НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: «Моніторинг даних кібербезпеки об'єкта критичної інфраструктури індустріального сектору»

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи __ФБ-03_____
(шифр групи)

Жигун Анастасія Володимирівна
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент кафедри ІБ к.т.н. Стьопочкіна І.В.
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий фізичко-технічний інститут
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ Завідувач кафедри

_____ Дмитро ЛАНДЕ (підпис)

«___»_____2023 р.

ЗАВДАННЯ

на дипломну роботу здобувачу вищої освіти

Жигун Анастасія Володимирівна (прізвище, ім’я, по батькові)

1. Тема роботи «Моніторинг даних кібербезпеки об'єкта критичної інфраструктури індустріального сектору», керівник роботи Стьопочкіна Ірина Валеріївна к.т.н., доцент, затверджені наказом по університету від « 31 » травня 2024 р. №2251-с.
2. Термін подання здобувачем вищої освіти роботи « » червня 2024 р.
3. Вихідні дані до роботи: літературні джерела, структура SCADA, система моніторингу SCADA, пристрій Raspberry Pi 5.
4. Зміст роботи: побудова моделі кіберзагроз, опис кібератак, проектування захищеної системи моніторингу об’єкта критичної інфраструктури, налаштування системи моніторингу кібератак на SCADA, аналіз результатів.
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.
6. Дата видачі завдання: 23 вересня 2023 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання та узгодження теми роботи	25.09.2023	Виконано
2	Огляд наукової літератури по темі	26.02.2024 - 15.03.2024	Виконано
3	Дослідження структури SCADA та модифікацій в процесі еволюції	18.03.2024 - 30.03.2024	Виконано
4	Опис моделі загроз та показників превентивного попередження атак	01.04.2024 - 06.04.2024	Виконано
5	Розробка архітектури системи моніторингу	08.04.2024 - 20.04.2024	Виконано
6	Програмна емуляція комунікації низькорівневих пристроїв мережі SCADA	22.04.2024 - 11.05.2024	Виконано
7	Здійснення комп’ютерного моделювання платформи моніторингу	13.05.2024 - 23.05.2024	Виконано
8	Аналіз результатів	24.05.2024 - 31.05.2024	Виконано

Здобувач вищої освіти _____ (підпис) Анастасія ЖИГУН

Керівник роботи _____ (підпис) Ірина СТЬОПОЧКІНА

РЕФЕРАТ

Обсяг дипломної роботи 65 сторінок, 20 ілюстрацій, 11 таблиць, 3 додатків і 10 джерел літератури.

Об’єкт дослідження: Об’єкти критичної інфраструктури індустріального сектору.

Предмет дослідження: Система моніторингу показників SCADA.

Мета дослідження: Розробка архітектури системи моніторингу кібератак об’єктів критичної інфраструктури індустріального сектору з використанням SCADA.

Методи дослідження: аналіз літературних джерел, аналіз та синтез архітектур та механізмів, комп’ютерний експеримент.

Отримані результати: спроектовано архітектуру IT інфраструктури об’єкта критичної інфраструктури індустріального сектору, розроблено узагальнену модель комунікації низькорівневих пристроїв SCADA з використанням емульованого збору даних на базі мікрокомп’ютера Raspberry Pi 5, протоколів передачі даних Modbus та MQTT, можливостей мови програмування Python; дашборд з віджетами для моніторингу на таких рівнях архітектури як низькорівневі пристрої, передачі даних та обробки даних.

Ключові слова: об’єкти критичної інфраструктури індустріального сектору, моніторинг, SCADA, кібератаки.

ABSTRACT

The volume of the thesis is 65 pages, 20 illustrations, 11 tables, 3 appendices and 10 sources of literature.

Research object: Critical infrastructure facilities of the industrial sector.

Research subject: SCADA monitoring system.

The purpose of the research: Development of an architecture for a monitoring system for cyberattacks on critical infrastructure facilities of the industrial sector using SCADA.

Research methods: analysis of literature sources, analysis and synthesis of architectures and mechanisms, computer experiment.

Obtained results: Designed the IT infrastructure architecture of a critical infrastructure object in the industrial sector, developed a generalized model of communication for low-level SCADA devices using emulated data collection based on a Raspberry Pi 5 microcomputer, Modbus and MQTT data transfer protocols, and Python programming language capabilities; a dashboard with widgets for monitoring at architecture levels such as low-level devices, data transmission, and data processing.

Keywords: industrial sector critical infrastructure facilities, monitoring, SCADA, cyber attacks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ICS - Industrial Control Systems, апаратне та програмне забезпечення, яке використовує система та її оператори для забезпечення безпечної роботи промислових систем керування.

SCADA - Supervisory Control and Data Acquisition, це підмножина ICS, яка зосереджена на мережах та інтерфейсах користувача, які сприяють роботі з промисловими системами.

HMI - Human-Machine Interface, апаратний пристрій, що підтримує програмне забезпечення, яке дозволяє людям взаємодіяти з промисловими процесами підприємства; є ключовим елементом для роботи та обслуговування обладнання. Більшість сучасних автоматизованих систем оснащені принаймні одним HMI.

АСУ ТП - автоматизована система управління технологічними процесами; функціональний програмно-технічний комплекс, призначений для контролю і управління промисловими об'єктами, процесами виробництва, оперативно-диспетчерського управління та моніторингу підстанцій.

RTU - Remote Terminal Unit, польовий пристрій, який відповідає за взаємодію з польовими датчиками та виконавчими механізмами. RTU збирають дані з численних датчиків і передають їх до системи SCADA в центрі моніторингу та управління. Вони також можуть отримувати інструкції через систему SCADA щодо роботи з пов’язаними польовими пристроями.

PLC - Programmable Logic Controller, інший клас польових пристроїв в системах SCADA. Зокрема, вони відповідають за керування конкретним обладнанням або процедурами. PLC мають можливість підключатися до основної системи SCADA, забезпечуючи централізований моніторинг і керування декількома PLC, розподіленими по структурі або промисловому процесу.

MTU - Master Terminal Unit, контролер, який також діє як і сервер, на якому розміщено керуюче програмне забезпечення, що спілкується з пристроями керування нижчого рівня, такими як віддалені термінальні пристрої (RTU) і програмовані логічні контролери (PLC).

MES - Manufacturing Execution System, система управління виробництвом на підприємстві.

MOM - Manufacturing Operational Management, управління виробничими операціями на підприємстві.

ERP - Enterprise Resource Planning, система керування ресурсами підприємства: фінансами, активами, аналітикою, моніторингом, процесом виробництва, працівниками, взаємодіями з партнерами.

Dos-атака - denial-of-service, тип кібератаки, під час якої зловмисник прагне зробити комп'ютер або інший пристрій недоступним для призначених користувачів, перериваючи нормальне функціонування пристрою; зазвичай перевантажують цільову машину запитами, що призводить до відмови в обслуговуванні для користувачів.

DDos-атака - distributed denial-of-service, зловмисна спроба порушити звичайний трафік цільового сервера, служби чи мережі, перевантаживши ціль або навколишню інфраструктуру потоком Інтернет-трафіку; використовують численні скомпрометовані комп'ютерні системи як джерела трафіку атак.

MitM - форма кібератаки, у якій злочинці, використовуючи слабкі веб-протоколи, проникають між об'єктами в каналі зв'язку, щоб викрасти дані.

ВСТУП

Останнім часом можна помітити значний ривок у розвитку технологій в системах автоматизованого управління об’єктами критичної інфраструктури, зокрема в індустріальному секторі, що включає в себе енергетичні системи, системи водопостачання, транспорт, телекомунікації, харчову та нафтогазову промисловість чи виробництво, охорону здоров’я. Одним із рівнів автоматизації виробництва на таких об’єктах є SCADA (Supervisory Control and Data Acquisition) - система диспетчерського управління та збору даних. SCADA відіграє вирішальну роль у забезпеченні ефективного функціонування та безпеки об'єктів критичної інфраструктури.

В процесі розвитку SCADA разом із ваговимими перевагами з’явились і значні ризики, адже зі зростанням кількості підключених до мережі пристроїв, з’являються і нові варіації реалізації атак для потенційних зловмисників. Оскільки діяльність об'єктів критичної інфраструктури покриває багато суспільно необхідних сфер, кібератаки на них можуть мати катастрофічні наслідки, починаючи економічними збитками і закінчуючи загрозами для життя і здоров'я людей. Також варто зауважити нинішню воєнну агресію зі сторони сусідньої держави, коли наша критична інфраструктура чи не перша в списку під удар - окрім фізичного фронту, протистояння в кіберпросторі може залишати за собою не менш жахливі наслідки.

Зважаючи на все вищезазначене, можна стверджувати, що нині питання моніторингу даних кібербезпеки на об'єктах критичної інфраструктури набуває особливої актуальності. Ефективна система моніторингу дозволяє відповідальним за інформаційну безпеку на підприємстві вчасно виявляти потенційні загрози, реагувати на інциденти та мінімізувати їх наслідки, проте розробка такої системи є складним завданням, яке вимагає ретельного аналізу архітектури мережі та її компонентів, ідентифікації потенційних вразливостей та вибору оптимальних інструментів моніторингу.

Актуальність роботи

Оскільки ми живемо в умовах стрімкого розвитку технологій, а кількість підключених пристроїв до глобальної мережі все збільшується, то відповідно кількість і складність кіберзагроз для об’єктів критичної інфраструктури постійно зростає. Комунікація в мережі SCADA передбачає обмін конфіденційними даними між дистанційно керованими об’єктами, що приваблює кіберзлочинців до компрометації процесів, виконаними спеціальними пристроями. В свою чергу це вимагає від нас розробки надійних архітектур систем моніторингу та захисту для своєчасного виявлення та протидії потенційним спробам реалізації атак зловмисників.

Кібератаки на такі об’єкти можуть мати серйозні наслідки для економіки, безпеки та добробуту суспільства, життя та здоров’я людей, саме тому забезпечення їх надійного захисту є для нас пріоритетним завданням. Дослідження та розробка методів підвищення безпеки систем SCADA, які широко використовуються для моніторингу та управління об'єктами критичної інфраструктури, є важливим напрямком у сфері кібербезпеки.

Метою роботи є доповнення засобів забезпечення надійного захисту мережі SCADA об’єктів критичної інфраструктури індустріального сектору.

Завданнями роботи є:

1) Здійснити аналіз структури мережі об’єкту моніторингу ICS/SCADA, її компонентів та протоколів комунікації.
2) Побудувати модель загроз та визначити показники превентивного попередження спроб несанкціонованого вторгнення в систему.
3) Запропонувати архітектуру захищеної системи моніторингу ICS/SCADA об’єкту критичної інфраструктури індустріального типу та інтегрувати рішення з комплексного моніторингу IT інфраструктури критичного об’єкта.

Об’єктом дослідження є об’єкти критичної інфраструктури індустріального типу.

Предметом дослідження є система моніторингу показників пристроїв мережі SCADA.

Методи дослідження – аналіз літературних джерел, аналіз та синтез архітектур та механізмів, комп’ютерний експеримент.

Практичне застосування - рішення, які пропонуються в результаті виконання даної дипломної роботи, можуть бути використані для підвищення стійкості та надійності систем захисту критичної інфраструктури індустріального сектору країни; результати дослідження дозволяють розробити ефективні стратегії модернізації застарілих або пошкоджених компонентів систем моніторингу критичної інфраструктури, та як результат, це допоможе в забезпеченні безперервності виробничих процесів індустріального сектору та мінімізує потенційні економічні збитки.

Новизна роботи: дана робота включає в себе інноваційні рішення, що не використовувались попередніми дослідниками даного напряму в кібербезпеці; запропонована архітектура системи моніторингу IT інфраструктури є оригінальним рішенням.

1 SCADA ЯК ЧАСТИНА ІТ-ІНФРАСТРУКТУРИ ТА ІСНУЮЧІ РІШЕННЯ АРХІТЕКТУРИ СИСТЕМИ

1.1 Участь SCADA в міжрівневій взаємодії виробничих процесів ІТ-інфраструктури

Історія активного розвитку автоматизації виробництва та інформаційних технологій у промисловості починається з кінця 70-х — початку 80-х. Важливим сектором промисловості є об’єкти критичної інфраструктури, які мають життєво важливе значення у функціонуванні економіки та забезпеченні безпеки держави, зокрема індустріальні - енергетичні об’єкти, виробничі потужності, транспортні системи, телекомунікаційні мережі, водопостачання та водовідведення.

Міжнародне товариство автоматизації (ISA) відіграло ключову роль у автоматизації ІТ в цьому напрямі. На сьогодні ISA пропонує чотири основні стандарти як основу для сучасних виробничих процесів: ISA-18, ISA-88, ISA-95 та ISA-99. Дані документи містять вичерпну документацію, рекомендації щодо найкращих практик та схеми взаємодії між різними рівнями виробництва. Основною метою цих стандартів є оптимізація виробничих процесів, підвищення ефективності виробництва, мінімізація ризиків, скорочення витрат та зменшення кількості помилок.

Серед цих стандартів ISA-95 набув найбільшого поширення та популярності у промисловості, в тому числі на об’єктах критичної інфраструктури. Він став де-факто стандартом для інтеграції різних систем автоматизації та управління виробництвом, забезпечуючи безперебійну комунікацію та обмін даними між різними рівнями підприємства.

Цей стандарт представляє сучасні системи автоматизації виробництва як складні багаторівневі структури, що поділяються відповідно до контролю технологічних процесів на різних етапах.

0. **Рівень фізичних пристроїв**. Сюди входять сенсори, виконавчі механізми та апаратне забезпечення (hardware). Саме на цьому рівні збираються

виробничі дані, показники для подальшої передачі на рівень вище.

1. **Рівень автоматизації**. Функціонує завдяки програмованим логічним контролерам (PLC) або ж віддаленим термінальним пристроям (RTU). Цей процес є циклічним та замкнутим. Це вже щодо управління механізмами: ці пристрої отримують сигнали від датчиків, обробляють їх відповідно до заданої логіки та генерують сигнали для запуску виконавчих механізмів.

2. **Рівень автоматизованої системи управління технологічним процесом (АСУ ТП)**. На цьому рівні головну роль відіграє людина-оператор, яка взаємодіє з системою через інтерфейси HMI (Human-Machine Interface) та SCADA (Supervision Control and Data Acquisition). SCADA забезпечує моніторинг виробничих процесів, також збирає та архівує дані в реальному часі. Цей рівень працює в рамках якогось певного технологічного процесу і саме з нього починається комп'ютеризований контроль та управління виробництвом у підприємстві.

3. **Рівень системи управління виробництвом (MES) або управління виробничими операціями (MOM)**. На відміну від попередніх рівнів, MES/MOM системи забезпечують комплексне управління виробничим процесом від початку до кінця. Вони інтегрують дані з різних джерел, включаючи SCADA системи, та надають узагальнену інформацію для прийняття більш комплексних управлінських рішень.

MES/MOM системи також управляють активами, запасами та якістю продукції. Вони є зв'язуючою ланкою між рівнями управління технологічними процесами та вищим рівнем управління підприємством - ERP (Enterprise Resource Planning) системами.

4. **ERP системи** призначені для автоматизації бізнес-процесів, організаційно-економічної діяльності та документообігу на рівні всього підприємства. Вони отримують узагальнені виробничі показники від MES/MOM систем, такі як сумарні витрати, питомі значення та інтегровані показники ефективності. Ці дані використовуються для довгострокового

планування, управління ресурсами та активами в масштабах всієї корпорації.

Серед прикладів популярних ERP систем SAP, Oracle, Microsoft Dynamics та вітчизняна 1С «Бухгалтерія», яка широко поширена серед наших українських підприємств.

Така багаторівнева архітектура забезпечує ефективне управління і контроль на всіх етапах виробничої інфраструктури (від окремих польових пристроїв до комплексного управління підприємством). Кожен з вищеперелічених взаємодіє з іншими рівнями, в результаті будучи частиною цілісної системи автоматизації.

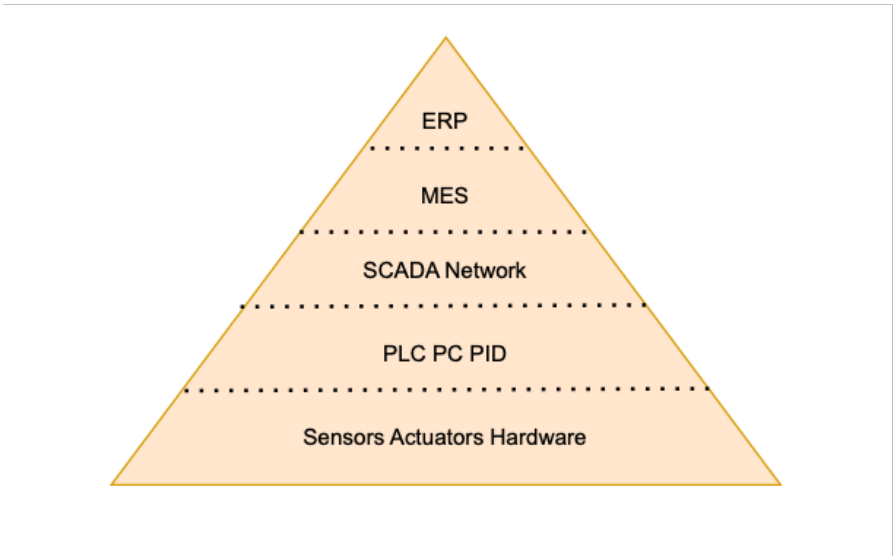

Рисунок 1.1 - Багаторівнева IT архітектура

1.2 Огляд ICS/SCADA

1.2.1 Основні поняття ICS/SCADA

Розглянемо детальніше третій рівень виробничої IT інфраструктури, тобто автоматизовану систему управління технологічним процесом, що включає в себе такі поняття як HMI (Human-Machine Interface) та SCADA (Supervision Control and Data Acquisition).

Якщо говорити про критичну інфраструктуру, то SCADA (Supervisory Control and Data Acquisition) є однією з найбільш широко використовуваних технологій ICS (Industrial Control Systems). ICS це системи промислового контролю, які використовуються для моніторингу та управління промисловими

технологічними процесами, що є важливим компонентом об'єктів критичної інфраструктури індустріального типу.

SCADA застосовується в таких сферах як виробництво, передача та розподіл електроенергії, виробничі галузі чи заводи, харчові та фармацевтичні виробництва, телекомунікаційні та IT-системи, контроль дорожнього руху, ліфт і управління ліфтом, нафтогазові системи, громадський та залізничний транспорт.

1.2.2 Структура SCADA

Ця технологія функціонує як програмний застосунок, призначений для керування промисловими процесами завдяки збору даних у режимі реального часу з віддалених об’єктів. Системи SCADA складаються як з апаратного, так і з програмного забезпечення. Апаратне забезпечення збирає та надсилає дані з датчиків ключового обладнання до контролера, який згодом передає дані іншим системам для обробки в реальному часі та відображення через HMI.

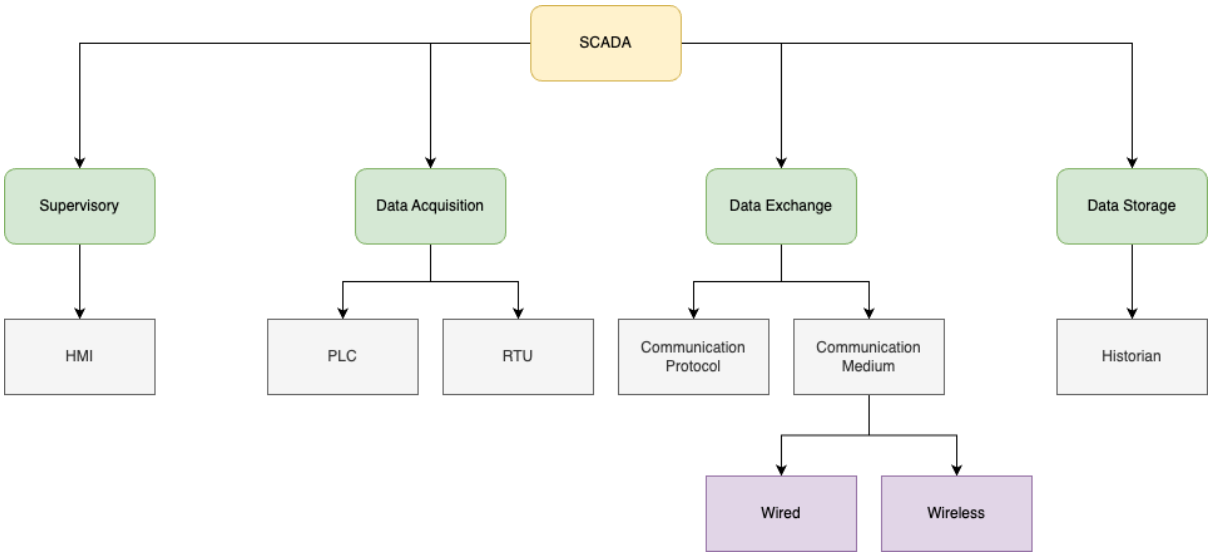

Рисунок 1.2 – Структура SCADA

SCADA складається з наступних компонентів:

Диспетчерський контроль (Supervisory): виконує основну роль HMI - інтерфейсу, відповідального за нагляд за промисловими процесами. З іншого

боку, головний термінал (MTU) функціонує як центральний диспетчерський контролер, який спілкується з нижчими польовими пристроями, такими як RTU, через мережу ICS.

Збір даних (Data Acquisition): дані можуть бути отримані з двох основних джерел: PLC і віддалених термінальних пристроїв (RTU). RTU спеціально розроблені для взаємодії з датчиками та збору телеметричних даних, які вони потім передають до основної системи для подальшого аналізу. PLC взаємодіють із приводами для підтримки та контролю промислових процесів на основі телеметричних даних, зібраних RTU. PLC і RTU діють як фізичні інтерфейси між системами SCADA і польовими пристроями. Однак їх зв'язок із системою SCADA відрізняється. RTU добре підходять для широких географічних зон завдяки використанню методів бездротового зв’язку. Навпаки, PLC більше пристосовані до програм локального керування.

Обмін даними (Data Exchange): для обміну даними між компонентами SCADA використовуються певні комунікаційні протоколи.

Зберігання даних (Data Storage): більшість систем SCADA використовують базу даних SQL для зберігання даних із часовими мітками. Historian — це повністю інтегроване програмне забезпечення SCADA, яке збирає дані в реальному часі з різних пристроїв SCADA та зберігає їх у базі даних.

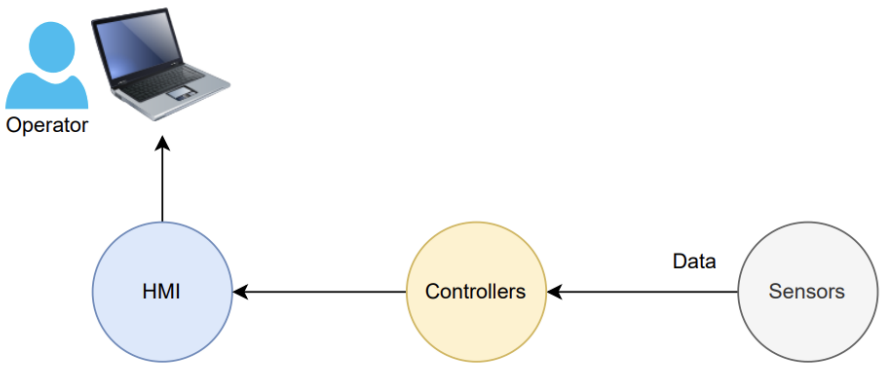

Рисунок 1.3 – Схема взаємодії

Система SCADA включає в себе локальні та глобальні мережі, обидва види передбачають певні протоколи комунікації для забезпечення передачі даних між головною станцією та наземними або ж польовими пристроями.

Датчик — це фізичне обладнання, підключене до PLC або RTU. RTU перетворюють сигнали датчиків у цифрові дані та надсилають цифрові дані на головний сервер. Деякі сучасні датчики мають вбудовані АЦП і можуть відразу передавати дані у цифровому вигляді.

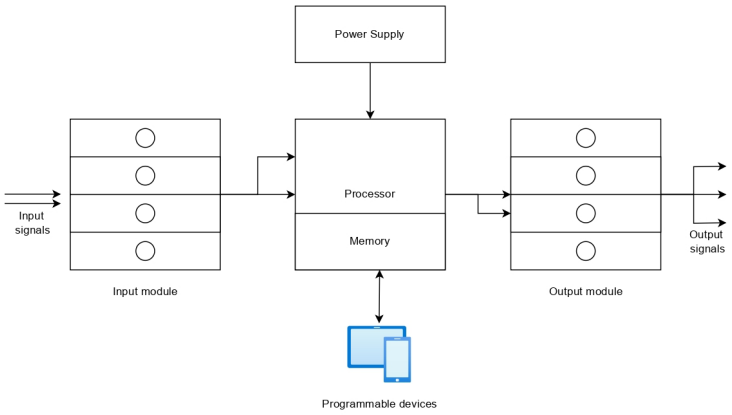

Рисунок 1.4 – Компоненти PLC

1.2.3 Еволюція SCADA

Еволюція та покоління систем SCADA, розуміння яких є важливим для розробки ефективних стратегій захисту, можуть бути описані наступним чином:

Таблиця 1.1 – Покоління SCADA

Рік	Покоління	Опис
1970-1980	1-ше: **Монолітне**	Монолітні системи, розроблені до поширення мережі Інтернет. Базовано на мейнфреймах. Без підключення до інших систем. Комунікаційні протоколи, розроблені виробниками обладнання RTU. Надлишковість досягалася використанням двох однаково оснащених центральних блоків, основного та резервного, підключених на рівні шини. Нині не використовуються.

Продовження таблиці 1.1

1980-1990	2-ге: **Розподілене**	Розподілена архітектура з використанням технології LAN. Обробка розподілена між кількома станціями, з'єднаними локальною мережею, яка обмінюється інформацією в реальному часі. Кожна станція відповідала за певне завдання, що робило розмір і вартість кожної станції нижчими, ніж ті, що використовувалися в першому поколінні. Зовнішні комунікаційні мережі були обмежені протоколами RTU, використовувані мережеві протоколи були все ще переважно пропрієтарні, що призводило до значних проблем безпеки систем SCADA та вразливостей до хакерських атак. Покращена надлишковість та надійність системи, але, оскільки протоколи були пропрієтарними, дуже мало людей за межами розробників і самих хакерів знали достатньо, щоб визначити, як захистити SCADA.
1990-2000	3-тє: **Мережне**	Відкрита системна архітектура. Закладено можливості управління та координації географічно розподілених АСУ ТП. Можливість запуску HMI інтерфейсів у браузерах мобільних пристроїв, можливість віддаленого редагування проекту і тестування нововведень без необхідності зупинення сервера та копіювання файлів проекту. Основне вдосконалення третього покоління полягало у розподілі функціональності через використання протоколів WAN, таких як інтернет-протокол (IP), для зв'язку між головною станцією та комунікаційним обладнанням. Це дозволило відокремити частину головної станції, відповідальну за зв'язок з польовими пристроями, від головної станції через WAN. Використання відкритих стандартів і протоколів.

Кінець таблиці 1.1

2000-Нині	4-те: **Internet of Things (IoT)**	Хмарні обчислення. Зменшення витрат на інфраструктуру та спрощення обслуговування й інтеграції. Використання протоколів глобальних мереж (WAN). Використання відкритих мережевих протоколів пропонує більш зрозумілий і керований периметр безпеки. Децентралізація та уніфікація. В результаті системи SCADA тепер можуть надавати статус майже в реальному часі та використовувати масштабуючі фактори, які забезпечуються хмарними обчисленнями, для реалізації більш складних алгоритмів керування.

Кожне нове покоління систем SCADA означало нові технологічні вдосконалення, покращення функціональності моніторингу, надлишковості, сумісності і зручності використання в робочому виробничому процесі. Однак варто відзначити, що з розширенням можливостей підключення та інтеграції, зросла і поверхня атаки для зловмисників, що в свою чергу створює нові виклики для відповідальних за безпеку систем SCADA на підприємстві критичної інфраструктури. Саме тому вирішення задачі захищеності моніторингу таких об’єктів є для нас нині одним із пріоритетних завдань в галузі кібербезпеки.

1.2.4 Протоколи комунікації в мережі SCADA та їх особливості

DNP3: протокол прикладного рівня, що є міжнародно визнаним стандартом для ICS. Зазвичай працює через протокол управління передачею (TCP) та використовує порт 20000.

Даний протокол реалізований в клієнт-серверній моделі, тобто включає дві функції: головну (клієнт) та підлеглу - зовнішню станцію, сервер. Сервер відповідає на запити клієнта, який поділяється на три рівні: канальний (відповідає за надсилання та отримання кадрів і містить інформацію заголовка,

таку як адреса DNP3 джерела та адреса DNP3 призначення, також відповідає за обчислення помилок за допомогою перевірки циклічної надлишковості (CRC) і перевірку стану зв'язку), транспортний (задача у фрагментації великих пакетів, отриманих прикладним рівнем, тоді як його заголовок містить інформацію, необхідну для повторного збирання фрагментів) та прикладний (створює повідомлення для передачі).

OPC UA: це стандарт обміну даними, що використовується в промисловій автоматизації та комунікації. Загалом протокол OPC UA розроблений як безпечний, масштабований і незалежний від платформи, що робить його ідеальним для промислової автоматизації та систем керування. Його гнучка архітектура дозволяє використовувати його в широкому діапазоні застосунків, від невеликих вбудованих систем до великих корпоративних середовищ.

Хоча протокол OPC-UA можна використовувати на різних транспортних рівнях, таких як TCP/IP, HTTP або MQTT, найпоширенішим є використання через TCP/IP.

Modbus: це стандарт забезпечення зв'язку програмованих логічних контролерів, що дозволяє головному пристрою ефективно обмінюватись даними з кількома підлеглими пристроями.

Протокол приймає унікальний протокольний блок даних (PDU), який відрізняється від звичайної архітектури. Має структуру master-slave. Пристрій, який запитує інформацію, називається клієнтом Modbus (slave), а пристрої, що надають інформацію, — серверами Modbus (master).

IEC 60870: цей стандарт використовується переважно в системах керування електроенергією та автоматизації промислових процесів. Він включає кілька частин, таких як IEC 60870-5-101, IEC 60870-5-102 та IEC 60870-5-104, які визначають протоколи для різних фізичних мереж та варіантів передачі даних.

Message Queuing Telemetry Transport (MQTT): це легкий протокол обміну повідомленнями для публікації та підписки, розроблений для мереж з низькою пропускною здатністю, високою затримкою або ненадійних мереж. Він широко використовується в програмах IoT для передачі даних у реальному часі між пристроями та системами. Легка природа MQTT робить його придатним для пристроїв з обмеженими ресурсами. MQTT може бути вразливим до прослуховування, атак типу "людина посередині" та неавторизованого доступу, якщо його не захищено належним чином. Надійні механізми безпеки та міркування безпеки часто впроваджуються на рівні застосунків, які включають використання TLS/SSL для шифрування та аутентифікації за іменем користувача/паролем.

1.3 Огляд стандартів захисту критичної інфраструктури

Таблиця 1.2 – Стандарти захисту критичної інфраструктури

Назва документу	Зміст
Framework for Improving Critical Infrastructure Security	Питання моніторингу в основному розглядається в розділі Detect (Виявлення): описується безперервний моніторинг активів для виявлення аномалій, індикаторів компрометації тощо. Моніторинг включає також певні підкатегорії, так як моніторинг мереж (DE.CM-01), фізичного середовища (DE.CM-02), активності персоналу та використання технологій (DE.CM-03), діяльності та послуг зовнішніх постачальників (DE.CM-06), апаратного та програмного забезпечення (DE.CM-09)
A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council	Згідно з документом, зростаюче використання кількості цифрових систем управління та моніторингу на підприємствах сприяє і збільшенню кількості потенційних ризиків; стандарт підкреслює, що безперервний моніторинг активів, подій та дій користувачів є ключовим для своєчасного виявлення потенційних інцидентів кібербезпеки.

Кінець таблиці 1.2

Scottish Public Sector Cyber Resilience Framework v1.2	Моніторинг повинен основуватись на оцінці ризиків та охоплювати мережі, системи і дані, які підтримують надання основних послуг; дані моніторингу повинні бути захищені, сповіщення безпеки мають доповнюватися знаннями про загрози і системи.

Дані стандарти дають важливі вказівки щодо спостереження атак, моніторингу системи та реагування на певні інциденти, але організації можуть доповнювати власний моніторинг залежно від особливостей підприємства, специфічних потреб та обставин.

Якщо говорити про об’єкти критичної інфраструктури індустріального типу, хорошим рішенням розширити традиційний моніторинг, щоб укріпити захист. Збір даних не лише на прикладному рівні, але й на більш фундаментальних рівнях технологічного процесу (враховуючи низькорівневі польові пристрої) дасть більш повне та комплексне розуміння активності системи та допоможе превентивно попереджати загрози.

Також варто, окрім моніторингу технологічних показників, відслідковувати події та показники кібербезпеки з усіх рівнів, щоб бачити більш цілісну картину. В такому випадку хорошим рішенням може стати хмарне середовище. Моніторинг на такій платформі відзначається ширшою видимістю - це дозволить вчасно виявляти аномалії та загрози, що можуть бути непомітними з внутрішньої точки присутності. Також таке рішення передбачає меншу поверхню атаки, більш гнучку масштабованість, централізований аналіз, стійкість (оскільки хмара фізично віддалена від критичної інфраструктури) та зовнішній погляд - тобто можливість виявляти активність потенційного зловмисника ще до того моменту, як він отримає доступ до внутрішньої мережі. Отже, є можливість застосування потужних додаткових

можливостей, щоб захистити критичні сервіси та об’єкти, відповідно до цілей даних стандартів.

Висновки до розділу 1

Перший розділ дипломної роботи присвячений технології моніторингу SCADA в об’єкті критичної інфраструктури індустріального сектору. В даному розділі ми розглянули поділ IT інфраструктури на рівні виробничих процесів та роль SCADA системи в цьому розподілі. Також було розглянуто основні поняття ICS/SCADA, саму структуру SCADA, її компоненти та взаємодію між ними.

У першому розділі також описано процес еволюції SCADA системи, зміни в її поколіннях, модифікацію крізь час та покращення. В останньому підрозділі розглянуті протоколи комунікації, характерні для SCADA, їх особливості, технології та застосування. Також описано питання моніторингу у декількох стандартах для критичних об’єктів та доцільність доповнення та покращення традиційного моніторингу.

2 КІБЕРБЕЗПЕКА В SCADA. МОНІТОРИНГ ІТ ІНФРАСТРУКТУРИ ЯК ПРОТИДІЯ КІБЕРЗАГРОЗАМ

2.1 Потенційні джерела загроз SCADA та мотиви зловмисників

Розуміння потенційних джерел загроз для систем SCADA допоможе нам визначити пріоритети безпеки, удосконалити архітектуру безпеки підприємства та розглянути можливості цільових стратегій пом’якшення наслідків. Розглянемо їх детальніше за допомогою таблиці:

Таблиця 2.1 – Джерела загроз SCADA

Джерело	Опис
Хакери	Джерелом загроз можуть виступати незалежні зловмисники (окремі особи чи невеликі угруповання з певними мотивами, навичками та мотивацією), хактивісти (зловмисники, що здійснюють несанкціоноване втручання з метою просування певних політичних або соціальних ідей) або кіберзлочинці (зловмисники, що втручаються в систему в погоні за фінансовою нагородою).
Інсайдери	Серйозною загрозою для підприємства в першу чергу є його співробітники, особливо на об’єкті критичної інфраструктури індустріального сектору, де багато персоналу має доступ до критичних систем та обладнання. Такі ризики можуть виникати через незадоволених співробітників (тих, що мають доступ до SCADA систем та зловживають ним, мотивуючись помстою, фінансовою вигодою або іншими особистими причинами), недбалих працівників (тих, хто становить загрозу безпеці через недотримання політик та процедур безпеки, використання слабких паролів або відкриття фішингових електронних листів тощо) або підрядників та партнерів (зовнішніх сторін, що мають доступ до критичних систем для виконання своїх обов'язків і через це можуть становити загрозу, особливо, якщо цей доступ суворо не контролюється).
Держави-спонсори	Іноземні уряди можуть здійснювати атаки на критичні SCADA системи в цілях шпигунства, саботажу або здобуття стратегічних переваг, в хід можуть йти спеціалізовані підрозділи, що займаються кібероперaціями, або ж можуть використовуватись треті сторони (хакерські угруповання, приватні компанії тощо).

Кінець таблиці 2.1

Терористичні організації	Кібертероризм: терористичні організації можуть атакувати SCADA системи критичних інфраструктур, щоб спричинити руйнування, паніку або підірвати довіру суспільства до влади.

Визначення та розуміння джерел загроз для SCADA є важливим для розробки актуальної моделі загроз. Це дозволяє визначити пріоритети своїх зусиль з безпеки, розробити цільові стратегії пом’якшення наслідків та ефективніше розподілити ресурси для захисту критично важливих систем.

Компоненти SCADA, що керуються на дистанції, у процесі комунікації обмінюються між собою конфіденційними виробничими даними чи показниками. Це часто стає ціллю кіберзлочинців для компрометації технологічних промислових процесів з різними мотивами:

Таблиця 2.2 – Мотиви компрометації SCADA систем

Ціль	Мотив
Порушення технологічних процесів	Зловмисники можуть прагнути порушити нормальне функціонування промислових технологічних процесів, що може призвести до збоїв у виробництві, пошкодження обладнання або навіть до аварійних ситуацій
Крадіжка конфіденційних даних	Зловмисники можуть намагатись отримати цінну інформацію на рівні SCADA про технологічні процеси, інтелектуальну власність, комерційні таємниці з метою промислового шпигунства або продажу інформації конкурентам
Вимагання	Зловмисники можуть шантажувати компанії, погрожувати здійснити атаки на SCADA чи використати скомпрометовані процеси щоб отримати викуп, завдати шкоди компанії, її підлеглим, користувачам, працівникам тощо

Кінець таблиці 2.2

Політичні або ідеологічні ідеї	Атаки на SCADA системи можуть бути здійсненими з політичних або ідеологічних міркувань, наприклад, щоб завдати шкоди економіці країни або висловити протест проти певних дій уряду чи корпорацій
Тестування та демонстрація можливостей	Зловмисники можуть пробувати скомпрометувати SCADA системи, щоб продемонструвати свої навички або знайти вразливості в системах безпеки з метою їх подальшого продажу конкурентам чи на чорному ринку
Підготовка до майбутніх атак	Зловмисники можуть здійснювати розвідку та встановлювати приховані точки доступу в SCADA системах, щоб полегшити собі проведення масштабніших та серйозніших атак у майбутньому

Враховуючи потенційні наслідки компрометації SCADA систем на об'єктах критичної інфраструктури індустріального типу, забезпечення їх надійного захисту є пріоритетним завданням для організацій та держави.

2.1 Модель загроз SCADA

Для правильної оцінки наслідків компрометації процесів у підприємстві, що використовує систему SCADA та визначення показників превентивного їх попередження необхідно скласти актуальну модель загроз. Вона дозволяє ідентифікувати потенційні ризики для підприємств критичної інфраструктури, пріоритезувати заходи безпеки, розробити стратегії пом’якшення наслідків та покращити архітектуру безпеки мережі, відповідаючи нормативним вимогам.

Імовірність реалізації атаки в даній моделі визначається оцінкою експертним методом за шкалою від 1 до 5, де:

Таблиця 2.3 – Оцінка імовірності реалізації атаки експертним методом

1	Дуже низька імовірність

Кінець таблиці 2.3

2	Низька імовірність
3	Середня імовірність
4	Висока імовірність
5	Дуже висока імовірність

Також в модель загроз включені властивості інформації, що порушує атака за успішної реалізації:

К - Конфіденційність,

Ц - Цілісність,

Д - Доступність.

Критичність атаки визначається на основі її потенційного впливу на систему та наслідків у разі успішної реалізації, оцінка надається в таких рівнях:

Таблиця 2.4 – Оцінка критичності атаки

Низька (Low)	Обмежений вплив на систему, не призводить до значних наслідків, можуть спричиняти тимчасові незручності чи збої в роботі системи
Середня (Medium)	Більш серйозні наслідки, такі як втрата функціональності системи, порушення конфіденційності чи доступності даних тощо
Висока (High)	Значний вплив на систему, може призвести до серйозних наслідків (повна втрата функціональності системи, значні фінансові збитки бізнесу, порушення безпеки системи та репутаційні ризики компанії)

Кінець таблиці 2.4

Критична (Critical)	Катастрофічний вплив на систему, може призвести до дуже серйозних наслідків, таких як масштабні збої в роботі системи об’єкта критичної інфраструктури, загроза життю та здоров’ю людей, значні економічні проблеми та фінансові втрати

На основі попередньо зібраного матеріалу розглянемо модель загроз SCADA, представлену в таблиці нижче:

Таблиця 2.5 – Модель загроз SCADA

Загроза	Імовірність	Властивість	Критичність	Механізм реалізації	Mitre Att&ck
Man-in-the-Middle Attack (MITM)	Висока (4)	К, Ц	Висока, критична	Атака "людина посередині" (MiTM) в смарт-мережі полягає в тому, що зловмисники прослуховують або переривають комунікацію між польовими пристроями або між контролером та системою SCADA. Їхні цілі включають зміну інформації, що передається, перешкодження вимірюванням та зміна даних лічильників. Крім того, атаки MiTM використовуються для зміни інформації, що обмінюється в каналі зв’'язку Modbus TCP. Атаки MiTM можуть бути спрямовані на протоколи зв’язку, такі як IEC 60870-5-104, які використовуються в системах SCADA.	Adversary-in-the-Middle T0830
Deception (Spoofing) Attack	Середня (3)	Ц	Висока	Передача хибних даних через датчик або контролер. Атака розроблена для того, щоб ввести систему моніторингу в оману, змусивши її припускати, що об'єкт працює номінально. Підкласом є False Data Injection Attack (FDIA), в якій зловмисник маніпулює показами датчиків, щоб згенерувати шкідливі керуючі дії. Передбачається, що зловмисник має доступ до датчиків і повністю знає систему.	Spoof Reporting Message T0856

Продовження таблиці 2.5

Denial of Service Attack (DoS)/ Distributed Denial of Service (DDos)	Висока (4)	Д	Критична	Канал передачі блокується шляхом передачі надмірної кількості повідомлення (вимірювань), що надходять від датчика. Уповільнюють або переривають роботу системи, що може мати серйозні наслідки, такі як втрата контролю над критичними процесами або збої в постачанні енергії; також можуть використовуватися як спосіб для замаскування інших атак.	Denial of Service T0814
Data Framing Attacks	Середня (3)	Ц	Висока	Вводить в оману центр керування, шкідливі вимірювання призводять до недостовірних даних, намагається ввести в оману ідентифікацію та видалення поганих даних (BDIR), щоб відокремити безпечні дані та надає результати в неточній оцінці стану.	Spoof Reporting Message T0856
Load Altering Attack	Висока (4)	Д	Висока	Спрямовані на зміну споживання електроенергії об'єктами критичної інфраструктури, такими як системи електропостачання. Їхня мета полягає в перевантаженні ліній електропередачі. Ці атаки можуть використовувати два основних методи: пряме вторгнення у навантаження та опосередковану модифікацію навантаження через експлуатацію.	Modify Parameter T0836
Malicious Command Injection Attack	Висока (4)	Ц, Д	Висока	Трансформатори зі зміщенням фаз або фазові зміщувачі використовуються в силових мережах для регулювання потоку електричної енергії. У системах автоматизованої електропостачання команди на зсув фаз передаються через систему SCADA. Тут вразливість до кібератак: зловмисні команди можуть викликати перевантаження ліній передачі, відключення електропостачання та фінансові втрати. Крім того, система SCADA може ініціювати зловмисні команди під легітимним виглядом, що може призвести до фізичних втручань. Зловмисні зміщувачі фаз також можуть модифікувати команди, що призводить до небезпечних змін у роботі трансформаторів.	Hooking T0874 Scripting T0853

Продовження таблиці 2.5

Load Redistribution Attacks	Середня (3)	Ц, Д	Висока	Атаки на перерозподіл навантаження (LR), які пов'язані з атаками внесення неправдивих даних в станову оцінку (SE-FDIAs), в яких вимірювання навантаження та електричних потоків змінюються, але попит на загальну потужність не модифікується. Таким чином, результатом атаки є перерозподіл навантаження через мережу. Крім того, це може призводити до фінансових втрат та інших фізичних пошкоджень, наприклад, відключення ліній або прямі атаки на них.	Spoof Reporting Message T0856
Coordinated Cyber Physical Topology Attacks	Низька (2)	Ц	Висока	Атаки поділяються на фізичні топологічні та кібер-топологічні. У фізичній топологічній зловмисник відключає лінію передачі, тоді як у кібер-топологічній він вводить в оману контрольний центр, маскує сигнал відключення відключеної лінії на кібер-рівні та генерує фальшивий сигнал відключення для іншої лінії передачі. Остаточною метою координованої атаки на топологію є навантаження критичної лінії, вводячи контрольний центр в оману та змушуючи його приймати неправильні рішення.	Service Stop T0881
Malware Attacks	Висока (4)	Ц, К, Д	Критична	Кібератаки на системи смарт-мережі включають в себе атаки за допомогою шкідливих програм, включаючи троянські програми BlackEnergy, Stuxnet і розповсюдження розшифрованих вірусів WannaCry.	Exploitation of Remote Services T0866
Zero Dynamics Attack	Низька (2)	Д, Ц	Критична	Це невидима атака з відкритим циклом, яка спрямована на внутрішню динаміку мережевої системи управління, вимагає знання системи. Враховує внутрішню поведінку системи мережі для зловживання нею та надання нульового виходу. Для генерації атаки з нульовою динамікою може бути внесений сигнал в систему для розбіжності внутрішнього стану, який не помітний лише зі звичайного спостереження. Наявність геометрично зростаючого входу без видимих змін на виході робить ZDA серйозною загрозою.	Masquerading T0849

Продовження таблиці 2.5

Data Integrity Attack	Середня (3)	Ц	Середня	Передачі модифіковані для створення помилкового сигналу. Атаки, під час яких дані пошкоджуються в прямому або зворотному шляху в потоці керування. Атака пошкоджує дані датчика, якими в даному випадку є дані PMU, або дані приводу, які є командою, наданою елементам захисту або елементам керування VAR. Це означає такі дії, як блокування сигналів відключення у сценаріях, коли контролер фактично надсилає команду відключення елементам захисту або контролер надає команду збільшити введення VAR, тоді як атака спричиняє зменшення введення або навпаки.	Modify Controller Tasking T0821
Replay Attack	Середня (3)	Ц	Висока	Є атакою із замкнутим циклом, тобто для створення сигналу атаки потрібна онлайн-інформація. Атака відтворення здійснюється у два кроки: спочатку зловмисник бере контроль над датчиками та записує вихідні дані датчика протягом достатнього часу (без введення додаткових даних у систему). Потім зловмисник вводить послідовність бажаних вхідних даних, одночасно відтворюючи вихідні дані, записані раніше.	Internet Accessible Device T0883
Covert Attack	Низька (2)	К, Ц	Критична	Зловмисник має доступ до датчиків і контролера, а також повні знання про систему. Зловмисник маніпулює як керуючими діями, так і показаннями датчиків, щоб шкідлива дія була повністю замаскована. Ця атака в основному працює за принципом скасування ефекту сигналу атаки шляхом обчислення виходу та віднімання показань, які вимірюються. Атака може отримати доступ до даних, а також ввести неправдиві дані в канали датчиків і виконавчих механізмів CPS.	Modify Parameter T0836

Кінець таблиці 2.5

Location Attack	Середня (3)	Ц, Д	Висока	Залежно від місця атаки з точки зору мережевого управління може бути декількох типів. Атака на датчик: передані вимірювання змінюються під час цієї атаки. Атака на контроль: контрольний сигнал змінюється. Атака на привід: сигнал привода спотворюється. Атака через навантаження: під час роботи LFC зловмисник також може проникнути через порушення навантаження.	Modify Parameter T0836
Template Attack	Висока (4)	Ц, Д	Середня, висока	Атака може бути введена шляхом зміни амплітуди сигналу повідомлення. Масштабна атака: Масштаб або значення повідомлень масштабується. Ramp attack: повідомлення постійної величини передається безперервно. Імпульсна атака: передача набуває форму імпульсу з фіксованим часом. Випадкова атака: поширюються повідомлення випадкових значень. Резонансна атака: повідомлення змінюється відповідно до джерела резонансу (наприклад, швидкість зміни частоти). Атака ін’єкції зміщення: у цій атаці постійний сигнал зсуву вводиться в канали датчиків або сигналу керування.	Modify Parameter T0836

2.3 Показники превентивного попередження загроз

2.3.1 Індикатори спроби реалізації атак

Man-in-the-Middle: дана атака працює в двох режимах: підслуховування або перехоплення/зміна. В першому режимі атакуючий підслуховує дані з каналу комунікації, щоб зрозуміти фізичні та комунікаційні операції цілі. Згодом атакуючий використовує отримані знання щоб перехопити або змінити певні специфічні пакети в каналі комунікації в другому режимі. Саме тому

спостереження такого типу атак на ранньому етапі, тобто в режимі прослуховування, є дуже бажаним.

У режимі підслуховування зловмисник MITM відстежує запити контролера та/або відповіді пристрою живлення, не роблячи жодних змін до цих повідомлень. Хоча атака MITM вважається неактивною в цьому режимі, її ефект можна помітити в часовій області в дротових і бездротових мережах зв'язку. Наприклад, в бездротових комунікаційних мережах зловмисник MITM може маніпулювати таблицею ARP відправника та одержувача щоб служити проміжним вузлом між ними. Хоча відправник транслює повідомлення в бездротової мережі, одержувач не отримує це повідомлення, оскільки воно містить MAC-адресу зловмисника MITM. Натомість зловмисник отримує це повідомлення, а потім надсилає його одержувачу.

Зловмисником можуть вводитись часові затримки для моніторингу та повторної передачі. Якщо спостерігаються незвичайні затримки або коливання часу відгуку, особливо для критично важливих команд або даних датчиків, це може свідчити про присутність зловмисника, який перехоплює та потенційно маніпулює трафіком.

Показниками спроби здійснення атаки стосовно працівників критичного підприємства можуть бути: неочікуване або повторюване відключення від мережі (інтернет стає нестабільним по незрозумілим причинам - здійснюється примусове відключення користувача для перехоплення логіну та паролю), дивні адреси в адресному рядку браузера (перенаправлення на підроблені веб-сайти - DNS перехоплення), загальнодоступні та незахищені Wi-Fi мережі.

“Червоними прапорцями” можуть бути незвична поведінка користувача в мережі, шкідливі мережні підключення.

Також варто звернути увагу на несподівані зміни в мережевій топології (поява невідомих пристроїв, несанкціоновані зміни конфігурації мережевих пристроїв або несподівані зміни в маршрутизації трафіку), розбіжності в сертифікатах і ключах шифрування, невідповідності протоколів (неправильно

сформовані пакети, несподівані команди або відповіді, які не відповідають стандартам, шаблонам зв'язку чи специфікаціям протоколу тощо).

Deception (Spoofing) Attack: про спробу здійснення цієї атаки можуть свідчити раптові або незвичайні зміни в показаннях датчиків, невідповідності між показаннями різних датчиків, які повинні корелювати або мати певні взаємозв'язки, значення датчиків, які виходять за межі нормальних робочих діапазонів або перевищують встановлені порогові значення.

Варто звертати увагу на аномальну поведінку процесу: наприклад, неочікувані зміни в процесі попри нормальні показання датчиків, процес реагує неадекватно на команди управління або не досягає очікуваних станів, аварійні сигнали або події без причини.

Також поганим знаком є несподівані шаблони зв’язку або сплески трафіку між датчиками, контролерами та серверами SCADA, спроби доступу до пристроїв або систем з невідомих або несанкціонованих IP-адрес та незвичайні протоколи або пакети даних.

Denial of Service Attack (DoS) / Distributed Denial of Service (DDos): про спробу реалізації однієї із даних атак можуть нам підказати раптова та висока інтенсивність вхідного шкідливого трафіку, що надходить до серверів SCADA, робочих станцій операторів або мережевих пристроїв. Затримки або переривання в обробці запитів легітимного трафіку - наприклад, при передачі даних від польових пристроїв або контролерів.

Поганим знаком є аномальне використання ресурсів - наприклад, висока зайнятість процесора, пам’яті або мережевих ресурсів на серверах SCADA або мережевих пристроях (зомбі-машини, задіяні в DDoS).

Індикаторами можуть також бути флуд ICMP, UDP або SYN пакетами, численні спроби підключення з однієї або декількох IP-адрес протягом короткого проміжку часу, численні записи про помилки, збої підключення або перевищення часу очікування на серверах SCADA або мережевих пристроях, повторювані повідомлення про недоступність служб або ресурсів.

Data Framing Attacks: поганим знаком є отримання суперечливих або неможливих значень вимірювань від датчиків або польових пристроїв, також значень, що виходять за межі очікуваних діапазонів або не відповідають фізичним обмеженням контрольованого процесу, різкі або нехарактерні зміни у вимірюваних даних без видимих причин, невідповідності між даними, отриманими від різних датчиків або систем, які повинні корелювати.

Генерація недійсних або недоречних команд управління на основі спотворених даних серед вимірювань, спроби надсилання даних від неавторизованих або невідомих джерел.

Load Altering Attack: такі атаки можуть призвести до неоптимального розподілу ресурсів, перевантаження обладнання або порушення стабільності системи SCADA.

Про спробу їх здійснення можуть свідчити несподівані команди управління або дії - наприклад, невиправдане відключення навантаження або перерозподіл ресурсів, погіршення продуктивності або стабільності системи, погіршення показників якості електроенергії, таких як коливання напруги або гармонійні спотворення, нестабільність або коливання в роботі системи управління без видимих зовнішніх чинників, спроби доступу або маніпулювання даними навантаження з неавторизованих або невідомих джерел.

Malicious Command Injection Attack: несподівані або недійсні команди управління, наприклад команди, які намагаються змінити критичні налаштування системи або обійти механізми безпеки. Непояснені зупинки, перезапуски або зміни режимів роботи системи. Спроби доступу до системи управління з невідомих або неавторизованих IP-адрес або пристроїв, підозріло високий обсяг або частота віддалених підключень до критичних компонентів системи.

Активація сигналізацій або захисних механізмів, таких як системи безпеки або блокування, без явної причини або ж спроби обійти та відключити

ці системи.

Load Redistribution Attacks: особливо актуальні для об’єктів критичної інфраструктури індустріального типу таких як енергетичні системи. Про спробу втручання можуть свідчити значні розбіжності між повідомленими вимірюваннями навантаження або потоку та очікуваними значеннями на основі історичних даних або моделей прогнозування, неочікувані або неавторизовані зміни в конфігурації комутаторів, лініях передачі або інших компонентах мережі.

Надмірне використання або перевантаження певних ліній передачі, трансформаторів або інших компонентів мережі. Порушення встановлених меж напруги, термічних обмежень або інших порогових значень безпечної роботи в певних сегментах мережі. Незвичайні звуки, вібрації або теплові сигнатури від трансформаторів, ліній передачі або іншого обладнання, що може вказувати на перевантаження або спрацьовування захисних реле, вимикачів чи інших механізмів без явних причин.

Coordinated Cyber Physical Topology Attacks: невідповідності між даними SCADA та фізичними вимірюваннями - наприклад, система SCADA може показувати, що лінія передачі працює нормально, тоді як фізичні вимірювання вказують на її відключення.

Несподівані зміни стану топології мережі, часті або постійні збої зв'язку між контрольним центром та віддаленими пристроями або підстанціями.

Malware Attacks: індикаторами компрометації можуть бути аномалії в мережевому трафіку, несподівані збої, перезавантаження або зависання системи або пристроїв.

Також свідчити про зловмисні дії можуть несанкціоновані зміни в конфігурації системи, налаштуваннях безпеки або обліковій політиці, використання облікових записів з високим рівнем привілеїв для виконання незвичних або несанкціонованих дій, створення нових облікових записів адміністратора або зміна привілеїв існуючих облікових записів без належної

авторизації. Спроби несанкціонованого доступу, модифікації або видалення важливих системних файлів або файлів даних. Підозріла активність запитів до бази даних, наприклад масове вилучення або зміна записів. Незвичайна активність процесора або пам'яті - запуск підозрілих або невідомих процесів, які споживають значні системні ресурси. Зміни в хеш-значеннях файлів або цифрових підписів критичних системних компонентів або виконуваних файлів, що вказує на несанкціоновані модифікації.

Zero Dynamics (ZD) Attack: аномалії в поведінці процесу, аномалії серед даних телеметрії або сенсорів, незвичайний мережевий трафік, зміни в кореляціях між змінними, несподівані зміни в конфігурації або прошивці контролерів, нестандартні або застарілі протоколи комунікації.

Data Integrity Attack: різкі зміни показників датчиків, функціонування виконавчих механізмів всупереч командам управління, спотворення, дублювання або втрата пакетів промислових протоколів, підозріла активність на портах, які зазвичай не використовуються в обміні даними, одночасна активація взаємовиключних механізмів.

Replay Attack: атака на відтворення вимагає онлайн-інформації для створення сигналу атаки. Вона виконується у два прості кроки: спочатку зловмисник бере під контроль датчики та записує дані на виході датчиків протягом достатнього періоду часу (без введення додаткових даних у систему). Потім зловмисник вводить послідовність бажаних вхідних даних, одночасно відтворюючи раніше записані вихідні дані. Ефект цієї атаки полягає в тому, що система буде поводитися так, ніби записані дані датчиків все ще генеруються, навіть якщо фактичний стан системи може змінитися.

Показники, за якими можна превентивно відстежувати атаку: довга незмінність, раптові стрибки або розриви в значеннях датчиків, надмірна частота оновлення даних, часові мітки даних від датчиків не співпадають з поточним системним часом.

Covert Attack: про спробу здійснення атаки можуть свідчити аномалії в

показаннях датчиків (застиглі або довго незмінні значення, раптові стрибки, падіння, відхилення від очікуваних значень), невідповідності між командами контролера та станом системи, несподіваний трафік чи спроби доступу, фізичні індикатори: незвичні звуки, вібрації або показники від фізичного обладнання, несподівані зміни в конфігурації системи.

Location Attack: дані датчиків раптово змінюються (різкі стрибки чи застигання), підозрілі зміни в мережевому трафіку (частота, розміри пакетів тощо), ігнорування або неправильне виконання команд оператора (щодо зміни режиму роботи пристроїв, запуску/зупинки обладнання тощо), підозрілі події в мережевому трафіку контролерів (неочікувані спроби підключення, зміни прошивок, перезавантаження тощо), неочікувані відхилення фактичного навантаження від прогнозованих, проблемний баланс потужності в енергосистемі, порушені обмеження в контрольних точках енергомережі.

Template Attack: монотонне зростання або спадання показників, вихід значень показників за встановлені безпечні межі, підозріле биття, вібрації або акустичний шум в обладнанні, зниження ефективності, підвищена витрата енергоносіїв, безпричинна активація сигналізацій.

2.3.2 . Узагальнення показників та спостереження на низькорівневих пристроях

Якщо узагальнювати показники спроб компрометації процесів по всій IT інфраструктурі стосовно пристроїв та обладнання, можна виділити інформацію в такій таблиці:

Таблиця 2.6 – Показники превентивного попередження атак

Мережеве обладнання (комутатори, маршрутизатори, фаєрволи)	Спроби сканування портів, підозрілі пакети чи потоки даних, аномальні сплески трафіку (напр. у вихідний день або неробочий час), підключення з невідомих зовнішніх IP-адрес, зміни в таблицях маршрутизації, ARP-таблицях, збільшення затримок або колізій в мережі, пакети з некоректними заголовками, фрагментацією чи TTL, втрати пакетів у мережі, спроби перепризначення портів або зміни конфігурації без відповідної авторизації

Кінець таблиці 2.6

Сервери (файлові, поштові, застосунків, веб тощо)	Невдалі спроби входу (особливо повідомлення щодо акаунтів з підвищеними привілеями), аномальні сплески використання CPU, пам'яті, дискового вводу-виводу, неочікувані з'єднання з невідомих IP-адрес або через незвичайні порти, несанкціоновані зміни важливих системних файлів або ключів реєстру
Бази даних	Спроби SQL ін'єкцій, аномальна кількість запитів від одного користувача або IP-адреси, спроби масового видалення даних
Робочі станції та ПК	Аномальна активність браузера (неочікувані перенаправлення, несподівано спливаючі вікна чи розширення), спроби деактивації або зміни налаштувань антивірусу, брандмауера; підозрілі мережеві з'єднання з незнайомими зовнішніми IP-адресами або незвичними доменами, аномальні сплески використання CPU, оперативної пам'яті, незвичайна активність користувача
Мобільні та IoT пристрої	Спроби підключення з невідомих або недовірених пристроїв, аномальний обсяг даних, що передаються на зовнішні сервери, використання нешифрованих або слабо захищених протоколів, спроби доступу до пристроїв або зміни налаштувань в обхід механізмів автентифікації, несподівані оновлення прошивки або конфігурації, особливо з недовірених джерел

Загалом перелічені показники можуть надходити від різних джерел, таких як системні журнали, мережеві пристрої, датчики, контролери та прикладні програми. Варто звернути окрему увагу на **низькорівневі** пристрої SCADA, включаючи програмовані логічні контролери (PLC), віддалені термінали (RTU), інтелектуальні електронні пристрої (IED), а також різноманітні сенсори та виконавчі механізми, які можуть бути цінним джерелом попередження: сигналізувати про тривогу можуть і фізичні показники, і вплив на мережеві протоколи.

Таблиця 2.7 – Показники превентивного попередження атак на низькорівневих пристроях SCADA

Несподівані зміни стану системи	Раптові неочікувані зміни в стані виконавчих пристроїв - регуляторів, вимикачів, засувок, клапанів тощо (без відповідних команд від оператора або алгоритму управління) або ж невідповідність фактичного стану виконавчого механізму команді управління
Аномалії в значеннях сенсорів	Показники сенсорів (тиск, температура, напруга тощо) різко змінюються, виходячи за рамки норми або ж взагалі перестають оновлюватись, невідповідність показників резервних сенсорів стосовно основних
Дивна поведінка в мережі комунікації	Неочікувані спроби підключення до PLC чи RTU з невідомих IP-адрес, в незвичний час; підозріло підвищена частота запитів до контролерів, поява нових протоколів в комунікації між пристроями (наприклад, нехарактерні для АСУ ТП рівня - HTTP, SSH, Telnet тощо), спроби зміни прошивки або конфігурації без відома відповідальних спеціалістів, спроби запису значень в регістри Modbus або теги DNP3, що зазвичай використовуються лише для читання
Підозріла поведінка пристроїв	Контролери перестають відповідати на запити чи команди управління SCADA-серверів або оператора, самовільно змінюють режим роботи, виключаються чи перезавантажуються, невідповідність часових міток подій, події на пристрої в неправильному, неочікуваному порядку, завантаження конфігурацій в контролери в неробочий час, підвищене енергоспоживання виконавчих механізмів, несподіване зношування або відмова механічного обладнання, аномальні шуми

Також не виключаємо можливість того, що дані індикатори можуть бути викликані певними технічними проблемами, але у поєднанні з іншими

(мережевими логами, подіями безпеки тощо) це може вказувати на спробу компрометації процесів зловмисниками.

Необхідно відстежувати поведінку низькорівневих пристроїв, їх стан та активність, регулярно передавати ці дані на верхні рівні інфраструктури для аналізу та кореляції подій. Щоб запобігти втручанням, обов’язково треба мінімізувати можливості фізичного доступу до польових пристроїв, регулярно оновлювати їх прошивки, відключати невикористовувані мережеві сервіси, застосовувати шифрування та аутентифікацію при обміні даними.

Висновки до розділу 2

Другий розділ диплому присвячено питанням безпеки SCADA систем. Розглянуто потенційні джерела загроз та мотиви зловмисників, що можуть здійснювати спроби несанкціонованого вторгнення в роботу SCADA систем на об’єктах критичної інфраструктури індустріального сектору. Також на основі здійсненого дослідження літературних джерел складено актуальну модель загроз для SCADA, описано атаки та їх вплив.

В останньому підрозділі визначено показники превентивного попередження атак на основі їх особливостей та методів реалізації, окремо закцентовано увагу на відстеженні подій на низькорівневих пристроях, індикаторах на них та рекомендаціях щодо захисту від несанкціонованого втручання у виробничі процеси.

3 ВПРОВАДЖЕННЯ ТА АНАЛІЗ МОЖЛИВОСТЕЙ МОНІТОРИНГУ SCADA СИСТЕМ

3.1 Архітектура мережі об’єкта критичної інфраструктури

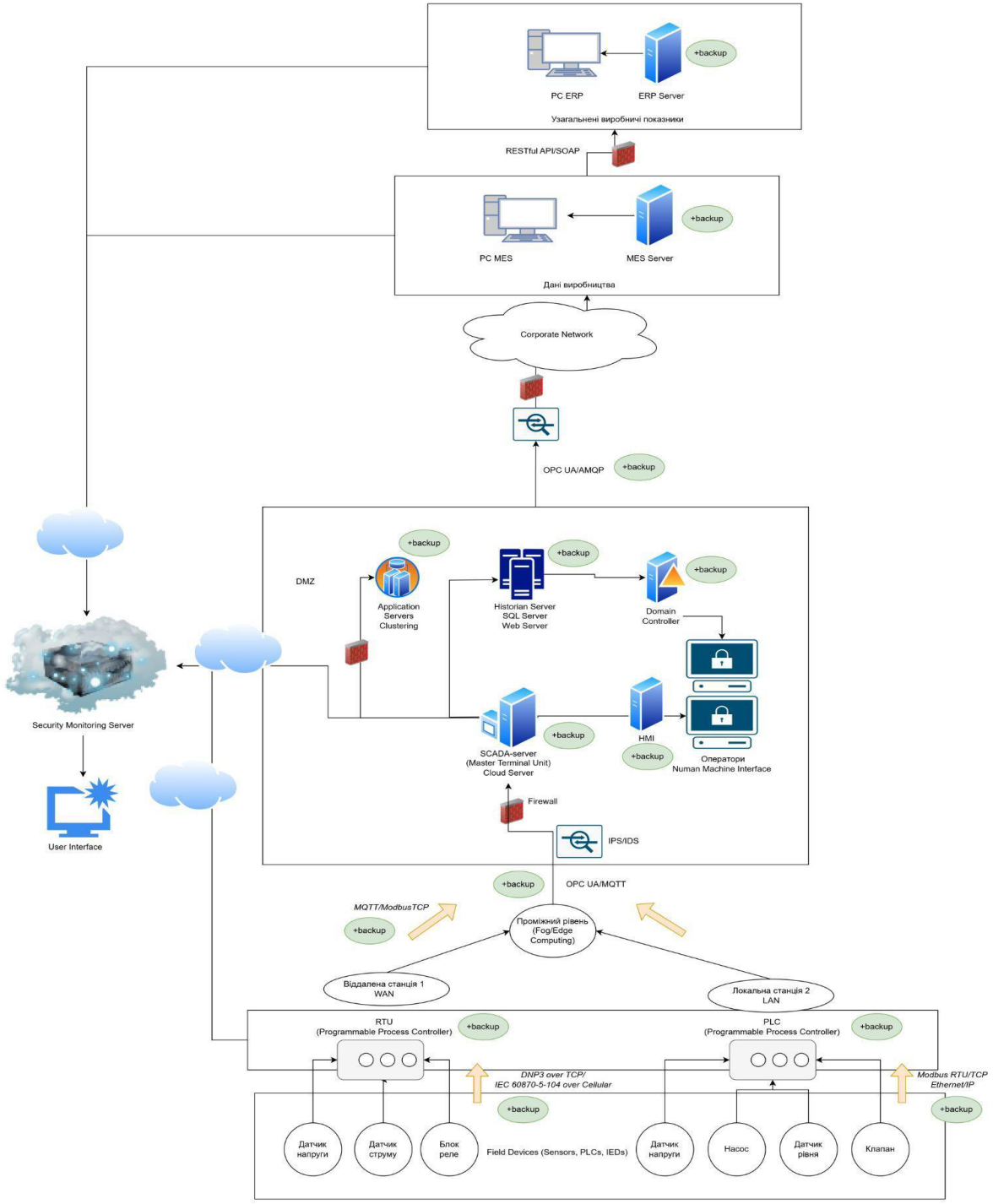

Рисунок 3.1 – Спроектована архітектура мережі

В даній запропонованій архітектурі взаємодія між компонентами SCADA системи відбувається наступним чином:

Таблиця 3.1 – Взаємодія в IT інфраструктурі критичного підприємства

Етап	Опис
Збір даних з рівня процесу	Виробничі датчики (напруги, струму, тиску, температури, рівня тощо) безперервно вимірюють параметри технологічного процесу. Програмовані логічні контролери (PLC) і віддалені термінали (RTU) опитують датчики по протоколах Modbus RTU, DNP3 з частотою 100-500 мс для аналогових сигналів і 10-100 мс для дискретних сигналів.
Обробка даних на Fog/Edge рівні	Fog вузли, розміщені поблизу PLC/RTU, збирають дані з декількох пристроїв, агрегують їх і виконують попередню обробку (фільтрація, перевірка достовірності). Fog вузли можуть виконувати локальні алгоритми управління процесом для швидкого реагування на зміни.
Передача даних на SCADA сервер	Fog вузли передають оброблені дані на центральний SCADA сервер за допомогою протоколів OPC UA, MQTT. Оновлення даних на SCADA сервері відбувається кожні 1-2 секунди (для даних реального часу).
Обробка і зберігання даних на серверах	SCADA сервер отримує, обробляє і відображає дані реального часу на автоматизованих робочих місцях (АРМ) операторів з використанням зручного людино-машинного інтерфейсу (HMI). Historian сервер отримує дані від SCADA сервера по протоколу OPC UA, зберігає історичні тренди параметрів і формує звіти. Web сервер отримує обрані дані від SCADA, Historian або SQL сервера і публікує їх на веб-порталі для віддаленого доступу авторизованих користувачів з відповідними правами доступу.

Кінець таблиці 3.1

Взаємодія з MES системою	MES сервер отримує агреговані дані про хід виробництва (обсяги продукції, параметри процесу, події простоїв і браку тощо) від SCADA або Historian сервера по протоколу OPC UA з інтервалом 1-5 хвилин. Також MES передає на SCADA завдання, вказівки і команди управління процесом, які головний SCADA сервер транслює на відповідні контролери через Fog вузли.
Взаємодія з ERP системою	На наступному рівні ERP сервер отримує узагальнені дані про виробництво (тобто обсяги випуску, витрати сировини, енергоресурсів, ключові показники ефективності) від MES сервера з інтервалом 10-60 хвилин. В ERP системі ці дані використовуються для планування ресурсів, управління запасами, розрахунку собівартості і фінансового обліку критичного підприємства.
Моніторинг подій кібербезпеки	Такі компоненти як PLC/RTU, Fog вузли, сервери і мережеве обладнання реєструють показники кібербезпеки (наприклад, логіни користувачів, зміни конфігурації, підключення/відключення пристроїв) і передають їх на сервер моніторингу, хмарну платформу. Система виявлення вторгнень (IDS) аналізує мережевий трафік в реальному часі, виявляє аномалії і генерує попередження, які надсилаються на сервер комплексного моніторингу IT інфраструктури підприємства.

Для об'єктів критичної інфраструктури індустріального типу (таких як електростанції, нафтопереробні заводи, металургійні комбінати, хімічні виробництва тощо) частота опитування датчиків і оновлення даних зазвичай більша, ніж для менш критичних об'єктів, адже потрібно відповідати підвищеним вимогам до надійності, безпеки і швидкості реагування на події в таких системах.

Для відстеження ситуації з технологічними показниками

використовується людино-машинний інтерфейс (HMI), що є фактично вікном у SCADA процеси: HMI графічно відображає всі об'єкти всередині системи.

Система зазвичай передбачає різні сигнали тривоги для того, щоб віддалено сповіщати операторів через пейджери, текстові повідомлення або якийсь інший тип віддаленого сповіщення. Завдяки цьому вона може постійно функціонувати без необхідності, щоб хтось сидів за комп'ютером 24 години на добу, 7 днів на тиждень.

Також розглянемо детальніше спосіб побудови захищеної архітектури мережі підприємства: для початку, між корпоративною мережею та мережею SCADA розміщення фаєрволу дозволяє контролювати та фільтрувати трафік між цими мережами, захищаючи мережу SCADA від потенційних загроз з боку корпоративної мережі або зовнішніх джерел. Додаткові міжмережеві екрани розміщені між різними сегментами мережі (віддалені станції (RTU, PLC), сервери SCADA, MES і ERP) - це забезпечує комплексну **сегментацію** мережі та дозволяє ефективно контролювати доступ між різними компонентами інфраструктури, тим самим мінімізуючи ризик поширення потенційних загроз.

Завдяки розміщенні серверів та служб, які повинні бути доступні з зовнішніх мереж (як веб-сервер або сервер застосунків) в демілітаризованій зоні (**DMZ**) відбувається ізоляція цих компонентів від внутрішньої мережі SCADA та тим самим забезпечується додатковий рівень безпеки.

Для всіх критичних компонентів системи (сервери SCADA, MES, ERP, бази даних та контролери) передбачаються резервні копії (**backup**), що дозволяє швидко відновлюватись у разі збоїв або кібератак, що призводять до втрати даних або функціональності.

Варто відмітити розміщення систем виявлення та запобігання вторгненням (**IPS/IDS**) на межі мережі SCADA, що надає можливість моніторингу вхідного трафіку в цю мережу, виявляти потенційні спроби атак, аномалії тощо та вчасно вживати заходи щодо їх запобігання чи блокування.

Також важливим компонентом архітектури мережі є **Security Monitoring**

Server, розміщений у хмарі. Використання такого рішення як хмарної платформи дозволяє збирати та аналізувати дані з точки зору кібербезпеки з різних компонентів та рівнів системи, забезпечувати централізований моніторинг та можливість агрегації даних з декількох об'єктів або систем. Також хмарне середовище дає нам змогу бачити більш комплексну ситуацію по мережі таких об'єктів, наприклад по всій енергосистемі і відповідно приймати більш виважені рішення.

Зважаючи на все вищезазначене, можна підсумувати, що розташування об'єктів захисту, яке запропоноване в даній архітектурі мережі, забезпечує багаторівневу модель безпеки. Такий підхід охоплює багато аспектів, починаючи мережевою сегментацією, контролем доступу та закінчуючи моніторингом з реагуванням на інциденти. Завдяки цьому ми можемо ефективно захищати IT інфраструктуру підприємства від потенційних кібератак, мінімізувати їх потенційні ризики, забезпечувати надійність та стійкість об'єкта критичної інфраструктури.

3.2 Комунікація на низькорівневих пристроях SCADA

Для емуляції передачі даних на низькорівневих пристроях, а саме сенсорах та контролерах через протокол Modbus було реалізовано скрипти за допомогою засобів мови програмування Python та бібліотеки pymodbus.

У якості Modbus-master було використано пристрій Raspberry Pi 5 з попереднім налаштуванням мікрокомп’ютера для подальшої роботи:

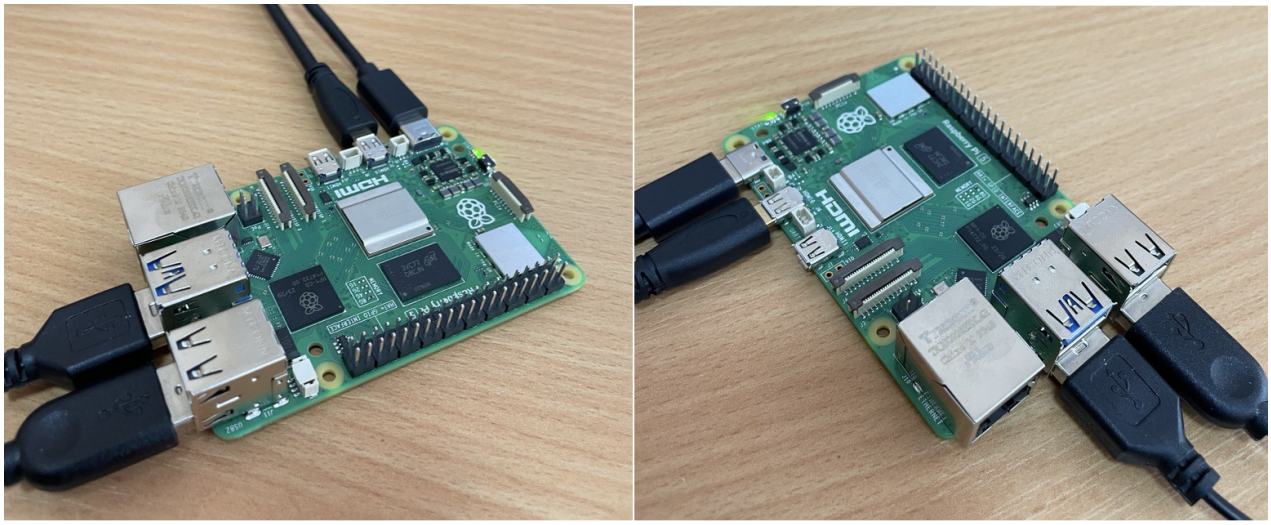

Рисунок 3.2 – Налаштований та підключений Raspberry Pi 5

З modbus-slave пристрою відбувається передача показників енергетичного підприємства критичної інфраструктури індустріального типу на modbus-master за допомогою функції:

```
def main():
    #Відкриття Modbus з'єднання та створення Modbus-client
    client = ModbusTcpClient(server_ip, port=server_port)

    #Підключення до Modbus-server
    client.connect()

    #Запис даних датчиків електростанції
    write_power_plant_data(client)

    #Закриття Modbus з'єднання
    client.close()
```

Рисунок 3.3 – Функція відкриття Modbus з'єднання

За допомогою pymodbus функції write_register дані записуються в Modbus input registers, тобто регістри вводу.

Modbus-master приймає ці дані для запису:

```
#Блоки даних для зберігання значень датчиків
sensor_data_block = ModbusSequentialDataBlock(40005, [0]*10)

#Створення контексту Modbus-slave з використанням блоків даних
store = ModbusSlaveContext(ir=sensor_data_block)
context = ModbusServerContext(slaves=store, single=True)

#Запуск Modbus-server
StartTcpServer(context=context, identity=identity, address=("192.168.[redacted]6", 502))
```

Рисунок 3.4 – Функція запису даних

Комунікація відбувається по стандартному порту Modbus 502.

Master приймає та записує дані:

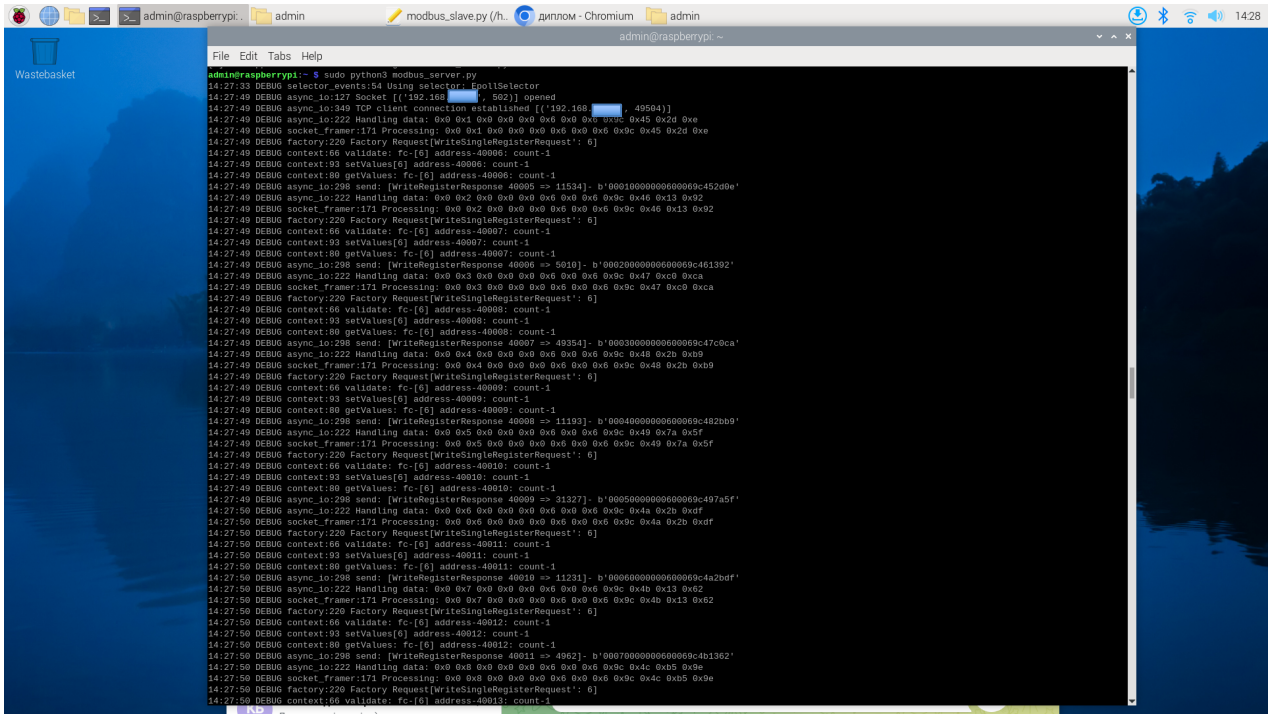

Рисунок 3.5 – Отримання даних сервером

За допомогою Wireshark можемо перехопити та переглянути структуру емульованого Modbus протоколу:

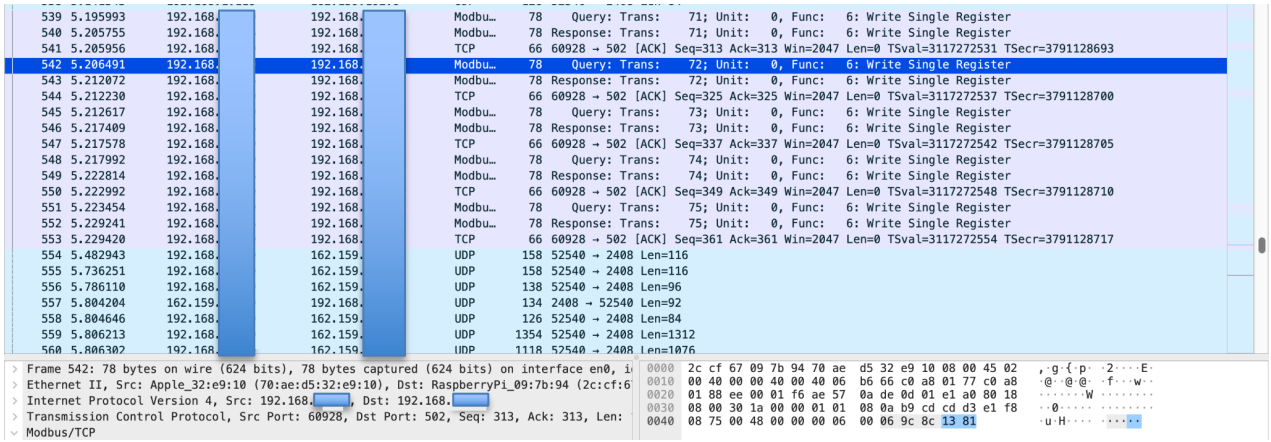

Рисунок 3.6 – Перехоплення Modbus

3.3 Security Monitoring Server як засіб комплексного моніторингу IT інфраструктури підприємства

Важливим етапом проектування мережі є вибір оптимального та

надійного центру моніторингу, який повинен централізовано збирати різноманітні показники та дані, що стосуються кібербезпеки, з усіх рівнів інфраструктури. Дані показники можуть надходити від різних джерел, таких як системні журнали, мережеві пристрої, датчики, контролери, прикладні програми тощо. Основні задачі Security Monitoring Server включають агрегування, аналіз, візуалізацію цих даних, надання операторам цілісного уявлення про стан безпеки інфраструктури та допомогу у своєчасному виявленні та реагуванні на потенційні загрози.

Оскільки ми вже визначились із тим, що наш центр буде в хмарному середовищі, для вирішення вищенаведених задач було обрано платформу з вихідним кодом ThingsBoard. Дане рішення надає операторам систем різноманітні інструменти для збору, візуалізації та аналізу даних, отриманих від різних пристроїв і датчиків.

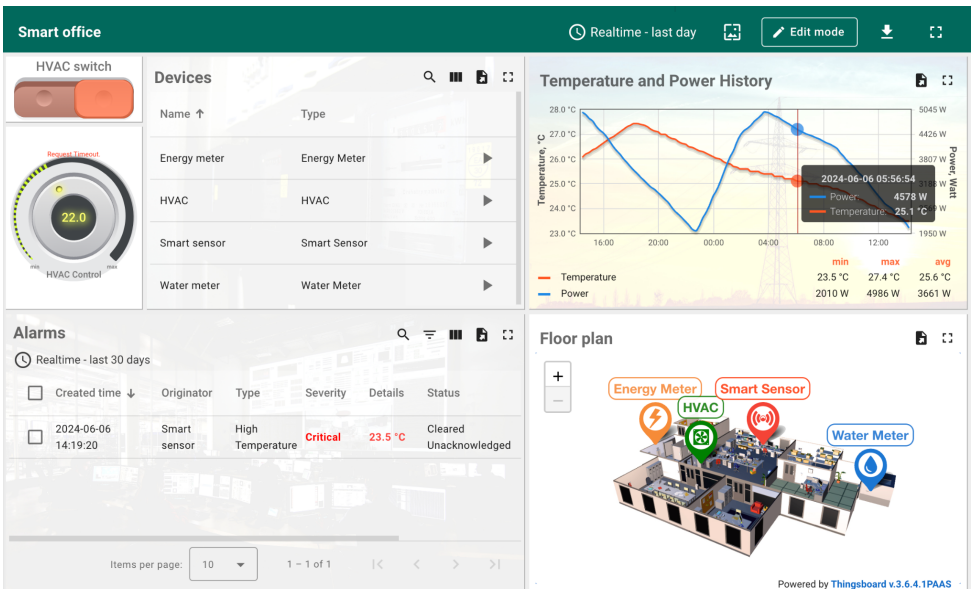

Рисунок 3.7 – Вигляд шаблону дашборду Smart Office в Thingsboard

Основні можливості ThingsBoard включають:

1. Підключення різноманітних пристроїв та датчиків за допомогою різних протоколів зв'язку - MQTT, CoAP, HTTP/HTTPS.
2. Візуалізацію даних у вигляді карт, графіків, дашбордів, віджетів тощо.
3. Обробку та аналіз даних в реальному часі.

4. Створення правил для автоматизації, обробки вхідних, алертів.
5. Управління та моніторинг пристроїв та активів системи.
6. Забезпечення надійної безпеки даних та доступу.

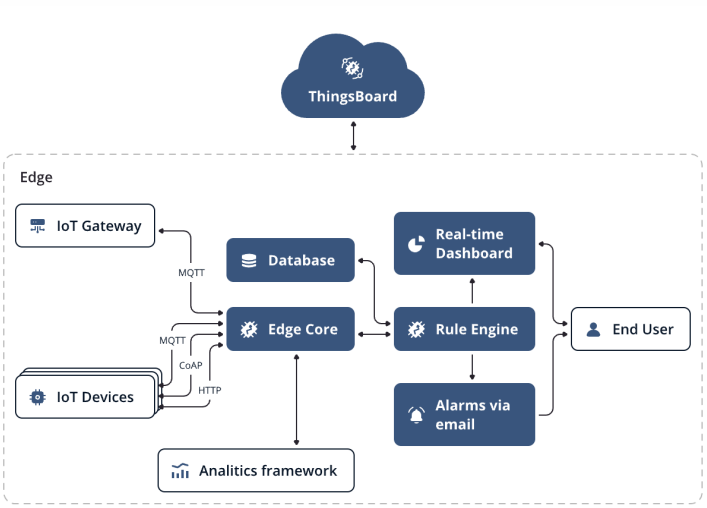

Рисунок 3.8 – Схема налаштування з документації Thingsboard [8]

Встановимо екземпляр Thingsboard для передачі даних на хмарний сервер за допомогою Docker контейнера. Встановивши десктопну версію, налаштуємо конфіги:

```
anastasiia.zhyhun@[redacted]-MAC-2 ~ % cd my_project
anastasiia.zhyhun@[redacted]-MAC-2 my_project % nano docker-compose.yml
anastasiia.zhyhun@[redacted]-MAC-2 my_project % nano docker-compose.yml
```

Рисунок 3.9 – Редагування конфігураційного файлу

Прописуємо дані для з’єднання з хмарою:

```
 UW PICO 5.09                                File: docker-compose.yml

version: '3.8'
services:
  mytbedge:
    restart: always
    image: "thingsboard/tb-edge-pe:latest"
    ports:
      - "8080:8080"
      - "1883:1883"
      - "5683-5688:5683-5688/udp"
    environment:
      SPRING_DATASOURCE_URL: jdbc:postgresql://postgres:5432/tb-edge
      EDGE_LICENSE_INSTANCE_DATA_FILE: /data/instance-edge-license.data
      CLOUD_ROUTING_KEY: [redacted]
      CLOUD_ROUTING_SECRET: [redacted]
      CLOUD_RPC_HOST: thingsboard.cloud
      CLOUD_RPC_PORT: 7070
      CLOUD_RPC_SSL_ENABLED: true
    volumes:
      - tb-edge-data:/data
      - tb-edge-logs:/var/log/tb-edge

  postgres:
    restart: always
    image: "postgres:15"
    ports:
      - "5432"
    environment:
      POSTGRES_DB: tb-edge
      POSTGRES_PASSWORD: postgres
    volumes:
      - tb-edge-postgres-data:/var/lib/postgresql/data

volumes:
  tb-edge-data:
    external: true
  tb-edge-logs:
    external: true
```

Рисунок 3.10 – Дані для з’єднання

Запускаємо:

```
anastasiia.zhyhun@[redacted]-MAC-2 my_project % docker compose up -d
WARN[0000] /Users/anastasiia.zhyhun/my_project/docker-compose.yml: `version` is obsolete
[+] Running 2/0
 ✔ Container my_project-mytbedge-1  Running
 ✔ Container my_project-postgres-1  Running
```

Рисунок 3.11 – Запуск контейнера

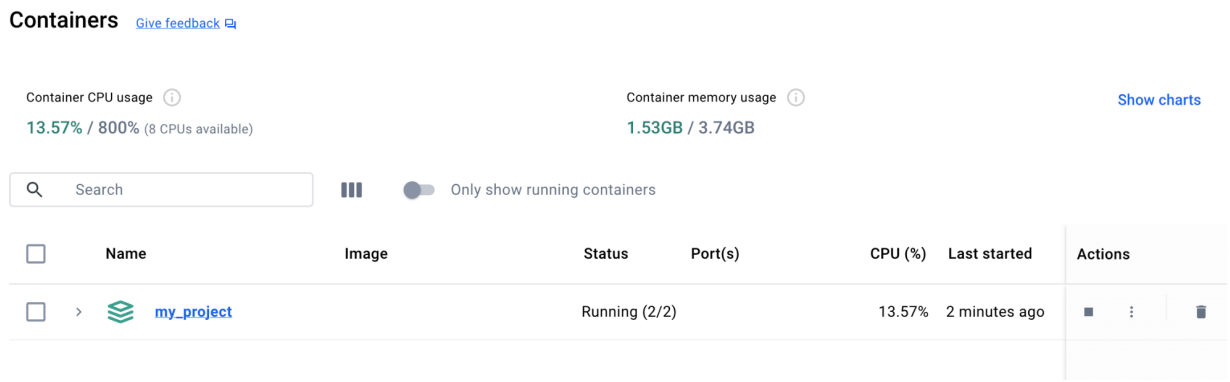

Рисунок 3.12 – Запущений контейнер

За http://localhost:8080/ отримуємо доступ до локального управління. Можемо відразу підключити пристрої:

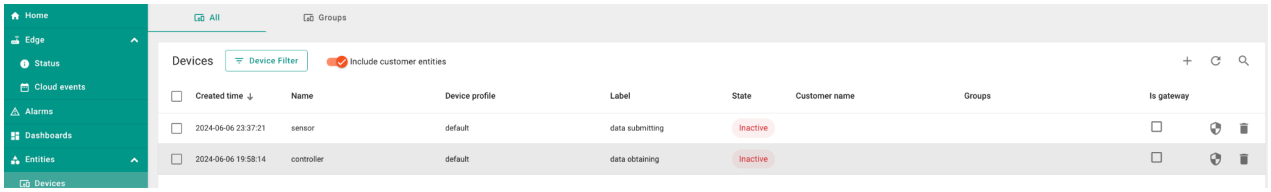

Рисунок 3.13 – Підключені пристрої

Документація надає нам тестовий зразок скрипта, за яким можна перевірити передачу даних на хмарну платформу з використанням MQTT з'єднання:

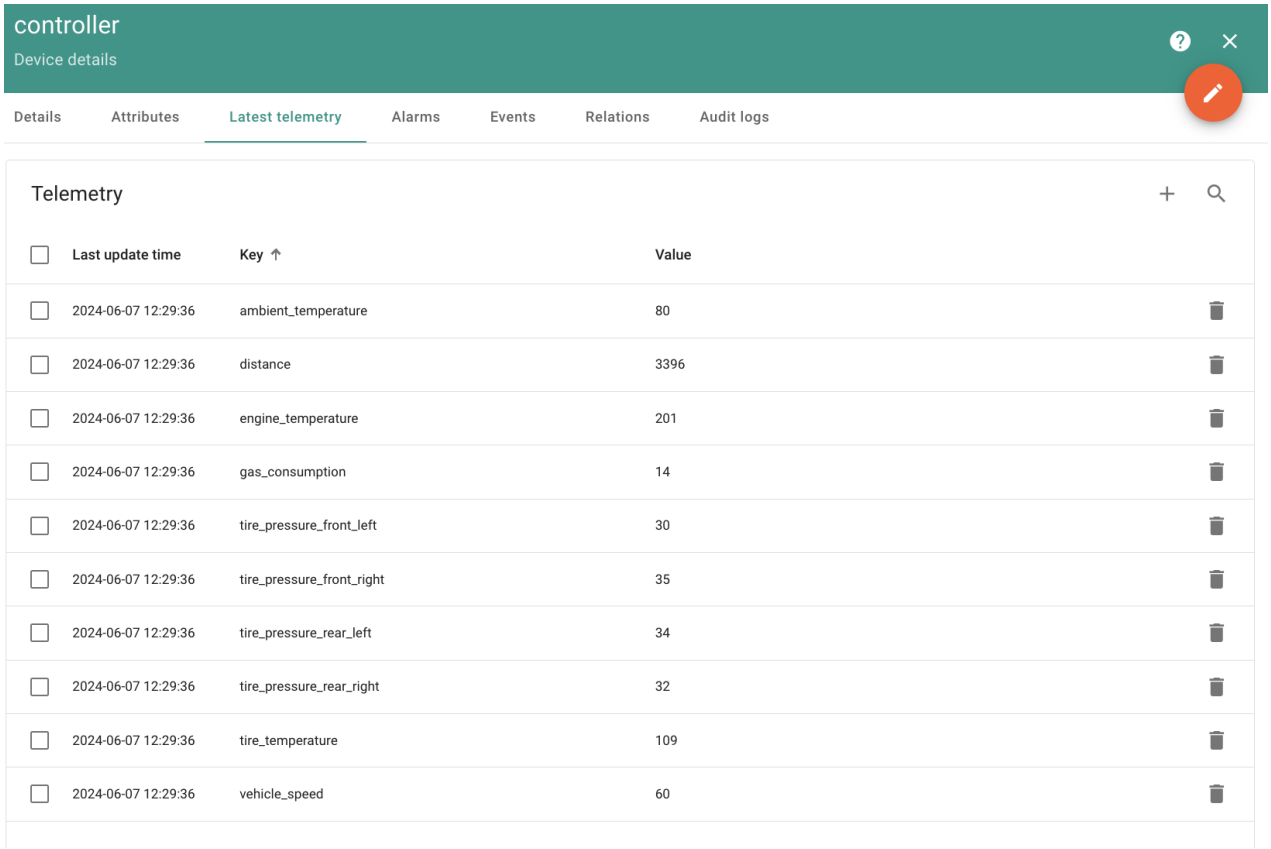

Рисунок 3.14 – Тестові телеметричні дані

Thingsboard надає можливість самотужки складати правила спостереження даних та подій, тому ми оновимо «Edge Root Rule Chain» - ланцюжок правил, за якими зберігатимуться необхідні нам показники.

У цьому ланцюжку ми додаємо вузол правила, який перетворює вхідні повідомлення та надсилає повідомлення в хмару.

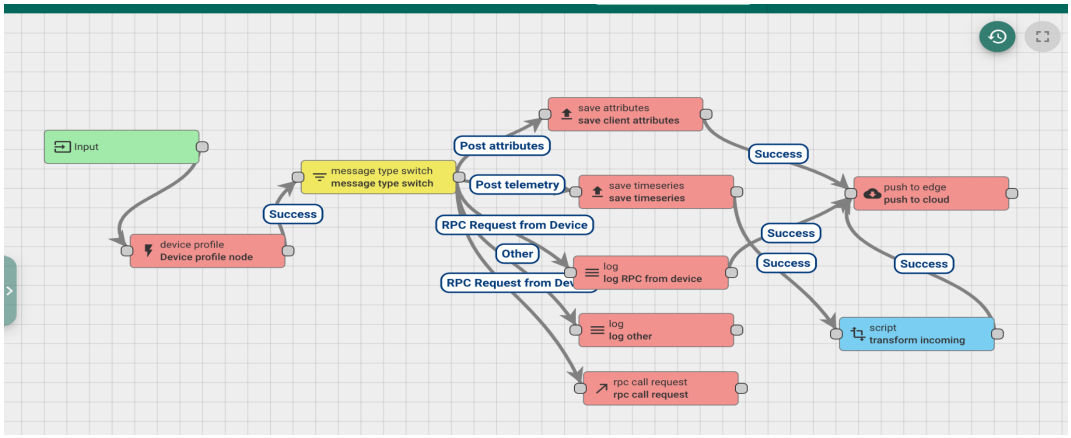

Рисунок 3.15 – Налаштування ланцюга правил

Модифікуємо скрипт із документації для передачі певних показників кібербезпеки, що будуть корисними для виявлення спроб реалізації атак на IT інфраструктуру підприємства. Для цього використаємо бібліотеку scapy, а саме її функцію sniff для відстеження кількості вхідних пакетів на пристрій в режимі реального часу. Scapy є зручним та потужним інструментом для роботи з мережевими пакетами та проведення досліджень у сфері інформаційної безпеки.

Також використаємо можливості psutil - бібліотеки, що надає інформацію про запущені процеси та використання системи (ЦП, пам’ять, диски, мережа, датчики). Такі функції дуже корисні в ході моніторингу системи, профілювання, обмеження ресурсів процесу та керування запущеними процесами.

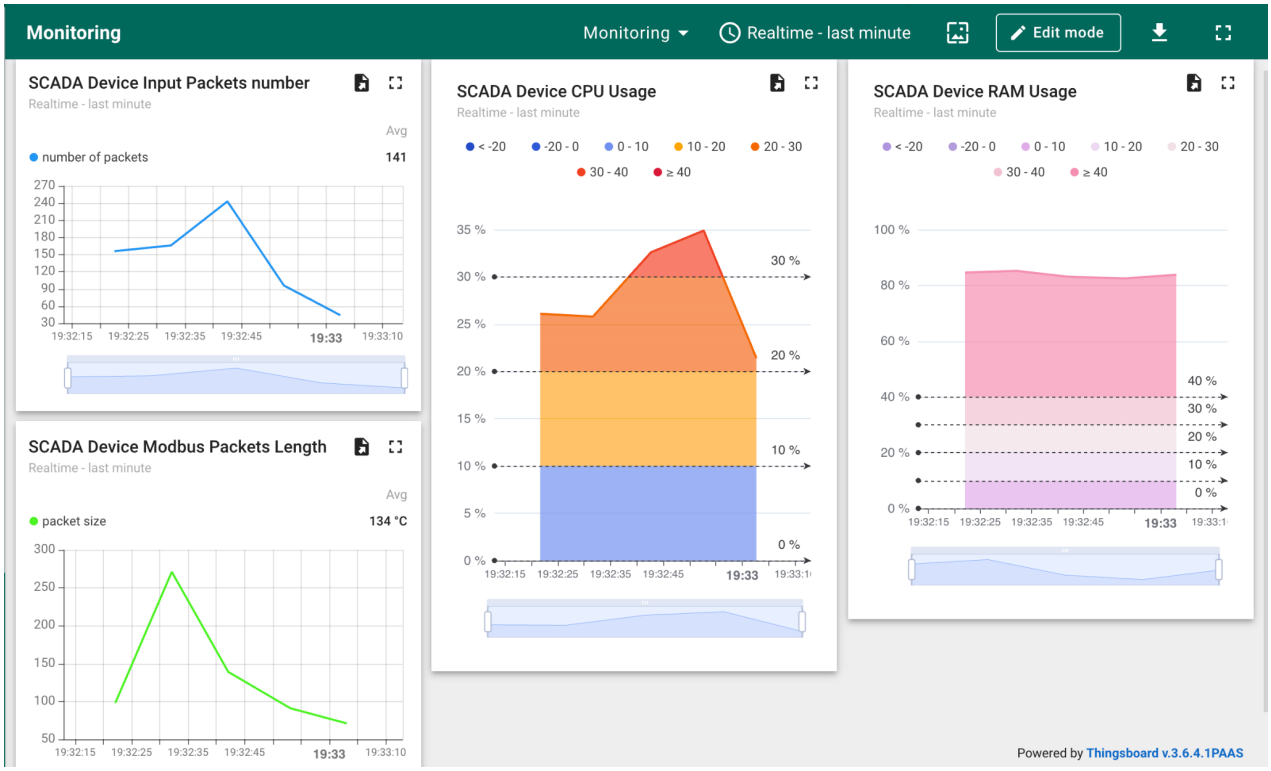

Рисунок 3.16 – Налаштування дашборду

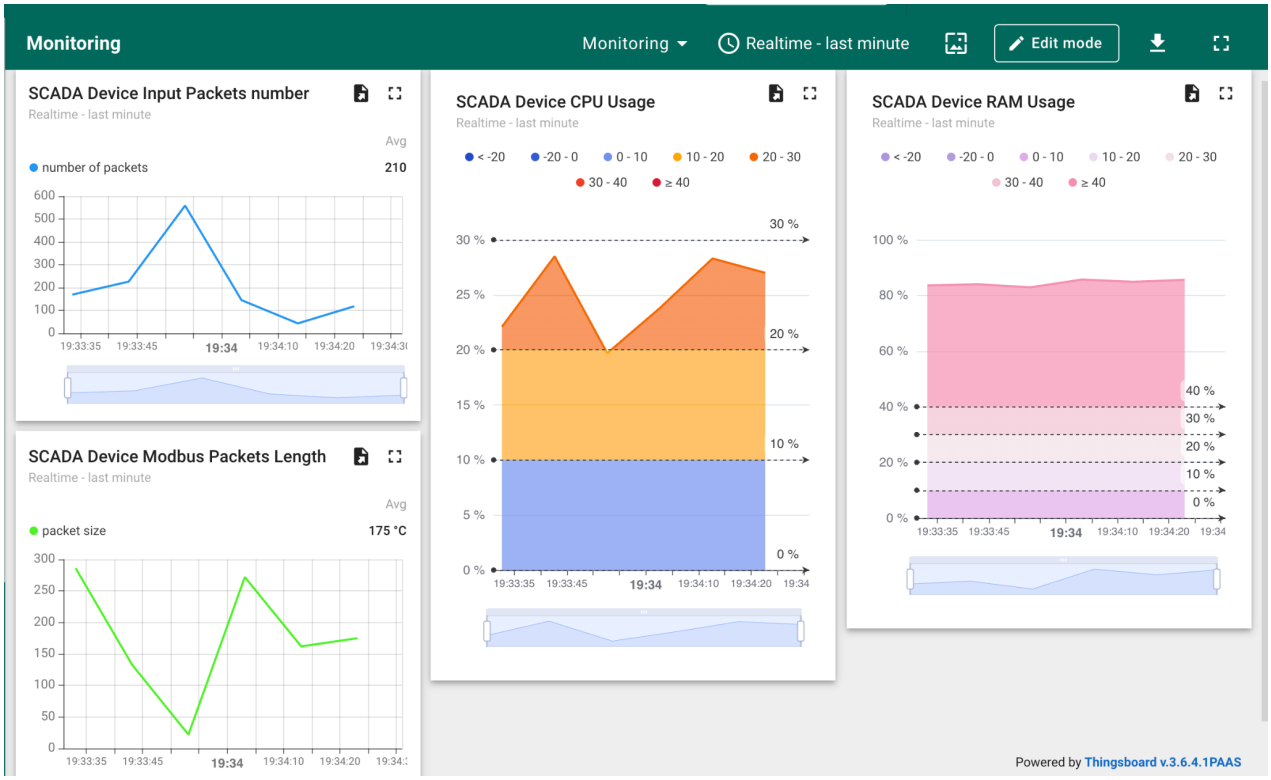

Рисунок 3.17 – Налаштований дашборд

Висновки до розділу 3

У даному розділі було обгрунтовано вибір хмарної платформи Thingsboard для виконання функцій Security Monitoring Server, що повинен проводити комплексний моніторинг усієї IT інфраструктури підприємства та забезпечувати надійний захист системи.

Також було продемонстровано можливості даного інструменту, зокрема підключення пристроїв, налаштування ланцюжків правил та передача телеметричних в хмарне середовище з низькорівневих пристроїв SCADA. Додатково реалізовано скрипт передачі показників безпеки на хмарний сервер моніторингу, на основі яких можна здійснювати аналіз стану та подій мережі.

ВИСНОВКИ

У даній роботі було досліджено можливості моніторингу кібератак на системи SCADA у контексті IT інфраструктури об’єктів критичної інфраструктури індустріального сектору.

Описана модель загроз та методичні вказівки по попередженню спроб здійснення атак є важливими при розробці ефективних методів превентивного виявлення намагань несанкціонованого втручання та покращення загальної безпеки системи.

Спроектована в результаті архітектура мережі IT інфраструктури об’єкта критичної інфраструктури є дуже корисною у створенні надійної та безпечної системи, оскільки дозволяє мінімізувати ризики втрати, викрадення або спотворення даних. Вона також включає в себе змогу збирати показники з нижчих рівнів, що надаватиме більш комплексну картину про ситуацію та повне розуміння активності системи.

Розташування центру моніторингу в хмарному середовищі дозволяє проводити централізований моніторинг подій навіть для кількох підприємств зі своєчасним реагуванням на інциденти безпеки. Зовнішнє спостереження за ключовими активами та інфраструктурою надає ширшу видимість подій, мережевої активності, кращу масштабованість, стійкість, можливість централізованого аналізу та прийняття рішень на основі подій всієї системи.

Подальше дослідження SCADA систем в контексті IT інфраструктури критичних бізнес-процесів дозволить укріпити захист конфіденційної інформації, запобігти небажаному втручанню зловмисників в роботу підприємства, реалізації їх мотивів, значним фінансовим та репутаційним втратам, забезпечити безперервність діяльності та стійкість бізнесу, захистити тисячі споживачів таких підприємств, їх здоров’я та навіть життя.

Отже, зважаючи на все вищеперелічене, результати дослідження та

розробки в ході даної роботи можуть бути використані для підвищення рівня безпеки та надійності систем моніторингу об'єктів критичної інфраструктури індустріального сектору. Це особливо важливо, враховуючи потенційні наслідки кібератак на такі об'єкти, як енергетичні системи, водопостачання, транспорт тощо.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions [Електронний ресурс] – 2022 – Режим доступу до ресурсу: https://www.researchgate.net/publication/363656704_Cyber_Threats_to_Smart_Grids_Review_Taxonomy_Potential_Solutions_and_Future_Directions

2. Cybersecurity Analysis of Load Frequency Control in Power Systems: a survey [Електронний ресурс] – 2021 – Режим доступу до ресурсу: https://digitalcommons.sacredheart.edu/computersci_fac/162/

3. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies [Електронний ресурс] – 2023 – Access Mode: https://www.mdpi.com/1424-8220/23/21/8840

4. Detecting and classifying man-in-the-middle attacks in the private area network of smart grids [Електронний ресурс] – 2023 – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S2352467723001753?via%3Dihub

5. NIAC. 2010. A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council. October 19, 2010. – Режим доступу до ресурсу: https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

6. Cyber Resilience Framework Self-Assessment Tool User Guide - Режим доступу до ресурсу: https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-framework/documents/cyber-resilience-framework-self-assessment-tool-user-guide-october-2019/cyber-resilience-framework-self-assessment-tool-user-guide-october-2019/govscot%3Adocument/Cyber%2B-%2BPublic%2BSector%2BAction%2BPlan%2B-%2BSelf-Assessment%2BTool%2B-%2BUser%2BGuide.pdf

7. Security Monitoring and Network Management for the Power Control Network [Електронний ресурс] – 2020 – Режим доступу до ресурсу: https://www.researchgate.net/profile/Sugwon-Hong/publication/347897788_Security_Monitoring_and_Network_Management_for_the_Power_Control_Network/links/6098b924458515d3150bf9b0/Security-Monitoring-and-Network-Management-for-the-Power-Control-Network.pdf

8. What is ThingsBoard PE Edge? [Електронний ресурс] - Режим доступу до ресурсу: https://thingsboard.io/docs/pe/edge/getting-started-guides/what-is-edge/

9. NIST Framework for Improving Critical Infrastructure Security [Електронний ресурс] - Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

10. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics [Електронний ресурс] - Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9066892

ДОДАТОК А ЕМУЛЯЦІЯ MODBUS КОМУНІКАЦІЇ МІЖ НИЗЬКОРІВНЕВИМИ ПРИСТРОЯМИ (MODBUS MASTER)

```
from pymodbus.datastore import ModbusSequentialDataBlock
from pymodbus.datastore import ModbusSlaveContext, ModbusServerContext
from pymodbus.server.sync import StartTcpServer
import logging

logging.basicConfig()
log = logging.getLogger()
log.setLevel(logging.DEBUG)

def run_modbus_server():
    #Створення блоків даних для зберігання значень датчиків
    sensor_data_block = ModbusSequentialDataBlock(40005, [0]*10)

    #Створення контексту Modbus slave із заданими блоками даних
    store = ModbusSlaveContext(ir=sensor_data_block)
    context = ModbusServerContext(slaves=store, single=True)

    #Запуск Modbus сервера
    StartTcpServer(context=context, address=("*****", 502)) #ip-адреса modbus-master

if __name__ == "__main__":
    run_modbus_server()
```

ДОДАТОК Б ЕМУЛЯЦІЯ MODBUS КОМУНІКАЦІЇ МІЖ НИЗЬКОРІВНЕВИМИ ПРИСТРОЯМИ (MODBUS SLAVE)

```
import random
from pymodbus.client import ModbusTcpClient

# Налаштування з'єднання Modbus
server_ip = "raspberry"  # IP-адреса modbus-master
server_port = 502

def generate_power_plant_data():
    # Генерація даних датчиків для електростанції
    generator_voltage = random.uniform(110, 120)
    generator_frequency = random.uniform(49.5, 50.5)
    boiler_temperature = random.uniform(450, 500)
    boiler_pressure = random.uniform(100, 120)
    turbine_speed = random.uniform(3000, 3600)
    return generator_voltage, generator_frequency, boiler_temperature,
boiler_pressure, turbine_speed
def write_power_plant_data(client):
        generator_voltage, generator_frequency, boiler_temperature, boiler_pressure,
turbine_speed = generate_power_plant_data()
        i = 0

        #Запис даних
        client.write_register(40005 + i, int(generator_voltage * 10))
        client.write_register(40006 + i, int(generator_frequency * 100))
        client.write_register(40007 + i, int(boiler_temperature))
       client.write_register(40008 + i, int(boiler_pressure))
        client.write_register(40009 + i, int(turbine_speed))
        i += 5
        print(f"Wrote power plant data: Generator Voltage={generator_voltage} V, "
            f"Generator Frequency={generator_frequency} Hz, "
            f"Boiler Temperature={boiler_temperature} °C, "
            f"Boiler Pressure={boiler_pressure} bar, "
            f"Turbine Speed={turbine_speed} RPM")
            time.sleep(1)
    print("Data transmission completed.")
```

```
def main():
    #Створення клієнта Modbus
    client = ModbusTcpClient(server_ip, port=server_port)
    #Підключення до Modbus сервера
    client.connect()
    #Запуск циклу запису даних
    write_power_plant_data(client)
    # Закриття з'єднання Modbus
    client.close()
if name == "__main__":
    main()
```

ДОДАТОК В ПЕРЕДАЧА ПОКАЗНИКІВ БЕЗПЕКИ НА ХМАРНУ ПЛАТФОРМУ МОНІТОРИНГУ

```
import paho.mqtt.client as mqtt
import json
import time
from scapy.all import sniff
import psutil
import random

ACCESS_TOKEN = '*****'  # device access token
THINGSBOARD_EDGE_HOST = '*****'  # ThingsBoard Edge server installation IP address or hostname, e.g. 'localhost'
THINGSBOARD_EDGE_MQTT_PORT = *****  # ThingsBoard Edge MQTT port, e.g. 11883 or 1883

packet_count = 0

def on_connect(client, userdata, rc, *extra_params):
    print('Connected to ThingsBoard with result code ' + str(rc))
    client.subscribe('v1/devices/me/rpc/request/+')

def count_packet(packet):
    global packet_count
    packet_count += 1

def get_telemetry():
    global packet_count
    packet_count = 0
    sniff(prn=count_packet, timeout=5)
```

```
    traffic_data = {'traffic_volume': packet_count,
                    'cpu_usage': psutil.cpu_percent(),
                    'ram_usage': psutil.virtual_memory().percent}
    return json.dumps(traffic_data)

client = mqtt.Client()
client.on_connect = on_connect
client.username_pw_set(ACCESS_TOKEN)
client.connect(THINGSBOARD_EDGE_HOST,
THINGSBOARD_EDGE_MQTT_PORT, 60)

try:
    while True:
        data = get_telemetry()
        print(data)
        client.publish('v1/devices/me/telemetry', data, 1)
        time.sleep(5)
        client.loop()
except KeyboardInterrupt:
    client.loop_stop()
    print("Exited!")
```