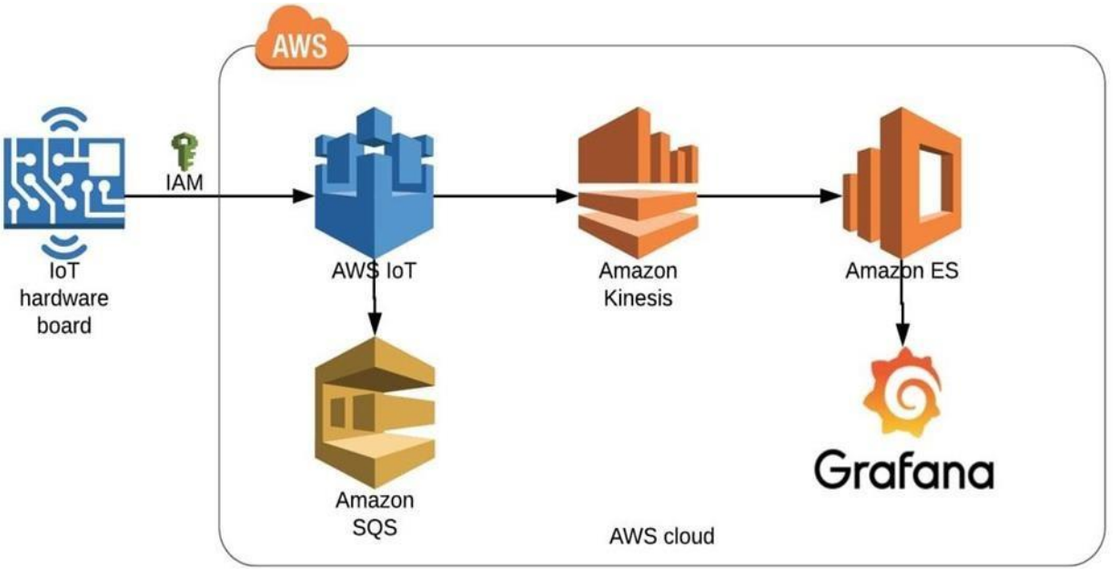

Рисунок 2.3 – Основна структура функціонування автоматизованої системи моніторингу

2.3 Prometheus – Grafana

Prometheus і Grafana – це комбінація інструментів, яка використовується широко для створення систем моніторингу. Завдяки цьому поєднанню можна отримати інформацію, наприклад, про обробку запитів протягом певного часового інтервалу (QPS), середній час відповіді, а також використання ресурсів, таких як процесор, пам'ять і введення/виведення.

Prometheus є системою, яка відслідковує роботу систем та служб, збираючи дані з попередньо визначених цілей за допомогою Pull-моделі. Ці цілі можуть бути знайдені автоматично за допомогою служби Discovery або налаштовані вручну для витягування даних з різних точок системи, таких як API-сервер, балансувальник навантаження та різноманітні SQL і NoSQL бази даних. Схема архітектури Prometheus представлена на рисунку 2.4.

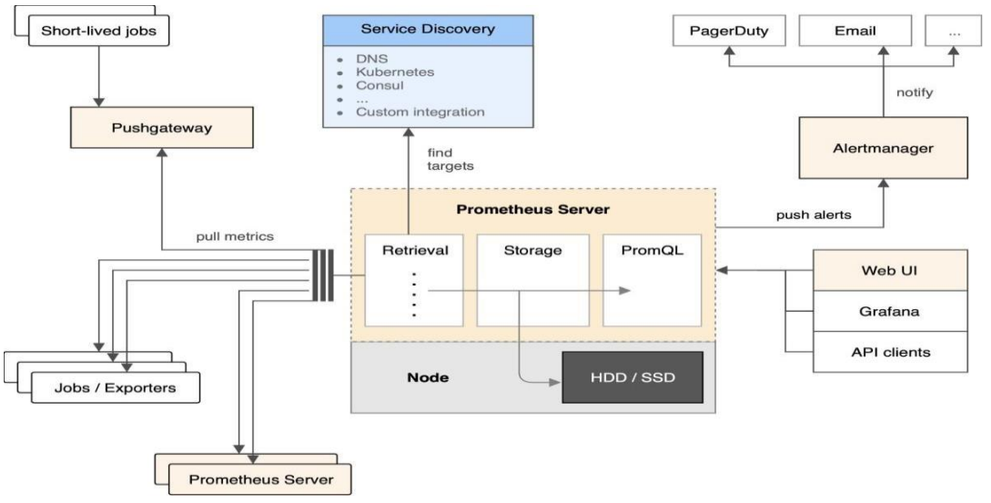

Рисунок 2.4 – Огляд архітектури Prometheus

Grafana має підтримку безлічі джерел даних, включно з CloudWatch, Stackdriver, Elasticsearch, InfluxDB і Prometheus. Підключення Grafana до цих джерел даних дає змогу легко створювати інформаційні панелі вручну або імпортувати готові інформаційні панелі з офіційного веб-сайту.

Для створення системи моніторингу з використанням Prometheus і Grafana потрібно три компоненти:

– експортер метрик: зазвичай це виконуваний файл, який збирає метрики на локальному рівні та робить їх доступними для завантаження, періодично оновлюючи їх;

– сервер Prometheus: періодично збирає показники від експортерів/робочих вузлів;

– grafana: запитує дані у сервера Prometheus для створення візуальних інформаційних панелей.

На рисунку 2.5 наведено приклад інформаційної панелі Grafana.

Рисунок 2.5 – Панель відображення візуалізованих даних в Grafana

2.4 Застосування Prometheus для виявлення аномалій

Зі збільшенням обсягу метрик, які обробляються за допомогою Prometheus,

виникає складність у визначенні сигналів серед інформаційного шуму. Стан системи відображається у вигляді графіків на інформаційних панелях, а також генеруються сповіщення про досягнення порогових значень, які задають оператори системи. Проте використання підходу, що ґрунтується на штучному інтелекті, відкриває можливість навчити модель машинного навчання прогнозувати часові ряди на основі історичних метричних даних. Реальні значення метрик можуть бути порівняні з прогнозами моделі, і якщо спостерігається значна розбіжність між прогнозом та фактичним значенням, це може бути розцінене як аномалія. Основні вимоги до системи виявлення аномалій включають:

– Prometheus – включають важливі метрики, які потрібно контролювати;

– І інструмент візуалізації Grafana, який дозволяє створювати графіки для відображення даних часових рядів з Prometheus.

На рисунку 2.6 показано приклад поєднання цих двох інструментів в одну систему.

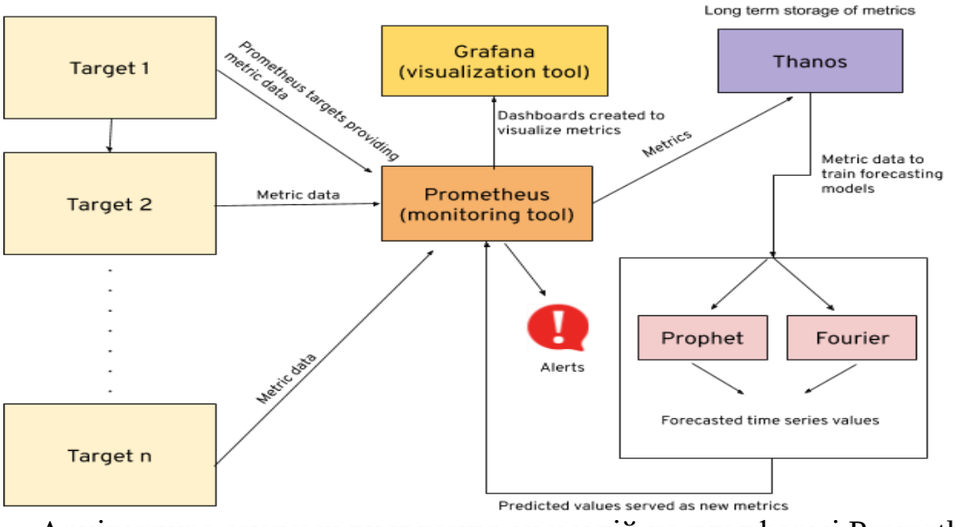

Рисунок 2.6 – Архітектура системи виявлення аномалій на платформі Prometheus – Grafana

Сповіщення: виявлені аномалії надсилаються як сповіщення за допомогою Prometheus AlertManager. Сповіщення можуть бути налаштовані на надсилання автоматичних повідомлень через чати Google та електронну пошту, або ж на будь-яке API повідомляючи про це відповідні команди. Для заданого часового проміжку метрики детектор аномалії Prometheus можна також запустити в "тестовому режимі", щоб перевірити, чи повідомили моделі машинного навчання про ці аномалії. Точність та продуктивність моделей потім можуть реєструватися як показники для MLFlow для порівняння результатів.

MLflow - це платформа з відкритим кодом для управління життєвим циклом ML, включаючи експерименти, відтворюваність. та розгортання. Наразі він пропонує три компоненти:

– відстеження Mlflow;
– проекти Mlflow;
– моделі Mlflow.

Тестовий режим корисний для відстеження модельних експериментів на локальній робочій станції, впорядкування коду в проектах для подальшого повторного використання та виведення найкращої моделі, яка буде розгорнута для виробництва.

2.5 Візуалізація інформації та спостережень за допомогою Grafana

Система виявлення аномалій може опрацьовувати дані в режимі реального часу, наприклад, передбачаючи можливі невдачі у процесі читання-запису бази даних. Це виявлення аномалій є корисним, оскільки кожен раз, коли прогнозується аномалія, система сповіщає, що база даних дійсно не працює належним чином.

Забезпечення системи виявлення аномалій може бути додатково підтверджено за допомогою налаштування системи сповіщень.

Приклад виявлення аномалії в Grafana зображено на рисунку 2.7.

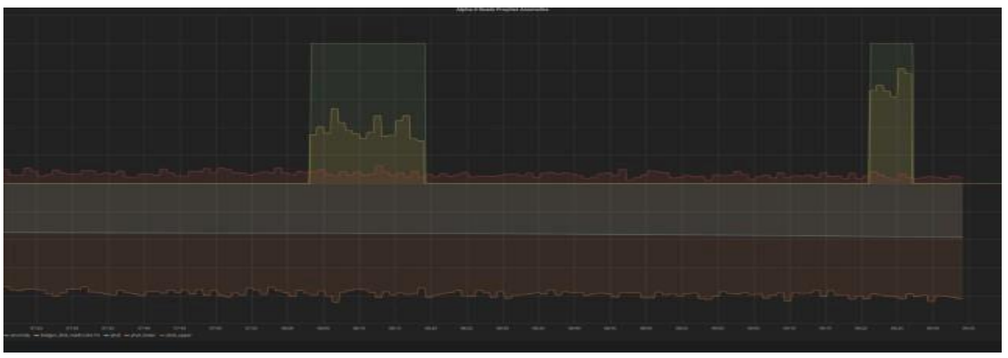

Рисунок 2.7 – Інформаційна панель Grafana: виявлення аномалії підчас обслуговування кластера PSI

2.6 Компоненти автоматизованого модуля моніторингу

На першому етапі потрібно визначитися, що потребує постійного контролю та що саме потребує негайного контролю. Одними з таких показників є параметри температурного режиму, вологості, тиску в системах, рівень рідини та інше. Щоб отримати ці дані, використовуються різноманітні датчики, які зчитують і передають інформацію до моніторингової системи через безпровідний зв'язок або проводове підключення.

Збирання і обробка даних: після реєстрації даних датчиками вони потрапляють до системи моніторингу, де збираються і обробляються. Цей процес може включати перетворення одиниць вимірювання, фільтрацію шуму, прибирання вібрації, усереднення значень для злагодження даних з різних джерел, а також можливий збір даних з кількох датчиків.

Виявлення аномалій: після обробки даних система моніторингу використовує алгоритми аналізу даних для виявлення аномальних змін або незвичайних паттернів в параметрах об'єктів. Це досягається шляхом порівняння значень даних з нормальними діапазонами, використанням статистичних методів і машинного навчання для виявлення відхилень. Якщо відхилення істотно перевищують задані межі, система сповіщає операторів або виконує запрограмовані автоматичні дії.

Візуалізація даних: результати аналізу даних можуть бути візуалізованими у вигляді графіків, діаграм, теплових карт або інших візуальних представлень. Це дозволяє операторам швидко наочно оцінити стан об'єктів і виявити зміни та аномалії.

Сповіщення та управління: у разі виявлення аномалій або надмірних відхилень система моніторингу сповіщає операторів через SMS, електронну пошту або спеціальні програми сповіщень. Оператори повинні прийняти рішення щодо подальших дій та вжити необхідні заходи для розв’язання проблеми, усунення неполадок, для цього можуть здійснювати підключення резервних систем, виклик технічного персоналу чи активування аварійних процедур.

Збереження даних: система може зберігати дані про параметри об'єктів протягом певного періоду часу та використовуватися для аналізу, відновлення подій, етапів роботи і формування звітів. Загалом це забезпечує здійснення статистичного аналізу й аналізу трендів та динамічний моніторинг короткочасних і тривалих змін параметрів об'єктів критичної інфраструктури.

2.7 Переваги автоматизованих модулів моніторингу

Покращена надійність: системи моніторингу дозволяють виявити можливі відхилення та аномалії в роботі об'єктів критичної інфраструктури. Це дозволяє операторам вживати вчасних заходів для запобігання відмовам або аваріям.

Ефективне управління ресурсами: моніторинг параметрів дозволяє ефективно використовувати розподілені ресурси, такі як електроенергія, вода або повітря. Оператори можуть отримувати реальний часовий огляд використання ресурсів та приймати рішення щодо їх оптимального розподілу.

Мінімізація витрат: раннє виявлення проблем, таких як витоки або несправність обладнання, допомагає запобігти потенційним аварійам, що може знизити витрати на ремонт та відновлення об'єктів критичної інфраструктури.

Збільшення безпеки: системи моніторингу гарантують операторам надійну інформацію щодо стану об'єктів критичної інфраструктури, допомагаючи уникнути потенційно небезпечних ситуацій та забезпечити безпеку персоналу та населення.

2.8 Висновок до розділу 2

На сьогоднішній день моніторинг є одним із найважливіших і необхідних складових функціонування всіх критичних інфраструктур. Зазвичай створюють окремий департамент, який займається суто задачами моніторингу, такими як: вибір оптимального рішення, імплементацією, налаштуванням, підтримкою та реагуванням на збої в роботі критичної інфраструктури. Адже збої в системах можуть призвести до зупинки потужних виробництв, припинення життєво-забезпечення цілого міста, а також значних фінансових втрат.

Одним з головних завдань з обслуговування критичної інфраструктури є моніторинг параметрів цих об'єктів. Під час моніторингу необхідно періодично контролювати такі характеристики, як рівень споживання електроенергії, напругу в мережі, температуру, тиск, інші параметри повітря та оточуючого середовища, відстань кількість перевезених пасажирів та багато інших параметрів.

Моніторинг критичної інфраструктури – це на підставі потужної вбудованої бази знань і даних система автоматичної діагностики проблем у роботі всіх компонентів інфраструктури. Повний стек моніторингу критичної інфраструктури включає:

- моніторинг обладнання – фізичний стан системи;
- моніторинг ОС – працездатність та використання ресурсів;
- моніторинг мережі – споживання пропускної здатності та помилки;
- моніторинг додатків – продуктивність та доступність.

Оскільки критична інфраструктура часто складається з декількох локацій розгортання компонентів (приватні, громадські та гібридні хмарні сховища) перед моніторингом стоїть завдання, якнайшвидче визначити і співвіднести проблеми, перш ніж вони вплинуть на кінцевих споживачів і в кінцевому підсумку на продуктивність організації.

В даному розділі були розглянуті основні принципи вибору систем моніторингу, опис популярних рішень, компонентів та переваг відповідно, а також приведений приклад використання Prometheus та Grafana.

3 РОЗРОБКА СЦЕНАРІЮ АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ СИСТЕМИ МОНІТОРИНГУ

У даному розділі буде розглянуто процес автоматизованого налаштування моніторингової системи на базі Prometheus та Grafana за допомогою експертних систем, з використанням інструменту Ansible. Основною вимогою до середовища розгортання є наявність серверів з операційною системою Linux. Крім того, буде розглянуто процес виявлення відхилень за допомогою запитів Prometheus, зокрема, аномалій.

Головна ідея полягає в тому, щоб використовувати безкоштовні рішення для автоматизації встановлення та створення системи моніторингу.

Інструмент Ansible не потребує додаткових витрат і є повністю безкоштовним рішенням, тому його було обрано для автоматичного встановлення моніторингової системи.

Поєднання Prometheus та Grafana відкриває безліч можливостей і не вимагає фінансових витрат.

3.1 Архітектура і конфігурація системи моніторингу

Експертна система має складатись з наступних компонентів:

– база даних (не обов’язково);
– база знань;
– інтерпретатор;
– інтерфейс користувача.

Натомість, побудована нами система моніторингу включає в себе такі компоненти, як:

– Prometheus exporter – база даних. Роль експортера доволі проста, його мета – зібрати дані у вигляді метрик на цільовому вузлі і, підготувавши їх для Prometheus, очікувати запиту;

– Prometheus – база знань та інтерпретатор. Основним компонентом нашої моніторингової системи є TSDB Prometheus. Нагадаємо, що людина-експерт має підготувати спеціальний файл, що містить перелік усіх цільових експортерів, вказавши IP-адресу вузла і порт, який прослуховується відповідним експортером. Своєю чергою Prometheus із зазначеною періодичністю відсилає http(s) запит усім цільовим експортерам

на зібрані метрики (дані), які підготували експортери на цільовому вузлі. Отримавши відповідь, записує отримані дані в базу даних. Особливістю є те, що використовуючи мову запитів Prometheus, людина-експерт має змогу обробляти та маніпулювати даними. Наприклад, вказати поріг сповіщення про навантаження на процесор або заповнення простору на диску. Подібні правила записуються в спеціальні файли, місце розташування яких необхідно вказати в головному конфігураційному файлі;

– Grafana – це інтерфейс для корисиувача. Підключившись до потрібного джерела даних (у нашому випадку це наш TSDB Prometheus), Grafana має доступ до всіх даних, що зберігаються там. Експерт може імпортувати готові або створювати власні інформаційні панелі, які слугуватимуть призначеним для користувача інтерфейсом і візуалізуватимуть стан компонентів, що перебувають під моніторингом. Grafana також має можливість повідомляти користувача про настання певних подій, які були попередньо вказані експертом. Наприклад, відсоток HTTP-відповідей з кодом 4xx або 5xx перевищує встановлену норму, або відсоток завантаження процесора на веб-сервері занадто високий і так далі;

– Prometheus AlertManager – це вирішувач. Основна роль цього компонента – повідомляти про події. Однак AlertManager здатний не тільки показувати повідомлення про події, а й надсилати відповідні запити до зазначених API-серверів, що дає змогу встановити й автоматизувати гнучкі рамки реагування на виявлені події. Наприклад, якщо один із веб-серверів не відповідає, система автоматично ініціалізує ще один і додає його в балансувальник навантаження. Подібна схема широко використовується в AWS EC2 Autoscale Group.

На рисунку 3.1 зображено схему взаємодії компонентів побудованої нами системи моніторингу.

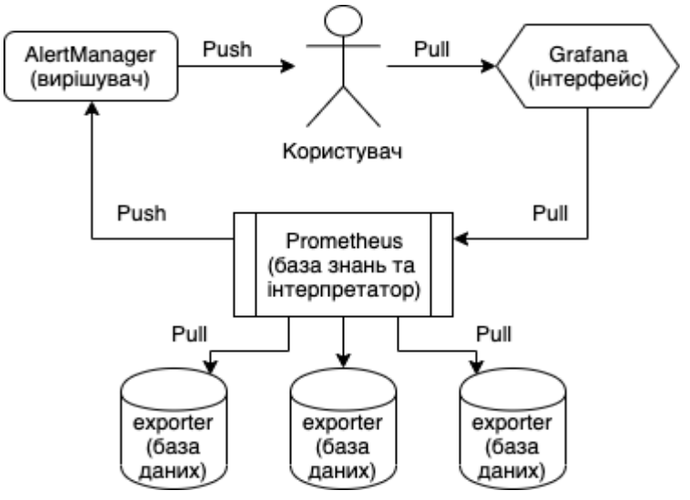

Рисунок 3.1 – Схема взаємодії компонентів побудованої системи моніторингу

Налаштування експортера Prometheus виявляється ключовим етапом, і його значення важко переоцінити, оскільки від цього залежить, які конкретно дані будуть передаватися до бази знань Prometheus. Цей етап, хоча й не вимагає значних зусиль, є вкрай важливим для забезпечення оптимального функціонування системи.

Зазвичай експортер втілюється у вигляді бінарного файлу, написаного на мові програмування Go. Його основні вимоги полягають в тому, щоб він міг працювати у фоновому режимі. У деяких випадках, для коректної роботи, він може потребувати певного набору вхідних параметрів. Крім того, експортер може функціонувати всередині Docker-контейнера в разі вимог середовища розробки.

Для збору інформації про використання ресурсів хоста, таких як ЦПУ, пам'ять, фізичний диск, і для отримання даних про його стан і доступність, ми використовували офіційний експортер Prometheus, відомий як "Node exporter". Деплоймент цього експортера виконувався за допомогою "systemd", де він запускався як фоновий сервіс. Параметри цього сервісу докладено в додатку А.

Конфігурація Promeheus дещо складніша, але так само не потребує значних зусиль. Після розгортання потрібних програмних компонентів основна конфігурація зберігається в таких файлах:

– prometheus.yml містить головні параметри конфігурації, такі як “scrape_interval” (інтервал зчитування метрик з експортерів) , “rule_files” (розташування правил для AlertManager), “ targets” (перелік розташування експортерів у форматі ip:port);

– alertmanager.yml містить параметри конфігурації AlertManager, наприклад параметри підключення до поштового серверу або інших засобів сповіщення, а також параметри надсилання сповіщень;

– rules містить перелік правил, по яким відбувається сповіщення у разі виявлення події.

Конфігурація Grafana має свої особливості, які відрізняються від конфігурації інших компонентів системи моніторингу. Це обумовлено тим, що для серверної частини необхідно встановити пакет, а всі інші налаштування доступу та інформаційних панелей виконуються через веб-інтерфейс.

На рисунках 3.2, 3.3, 3.4, 3.5 та 3.6 ілюстровано поетапну конфігурацію Grafana, включаючи підключення до Prometheus та налаштування інформаційної панелі щодо навантаження сервера.

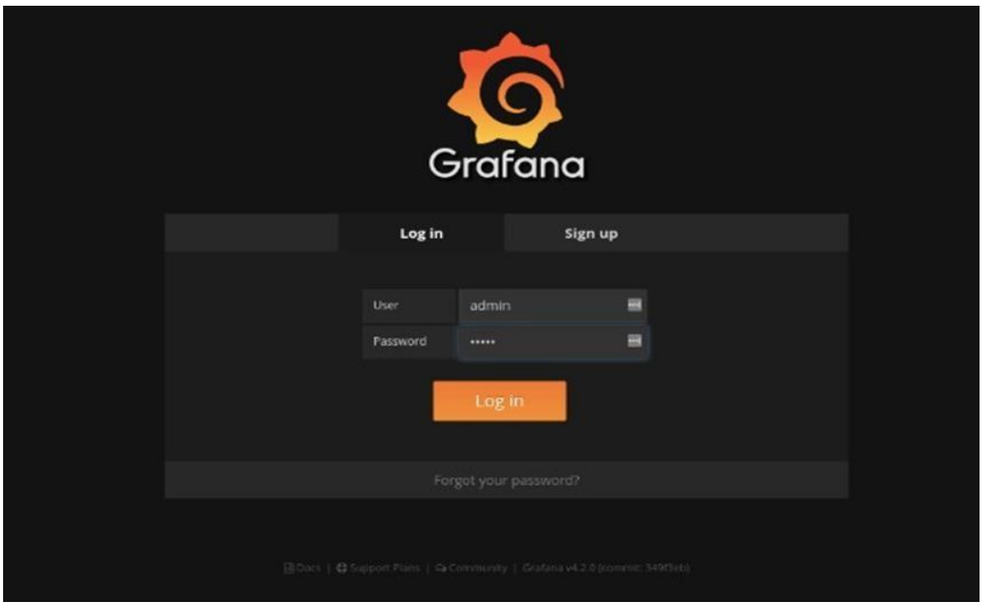

Рисунок 3.2 – Сторінка авторизації до веб-інтерфейсу

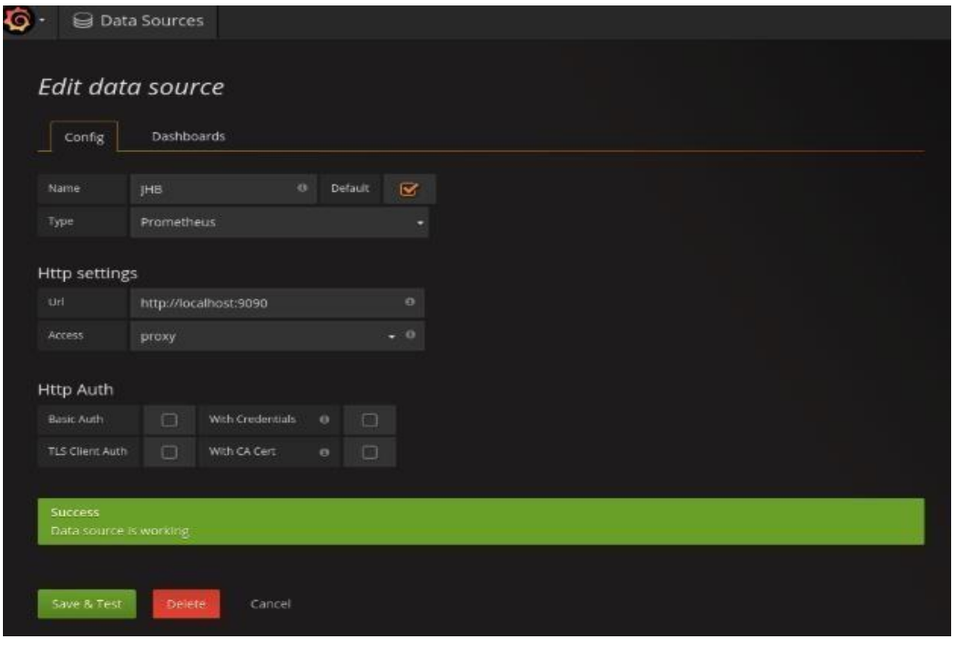

Рисунок 3.3 – Сторінка редагування джерела метрик

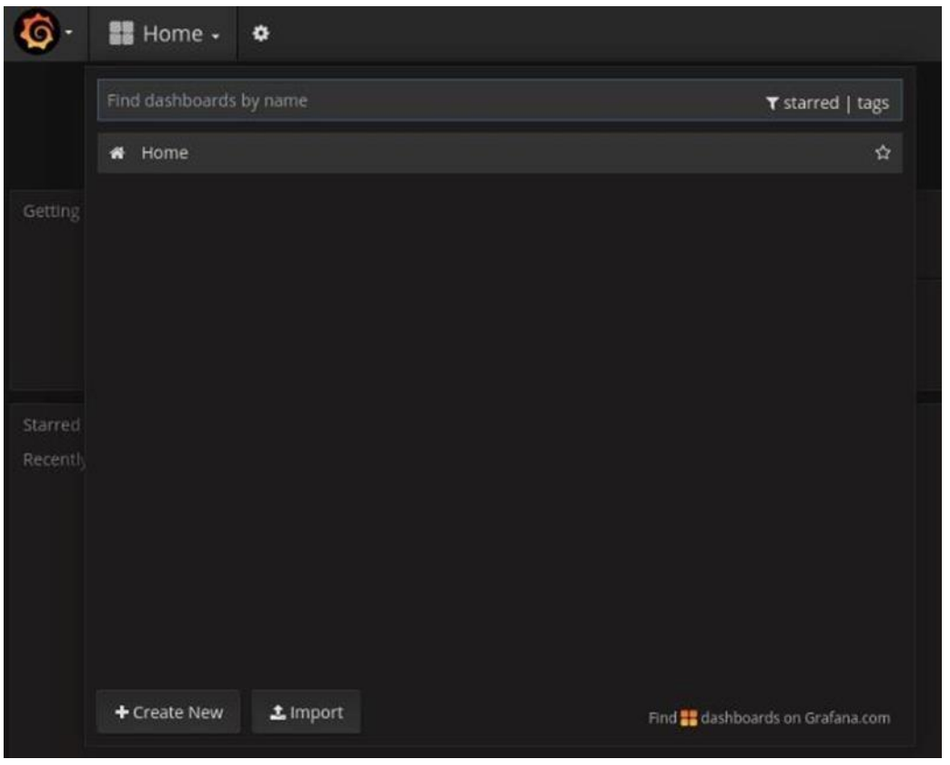

Рисунок 3.4 – Сторінка пошуку необхідних інформаційних паналей

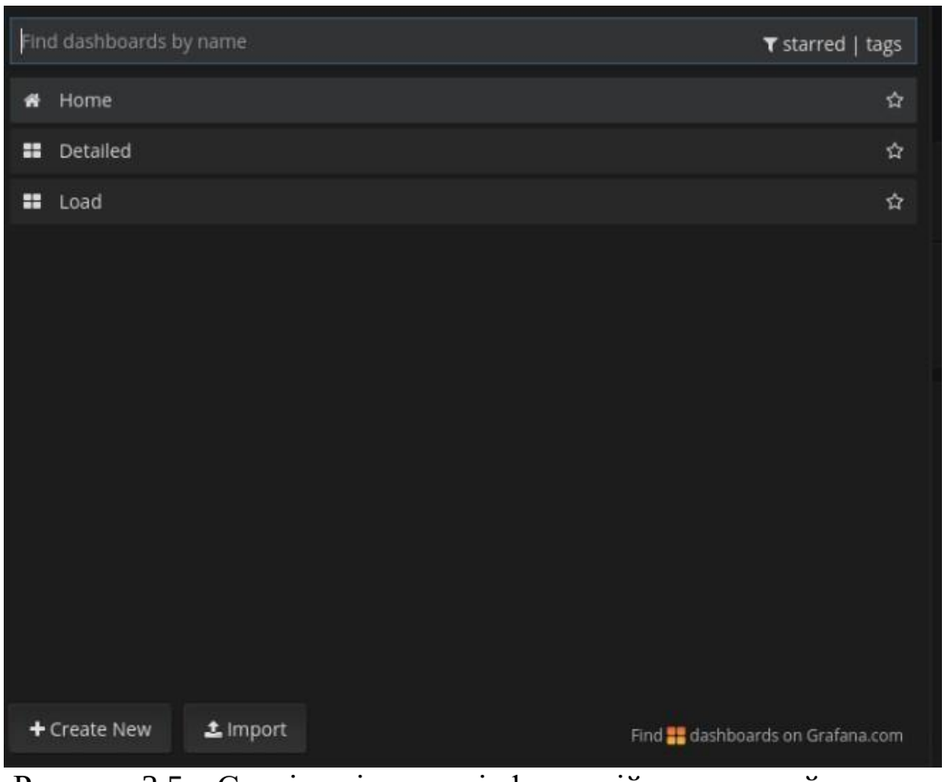

Рисунок 3.5 – Сторінка імпорту інформаційних панелей

Рисунок 3.6 – Вигляд завантаженої інформаційно панелі навантаження на ЦПУ сервера

3.2 Anomally detection як одна з можливостей побудованої системи моніторингу

Однією з ключових характеристик запитів у Prometheus є можливість агрегування даних та їх подальша обробка у режимі реального часу. Ці можливості відкривають можливість ефективного використання системи моніторингу для виявлення аномалій.

Існує чотири ключові причини, чому важливо виявлятиити аномалії:

– діагностування інцидентів;

– виявлення регресій продуктивності програми;

– визначення та вирішення зловживання;

– безпека.

По-перше, дані часових рядів повинні бути агреговані правильно. Використаємо стандартний лічильник http_requests_total, що вказаний на рисунку 3.7, як джерело даних, хоча багато інших показників можна застосувати за допомогою тих же методів.

```
http_requests_total{
 job="apiserver",
 method="GET",
 controller="ProjectsController",
 status_code="200",
 environment="prod"
}
```

Рисунок 3.7 – Функція агрегації даних

Як видно на рисунку 3.7, у нас є додаткові параметри: "method", "controller", "status_code", "environments", а також параметри, які додає Prometheus, наприклад, "instance" та "job".

Далі необхідно вибрати правильний рівень агрегації для використовуваних даних.

Це відомо як проблема Goldilocks - "занадто багато", "занадто мало" або "в самий раз", що є ключовим аспектом у виявленні аномалій. Агрегуючи дані із занадто великими проміжками часу, ми можемо зменшити їх до надто малих розмірів, що створює дві потенційні проблеми:

– ми можемо пропустити справжні аномалії, оскільки агрегація приховує проблеми, які виникають у підмножинах наших даних;

– якщо ми виявимо аномалію, важко віднести її до певної частини нашої системи без додаткового дослідження аномалії.

Але якщо агрегувати дані за дуже короткий проміжок часу, може виникнути серія даних із надто малими розмірами вибірки, що може призвести до невірних результатів та помилкового визначення підозрілих даних як правильних.

Давайте проведемо агрегацію всіх HTTP-запитів до серверів продуктового середовища за часовим проміжком у п'ять хвилин. Результат буде записаний із виразом, конфігурація якого наведена на рисунку 3.8.

```
- record: job:http_requests:rate5m
expr: sum without(instance, method, controller, status_code)
(rate(http_requests_total[5m]))
# --> job:http_requests:rate5m{job="apiserver", environment="prod"}  21321
# --> job:http_requests:rate5m{job="gitserver", environment="prod"}  2212
# --> job:http_requests:rate5m{job="webserver", environment="prod"}  53091
```

Рисунок 3.8 – Конфігурація агрегації данних з п’ятихвилинним вікном

Деякі основні принципи статистики можуть бути використані для виявлення аномалій у Prometheus.

Якщо ми маємо інформацію про середнє значення та стандартне відхилення (σ) величини в серії даних, можемо розраховувати z-score за допомогою будь-якої вибірки з цієї серії. Z-score вимірюється в кількості стандартних відхилень від середнього значення. Таким чином, z-score 0 вказує на ідентичність з середнім у наборі даних з нормальним розподілом, тоді як z-score 1 дорівнює 1.0 σ від середнього. Якщо припустити, що базові дані мають нормальний розподіл, 99.7% зразків повинні мати z-score від 0 до 3. Чим менше значення z-score, тим менше ймовірність його наявності. Ми використовуємо цю властивість для виявлення аномалій у серії даних Prometheus.

Для обчислення середнього та стандартного відхилення використовуємо дані з великою кількістю вибірок, зібраних протягом одного тижня. На рисунку 3.9 ми використовуємо дані, зібрані протягом цього тижня, при зборі інформації кожну хвилину, що складає трошки більше 10 000 зразків.

```
# Long-term average value for the series
- record: job:http_requests:rate5m:avg_over_time_1w
expr: avg_over_time(job:http_requests:rate5m[1w])

# Long-term standard deviation for the series
- record: job:http_requests:rate5m:stddev_over_time_1w
expr: stddev_over_time(job:http_requests:rate5m[1w])
```

Рисунок 3.9 – Збирання даних раз на 5 хвилин протягом тижня

Ми можемо обчислити z-score для запиту Prometheus, зображеного на рисунку 3.10, як тільки будемо мати середнє та стандартне відхилення дляагрегації.

```
# Z-Score for aggregation
(
job:http_requests:rate5m -
job:http_requests:rate5m:avg_over_time_1w
) /  job:http_requests:rate5m:stddev_over_time_1w
```

Рисунок 3.10 – Розрахунок z-score для агрегаціїї

Виходячи зі статистичних принципів нормальних розподілів, можна припустити, що будь-яке значення, яке виходить за межі діапазону приблизно від 3 до -3, є аномалією.Приклад виявлення таких аномалій зображено на рисунку 3.11.

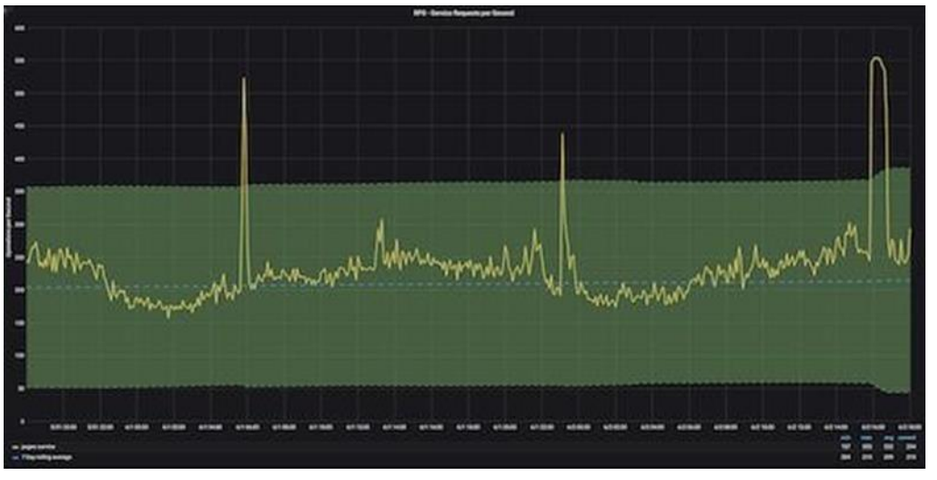

Рисунок 3.11 – Виявлення аномалій поза межами інтервалу від 3 до -3

Z-score трохи незручно інтерпретувати на графіку, оскільки вони не мають одиниці вимірювання. Але аномалії на цій діаграмі легко виявити. Все, що з’являється за межами зеленої зони (що позначає z-score, які потрапляють в інтервал від +3 до -3),є аномалією.

Ми припускали, що наша основна агрегація має нормальний розподіл. Якщо ми обчислимо z-score за допомогою даних, які зазвичай не

розподіляються, наші результати будуть неправильними.

Існує чимало статистичних методів тестування даних для нормального розподілу, але найкращим варіантом є перевірка того, що базові дані мають z-score приблизно від 4 до -4, що зображено на рисунку 3.12.

```
(
 max_over_time(job:http_requests:rate5m[1w]) - avg_over_time(job:http_requests:rate5m[1w])
) / stddev_over_time(job:http_requests:rate5m[1w])
# --> {job="apiserver", environment="prod"}  4.01
# --> {job="gitserver", environment="prod"}  3.96
# --> {job="webserver", environment="prod"}  2.96

(
 min_over_time(job:http_requests:rate5m[1w]) - avg_over_time(job:http_requests:rate5m[1w])
) / stddev_over_time(job:http_requests:rate5m[1w])
# --> {job="apiserver", environment="prod"}  -3.8
# --> {job="gitserver", environment="prod"}  -4.1
# --> {job="webserver", environment="prod"}  -3.2
```

Рисунок 3.12 – Перевірка мінімального та максимального z-score

Показники, які ймовірно не мають нормального розподілу, включають частоту помилок, затримки, довжину черги тощо. В той час як обчислення z-score ефективно застосовується до даних з нормальним розподілом у часових рядах, існує інший метод, який може забезпечити ще більш точні результати виявлення аномалій. Сезонність визначає характеристику метрики часового ряду, де метрика демонструє регулярні та передбачувані зміни, що повторюються в кожному циклі. Графік значень запитів в секунду представлено на рисунку 3.13.

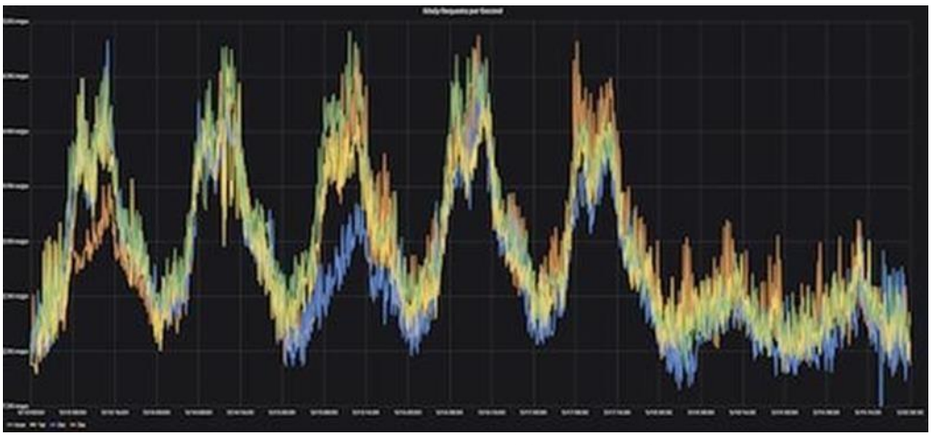

Рисунок 3.13 – Графік RPS діапазоном в місяць

Цей графік відображає значення RPS (запити в секунду) протягом чотирьох послідовних тижнів. Семиденний інтервал називається "компенсацією", яка представляє собою шаблон, що буде вимірюватися.

Кожен тиждень на графіку позначений різним кольором. Сезонність даних вказує на узгодженість тенденцій, відзначених на графіку – щоранку у понеділок ми спостерігаємо однаковий ріст значень RPS, а ввечері у п'ятницю ми спостерігаємо

зниження значень RPS.

Використовуючи сезонність у наших часових рядах, ми можемо розробити більш точні прогнози, що допомагає у більш ефективному виявленні аномалій. Обчислення сезонності за допомогою Prometheus передбачало використання кількох різних статистичних принципів.

У першій ітерації ми обчислюємо, додаючи тенденцію зростання, яку ми спостерігали за тижневий період, до значення попереднього тижня. Обчислимо тенденцію зростання, віднімаючи середнє однотижневе за останній тиждень від поточного середньо-тижневого на даний момент, що зображено на рисунку 3.14.

```
- record: job:http_requests:rate5m_prediction
  expr: >
    job:http_requests:rate5m offset 1w                    # Value from last period
    + job:http_requests:rate5m:avg_over_time_1w           # One-week growth trend
    - job:http_requests:rate5m:avg_over_time_1w offset 1w
```

Рисунок 3.14 – Розрахунок тенденцій

Перша ітерація є дещо обмеженою; ми використовуємо п'ятихвилинне вікно за поточний тиждень та попередній тиждень для отримання прогнозів.

У другій ітерації ми розширюємо область застосування, узявши в середньому чотиригодинний період з попереднього тижня і порівнюючи його з поточним тижнем.

Таким чином, якщо ми намагаємось передбачити значення показника о 8 годині ранку в понеділок, замість використання того ж п'ятихвилинного вікна за тиждень до цього, ми використовуємо середнє значення показника від 6 ранку до 10 ранку для попереднього дня. Схема такого розрахунку подана на рисунку 3.15.

```
- record: job:http_requests:rate5m_prediction
  expr: >
    avg_over_time(job:http_requests:rate5m[4h] offset 166h) # Rounded value from last period
    + job:http_requests:rate5m:avg_over_time_1w             # Add 1w growth trend
    - job:http_requests:rate5m:avg_over_time_1w offset 1w
```

Рисунок 3.15 – Розрахунок тенденцій

Ми використовуємо 166 годин у запиті замість одного тижня, тому що ми хочемо використовувати чотиригодинний період, виходячи з поточного часу доби, тому нам потрібно, щоб компенсація не містила дві години в тиждень.

На рисунку 3.16 зображено два графіки, реального та прогнозованого значення запитив за секунду інтервалом в два тижні:

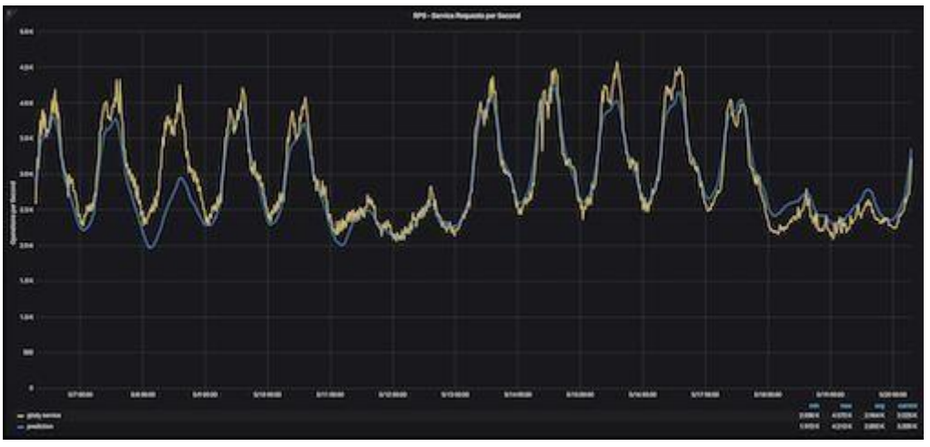

Рисунок 3.16 – Реальне значення RPS (жовтий) та прогнозоване (синій), протягом двох тижнів

Однією з проблем цього підходу є те, що ми намагаємось агрегувати три ряди, які фактично представляють собою одні й ті самі дані протягом трьох тижнів. Іншими словами, всі три ряди мають однакові мітки, що ускладнює їх об'єднання. Щоб уникнути непорозумінь, ми вводимо нову мітку під назвою "зміщення" і використовуємо функцію заміни міток для додавання зміщення до кожного з трьох тижнів. Під час квантильної агрегації ми беремо це до уваги, обчислюючи середнє значення з трьох агрегованих рядів. Цей процес зображено на рисунку 3.17.

```
- record: job:http_requests:rate5m_prediction
  expr: >
   quantile(0.5,
     label_replace(
       avg_over_time(job:http_requests:rate5m[4h] offset 166h)
       + job:http_requests:rate5m:avg_over_time_1w - job:http_requests:rate5m:avg_over_time_1w offset 1
w
       , "offset", "1w", "", "")
     or
     label_replace(
       avg_over_time(job:http_requests:rate5m[4h] offset 334h)
       + job:http_requests:rate5m:avg_over_time_1w - job:http_requests:rate5m:avg_over_time_1w offset 2
w
       , "offset", "2w", "", "")
     or
     label_replace(
       avg_over_time(job:http_requests:rate5m[4h] offset 502h)
       + job:http_requests:rate5m:avg_over_time_1w - job:http_requests:rate5m:avg_over_time_1w offset 3
w
       , "offset", "3w", "", "")
   )
   without (offset)
```

Рисунок 3.17 – Розмічене середнє значення з трьох серій

Тепер наше прогнозування, яке зображено на рисунку 3.18, що виводить середнєзначення з серії трьох агрегацій, набагато точніше.

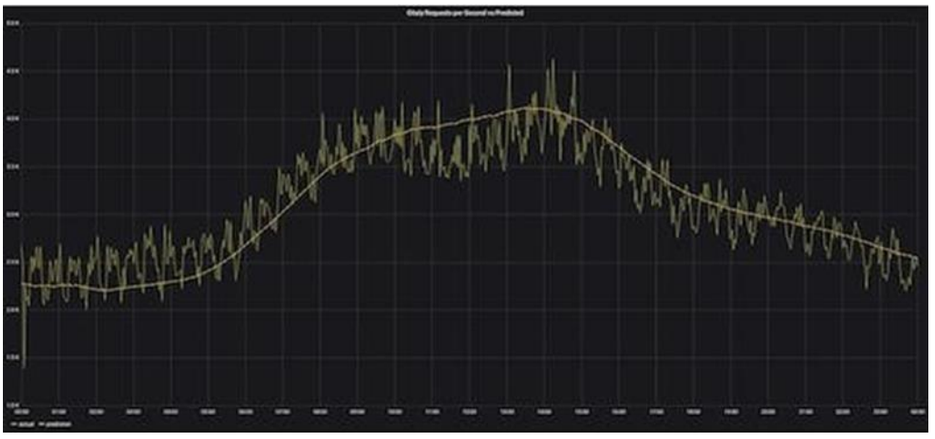

Рисунок 3.18 – Графік агрегації з трьох серій

Для перевірки точності нашого прогнозування ми можемо використовувати z-score. Він дозволяє виміряти відстань вибірки від прогнозування у стандартних відхиленнях, як показано на діаграмі 3.19. Чим більше стандартних відхилень від нашого прогнозу, тим вища ймовірність того, що певне значення є відхиленням.

Рисунок 3.19 – Використання z-score до агрегованого значення

Ми можемо оновити наш графік, переходячи до сезонного прогнозування замість середнього значення за тиждень. Діапазон нормальності для певного часу доби буде позначений зеленим кольором. Все, що виходить за межі цієї зеленої зони, розглядається як аномалія.

У цьому випадку аномалія була виявлена у відділенні в неділю вдень. Використання меж ± 2σ з обох боків нашого прогнозу є ефективним критерієм для визначення відхилень у сезонних прогнозах.

Ми можемо застосувати досить просте правило для AlertManager, яке перевіряє, чи є z-score метрики в діапазоні стандартного відхилення +2 або -2. Параметри сповіщення зображені на рисунку 3.20.

```
- alert: RequestRateOutsideNormalRange
  expr: >
   abs(
     (
       job:http_requests:rate5m - job:http_requests:rate5m_prediction
     ) / job:http_requests:rate5m:stddev_over_time_1w
   ) > 2
  for: 10m
  labels:
    severity: warning
  annotations:
    summary: Requests for job {{ $labels.job }} are outside of expected operating parameters
```

Рисунок 3.20 – Налаштування сповіщення в разі виявлення аномалій

Ми використовуємо правило маршрутизації, яке надсилає сповіщення в Slack при виявленні будь-яких аномалій, що зображено на рисунку 3.21.

Рисунок 3.21 – Приклад сповіщення в Slack

3.3 Висновки до розділу 3

У даному розділі наводиться конфігурація розробленої системи моніторингу, що ґрунтується на принципах експертних систем, а також подається детальний опис основних аспектів її налаштування. Це включає в себе розкриття параметрів сценарію Ansible, процедури встановлення та конфігурування Prometheus і AlertManager, а також тонкощі налаштування інструменту візуалізації Grafana.

З огляду на концепцію експертних систем у побудованій системі моніторингу, експортер Prometheus використовується як база даних, а сам Prometheus виступає як база знань та інтерпретатор. Додатково, для вирішення завдань і керування алертами використовується Prometheus AlertManager.

Для виявлення аномалій використовується агрегація даних за різними проміжками часу, а також встановлення "безпечного діапазону" за допомогою z-score. Розроблена система моніторингу виявляє зміни в зазначених параметрах і може самостійно

адаптуватися до зростання або зниження користувачів, постійно аналізуючи свіжі дані. Важливо відзначити, що система також налаштована на надсилання сповіщень через Slack у випадку виявлення аномалій, щоб користувачі могли оперативно реагувати на потенційні проблеми.

4 ОХОРОНА ПРАЦІ

4.1 Нормативно-правові положення з охорони праці та безпеки в надзвичайних ситуаціях автоматизованого комплексу життєзабезпечення житлового приміщення

Україна має кілька правових актів, які регулюють питання забезпечення безпеки праці в автоматизованому комплексі, що забезпечує життєві потреби в житловому приміщенні. Основними нормативними документами є:

– закон України "Про охорону праці" від 14 жовтня 1992 року № 2694-XII: Цей закон встановлює загальні принципи та норми охорони праці в Україні, включаючи вимоги до безпеки праці та обладнання. Він охоплює всі галузі економіки, включаючи житлові приміщення;

– наказ Міністерства соціальної політики України "Про затвердження Правил охорони праці під час експлуатації електроустановок" від 25 червня 2013 року № 326: Цей наказ встановлює вимоги щодо безпеки праці під час використання електричних систем, які можуть бути частиною автоматизованого комплексу, що забезпечує життєві потреби в житлових приміщеннях;

– наказ Державного комітету України з питань промислової безпеки, охорони праці тагірничого нагляду "Про затвердження Правил охорони праці під час експлуатації ліфтів" від 29 грудня 2010 року № 512: Цей наказ містить вимоги до безпеки праці під час експлуатації ліфтів, які також можуть використовуватись в автоматизованих комплексах життєзабезпечення;

– нормативні документи з пожежної безпеки: Україна також має нормативні документи, які встановлюють вимоги до пожежної безпеки, такі як "Правила пожежної безпеки в Україні" та "Правила пожежної безпеки під час експлуатації будівель та споруд".

Ці документи містять загальні вимоги щодо безпеки та охорони праці в житлових приміщеннях, включаючи автоматизовані комплекси. Повний перелік нормативних актів можна знайти на офіційних веб-сайтах відповідних державних органів, таких як Державна інспекція з охорони праці, Міністерство соціальної політики України та Державний комітет України з питань промислової безпеки, охорони праці та гірничого нагляду. Нормативні вимоги щодо охорони праці в автоматизованому комплексі житлового приміщення можуть варіюватися в залежності від його складу та особливостей, але існують загальні принципи та рекомендації, які часто використовуються для забезпечення безпеки праці в таких комплексах. Дотримання цих

правил та норм є важливим для забезпечення безпеки працівників. Крім того, слід користуватися стандартами безпеки, що встановлюються органами з охорони праці. Ці стандарти можуть включати вимоги щодо розробки, встановлення, експлуатації та обслуговування автоматизованих систем. Дотримання цих стандартів сприятиме забезпеченню безпеки працівників і уникненню можливих ризиків. Важливим етапом є оцінка ризиків, пов'язаних з автоматизованим комплексом, для визначення потенційних небезпек та прийняття відповідних заходів для їх уникнення. Слід розглядати можливі небезпечні ситуації, пов'язані з електробезпекою, пожежною безпекою та впливом на здоров'я.

Надання належного навчання та інструктажу працівникам стосовно безпеки при роботі з автоматизованим комплексом є також критичним. Працівники повинні бути ознайомлені з правилами та процедурами безпеки, вміти використовувати систему безпечно та уникають можливих ризиків.

Регулярні перевірки та обстеження автоматизованого комплексу дозволяють виявити проблеми та несправності, які можуть виникнути, і вживати відповідних заходів для їх усунення. Попередження аварійних ситуацій включає заходи безпеки, такі як відключення електроенергії, захист від пожежі та затоплення, з використанням систем попередження, аварійних вимикачів та інших захисних засобів.

Медичний контроль та надання необхідної медичної допомоги працівникам є ще однією важливою складовою безпеки. Важливо враховувати національне законодавство та рекомендації з охорони праці для автоматизованих систем, що забезпечують життєво важливі функції в житлових приміщеннях. Перед впровадженням таких систем рекомендується звертатися за консультацією до фахівців з охорони праці або відповідних регулюючих органів та профспілок України.

4.2 Покращання безпеки та охорони праці в екстремальних ситуаціях автоматизованого комплексу, що забезпечує життєві потреби в житловому приміщенні

Мета забезпечення безпеки мешканців та запобігання негативним наслідкам надзвичайних ситуацій в розумному домі вимагає впровадження ефективних заходів з охорони праці та безпеки. Основними заходами, які необхідно вживати, є наступні:

– планування евакуації: Створення плану евакуації у разі виникнення пожежі, природних лих або інших надзвичайних ситуацій. План повинен включати маршрути виходу, місця збору, контактну інформацію та інструкції щодо правильної поведінки в надзвичайних ситуаціях;

– пожежна безпека: Монтаж датчиків диму, вогнегасників та інших пристроїв для захисту від пожежі. Регулярна перевірка та обслуговування систем пожежного захисту. Визначення безпечних місць для зберігання вогнегасників та іншого обладнання, призначеного для боротьби з вогнем;

– безпека електроенергії: Важливо правильно встановлювати і заземлювати електроприлади та системи. Необхідно використовувати захисні пристрої, такі як автоматичні вимикачі, заземлення і розетки з диференціальним захистом від струму. Необхідно уникати перевантажень і користуватися електроприладами з надійними сертифікатами;

– безпека систем автоматизації: Завдяки впровадженню заходів безпеки, можна забезпечити надійний захист систем розумного будинку від несанкціонованого доступу. Важливо також забезпечити конфіденційність та безпеку персональних даних. Це можна зробити шляхом оновлення програмного забезпечення та використання надійних паролів, що дозволить уникнути хакерських атак та вірусів;

– системи безпеки: Монтаж системи відеоспостереження, датчиків руху та сигналізаційної системи. Регулярний технічний огляд та обслуговування системи безпеки. Оповіщення про надзвичайні ситуації через мобільні додатки або спеціальні пультів управління;

– інструктування мешканців: Гарантувати правильне навчання мешканців щодо використання систем розумного будинку та дотримання правил безпеки. Надати інформацію про процедури в надзвичайних ситуаціях і контактні дані екстрених служб. Важливо також враховувати нормативно-правові акти та рекомендації з охорони праці та безпеки, для чого рекомендується звернутися у відповідні державні органи, щоб отримати детальну інформацію та консультації щодо заходів з охорони праці та безпеки в надзвичайних ситуаціях.

ВИСНОВКИ

Надана кваліфікаційна робота розглядає важливість автоматизованого модуля для контролю за параметрами об'єктів критичної інфраструктури. У ній також було розроблено та запропоновано рішення для створення експертної системи на основі інструментів моніторингу Prometheus - Grafana. Однак для налаштування конфігурації було використано рушій арифметичної обробки Ansible's arithmetic processing engine.

Під час виконання поставленого завдання було розроблено модульну систему, яка, крім обчислювальних операцій, може зробити певні висновки, базуючись на своїх знаннях. Окрім того, для виявлення та запобігання збоїв використовується значна кількість даних, а моніторинг на основі Prometheus - Grafana забезпечує сповіщення відповідальної особи про поточний стан критичної інфраструктури або її компонентів.

У наданій роботі запропоновано рішення для автоматизації розгортання експертної системи на основі інструментів моніторингу Prometheus - Grafana за допомогою засобу керування конфігураціями. Застосування саме експертних систем у сучасних системах моніторингу дасть змогу ефективно виявляти не закономірну роботу системи та запобігати збоям, що можуть бути спричинені різними факторами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні вказівки з підготовки та захисту кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 151 Автоматизація та комп'ютерно–інтегровані технології, освітньо–професійних програм:

«Автоматизоване управління технологічними процесами»; «Комп'ютерно–інтегровані технологічні процеси і виробництва»; «Комп'ютеризовані та робототехнічні системи» / Упоряд.: І. Ш. Невлюдов Р. В. Артюх В. В. Безкоровайний Н. П. Демська В. В. Євсєєв О.І. Филипенко О. М. Цимбал. Харків: ХНУРЕ, 2021. 55 с.

2. ДСТУ 3008–15. Документація. Звіти у сфері науки та техніки. структура та правила оформлення. – Введ. 2015–06–22. – К. Держстандарт України, 2017 – 29 с.

3. Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2023) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2023. – Вип. 2. – 408с;

«Розробка автоматизованого модуля моніторингу параметрів об'єктів критичної інфраструктури». / О.О. Рак

4. Офіційний сайт Наукової бібліотеки ХНУРЕ [Електронний ресурс]. – Електрон.текстові дані. – Режим доступу: http://lib.nure.ua/?page=1. – 27.12.2018.

5. Стандарт вищої освіти магістра за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 151 «Автоматизація та приладобудування» затверджено і введено в дію Наказом Міністерства освіти і науки України від 10.08.2020 р. No 1022. Режим доступу: https://mon.gov.ua/storage/app/media/vishchaosvita/zatverdzeni%20standarty/2020/08/10/151-avtomatizatsiya-ta-kit-magistr.pdf

6. Production Monitoring System and Its Benefits [Електронний ресурс] / techna-tool.com. – Режим доступу: www/ URL: https:// www.techna-tool.com/blog/production-monitoring-system-and-its -benefits/

7. Освітньо-професійна програма «Комп'ютеризовані та робототехнічні системи». – Режим доступу: https://nure.ua/wpcontent/uploads/ Education_programs/2021/2021_mag_151_opp_ktrs.pdf.

8. Основы мониторинга и сбора метрик. 8host. URL: https://www.8host.com/blog/osnovy-monitoringa-i-sbora-metrik/

9. Automated Monitoring and Visualization System in Production / Lyashenko V., Abu-Jassar A. T., Yevsieiev V., Maksymova S. // Int. Res. J. Multidiscip. Technovation,

5(6), 09-18.

10. What Is Prometheus? Oreilly.URL: https://www.oreilly.com/library/view/prometheus- up/9781492034131/ch01.html

11. Prometheus Annomally Detection. A RED HAT BLOG. URL: https://next.redhat.com/2019/11/18/prometheus-anomaly-detection/

12. EJ HSU. Build A Monitoring Dashboard by Prometheus + Grafana. DeepQ Research Engineering Blog. URL: https://medium.com/htc-research- engineering-blog/build-a-monitoring-dashboard-by-prometheus-grafana- 741a7d949ec2

13. IT Infrastructure Monitoring Essentials. Heroix. URL: https://go.heroix.com/it-infrastructure-monitoring