Додаток А

«ЗАТВЕРДЖУЮ»
_____ Ім’я, ПРІЗВИЩЕ
(директора ННІ)
«___» _____ 20__ р.

Директору
Навчально-наукового інституту
Віталій САВЧЕНКО_____
_____ Ім’я, ПРІЗВИЩЕ

Здобувача(ки) Матвієнко О.В._____
6 курсу, групи _____
Домашня адреса: 03186 м. Київ,_____
Чоколівський бульвар, 20 кв 69_____
Телефон +38 099 541 39 51_____

ЗАЯВА

Прошу затвердити тему магістерської роботи: **ТЕХНОЛОГІЯ ЗАХИСТУ ПРОМИСЛОВИХ IoT ІЗ ВИКОРИСТАННЯМ CISCO CYBER VISION**
(повна назва теми)
Прошу призначити керівником _____Борсуковського Юрія
_____
(ПІБ, посада, місце роботи)

Підпис керівника _____

(Керівник письмово звітує першого числа кожного місяця про стан написання роботи)

Зобов’язуюсь перевірити магістерську роботу на плагіат. Коефіцієнт подібності не вище 35%.

Даю згоду на розміщення магістерської роботи в електронному репозитарії на сайті Університету.

Завідувач кафедрою _____
(ПІБ, підпис)

Про себе повідомляю

Прізвище та ім’я англійською мовою
Matviienko Oleksii_____

Паспортні дані (серія, номер, ким виданий)
005994722, 8017_____

Місце роботи
_____

Посада _____

_____
(особистий підпис здобувача)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ПРОМИСЛОВИХ IoT ІЗ ВИКОРИТАННЯМ CISCO CYBER VISION»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
Матвієнко Олексій
(ПРІЗВИЩЕ, Ім'я)

Керівник: Борсуковський Юрій
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: Туровський Олександр
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Матвієнко Олексію Володимировичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія захисту промислових IoT із використанням Cisco Cyber Vision»
керівник кваліфікаційної роботи Борсуковський Юрій, к.т.н., доцент
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__» _____ 2023р. №___.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
промисловий Інтернет речей
технологія захисту промислових IoT із використанням Cisco Cyber Vision
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз вразливостей пристроїв та мереж IoT від зловмисних атак та загроз.
2. Способи захисту систем і пристроїв промислових інтернет речей
3. Розроблення варіанта технології виявлення і усунення загроз за допомогою Cisco Cyber Vision

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми загроз безпеки, для промислових IoT	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз векторів атак та загроз безпеки для примислових IoT	27.10. 2023р.	
4.	Способи захисту систем і пристроїв, вимоги до безпеки, можливості і напрямки вирішення	03.11.2023 р.	
5.	Розроблення варіанта технології захисту промислових IoT за допомогою Cisco Cyber Vision	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

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

Керівник
кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

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

Направляється здобувач Матвієнко О.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту промислових IoT за допомогою Cisco Cyber Vision».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***МАТВІЄНКО Олексій*** обрав тему роботи, метою якої було дослідити зміст технології захисту промислових IoT. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***МАТВІЄНКО Олексій*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***МАТВІЄНКА Олексія*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***МАТВІЄНКА Олексія*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Матвієнко Олексія
на тему: «Технологія захисту промислових IoT за допомогою Cisco Cyber Vision».

Актуальність:

Промисловий IoT розвивається дуже швидко, тому головною метою є його безпека. Питання безпеки є надзвичайно важливим через зростаючу вразливість до атак і витоків даних. Промислові процеси не можна зупинити, щоб встановити патч. Тому потрібен такий захист безпеки, який зможе працювати з безперебійним процесом. Саме таким захистом для промислових IoT є Cisco Cyber Vision. Завдяки йому можна забезпечити повну видимість інфраструктури ІКС, включаючи моніторинг даних процесів в режимі реального часу і розвідку загроз, що дозволить створювати безпечну інфраструктуру. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту промислових IoT.
2. Досліджено методи та засоби боротьби з кібератаками, вразливості пристроїв та мереж IoT.
3. Запропоновано варіант технології захисту за допомогою Cisco Cyber Vision.
4. Текст викладено достатньо чітко, послідовно. Сформульовано змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально зупинитися на порівнянні способів захисту ситем і пристроїв промислови IoT .
2. Запропонований варіант технології захисту промислового IoT краще було показати на прикладі конкретного підприємства.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре**», а здобувач **МАТВІЄНКО Олексій** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ Олександр Туровський
д.т.н., професор *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина бакалаврської (магістерської) кваліфікаційної роботи:67 стор., 7 рис., 4 табл., 36 джерел.

Об'єкт дослідження – процес захисту промислових мереж і пристроїів від зловмисних атак.

Предмет дослідження – технологія захисту промислових IoT із використанням Cisco Cyber Vision.

Мета роботи – провести аналіз вразливості пристроїв і мереж промислових IoT, розробити варіанти технології захисту промислових IoT із використанням Cisco Cyber Vision, та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за цією темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівння, моделювання процесу захисту промислової мережі за допомогою Cisco Cyber Vision.

В роботі проведено аналіз проблеми захисту промислових пристроїв та мереж IoT від зловмисних атак та загроз безпеці. Проаналізовано вже існуючі техгології захисту промислових мереж.

Досліджено методи та засоби контролю захисту промислових мереж, щоб вони були менш вразливими до кібератак.

Запропоновано варіант технології захисту промислових IoT із використанням Cisco Cyber Vision. Визначено призначення, основні функції та принцип роботи даної технології.

На основі проведених досліджень, в роботі розроблено варіант технології захисту промислової мережі за допомогою Cisco Cyber Vision, щоб забезпечити повну видимість промислових мереж, а також забезпечити цілісність процесів, для побудови безпечної інфраструктури.

Галузь використання – кібербезпека промислової мережі.

ПРОМИСЛОВИЙ ІНТЕРНЕТ РЕЧЕЙ, ПРОГРАМНО-ВИЗНАЧЕНА МЕРЕЖА, ВИЯВЛЕННЯ ВТОРГНЕНЬ, ІНТЕРНЕТ РЕЧЕЙ, ПЕРЕФЕРІЙНЕ ОБЧИСЛЕННЯ, ІНДУСТРІЯ 4.0, КІБЕРФІЗИЧНІ СИСТЕМИ, КІБЕРБЕЗПЕКА, ОПЕРАЦІЙНІ ТЕХНОЛГІЇ

ABSTRACT

Text part of the master's qualification work:
67 pages, 7 pictures, 4 table, 36 sources.

Object of research - process of protecting industrial networks and devices from malicious attacks.

Subject of research - technology for protecting industrial IoT using Cisco Cyber Vision.

Purpose of research - is to analyze the vulnerability of industrial IoT devices and networks, develop options for industrial IoT security technology using Cisco Cyber Vision, and recommendations for the use of this technology.

Research methods: studying the literature on this topic, analyzing operational documentation, international standards and comparing them, modeling the process of protecting an industrial network using Cisco Cyber Vision.

The paper analyzes the problem of protecting industrial devices and IoT networks from malicious attacks and security threats. Existing industrial network security technologies are analyzed.

Methods and controls for protecting industrial networks to make them less vulnerable to cyberattacks are investigated.

A variant of industrial IoT protection technology using Cisco Cyber Vision is proposed. The purpose, main functions and principle of operation of this technology are determined.

Based on the research, the paper develops a variant of industrial network protection technology using Cisco Cyber Vision to provide full visibility of industrial networks, as well as to ensure the integrity of processes to build a secure infrastructure.

The field of application is the cybersecurity of an industrial network.

INDUSTRIAL INTERNET OF THINGS, SOFTWARE-DEFINED NETWORK, INTRUSION DETECTION, INTERNET OF THINGS, EDGE COMPUTING, INDUSTRY 4.0, CYBER-PHYSICAL SYSTEMS, CYBERSECURITY, OPERATIONAL TECHNOLOGY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LPWAN - Low-Power Wide-Area Network

CRM - Customer Relationship Management

CPS - Cost-per-Sale

MCC - Merchant Category Code

AI - Artificial intelligence

RFID - Radio Frequency IDentification

RPL- Rocket Pool

OLE - Object Linking and Embedding

ICS - International Code of Signals

SSI - Server Side Includes

PLC - Programmable logic controller

RTU - Remote Terminal Unit

IACS- International Association of Classification Societies

ВСТУП

Актуальність дослідження. Промисловий Інтернет речей - це інноваційна спроба створити розумне виробниче середовище, використовуючи переваги Інтернету речей в управлінні промисловими процесами. IIoT розвивається дуже швидко, але існують різні виклики, які можуть вплинути на його майбутнє зростання. Це і інтеграція даних, і нестача кваліфікованих кадрів у цій галузі, а головне - безпека.

Питання безпеки є надзвичайно важливими через зростаючу вразливість до атак та витоків даних. У контексті промислового інтернету речей дані вважатимуться критично важливими і конфіденційними, оскільки вони охоплюватимуть різні аспекти промислової діяльності, в тому числі дуже конфіденційну інформацію про продукти, бізнес-стратегії та компанії. Перехід до більш вразливих і відкритих мереж і можливостей обміну даними в Інтернеті речей підвищує ризики в промислових галузях.

Витік конфіденційних даних може призвести до значних збитків і втрат. Таким чином, безпека стала серйозною проблемою в промислових системах Інтернету речей через їхню чутливу природу. Надійність, безпека та доступність промислових систем IoT ставляться під загрозу через відсутність параметрів безпеки в протоколах зв'язку.

Основною метою є захист промислових пристроїв та мереж IoT. Захист промислових операцій є дуже специфічним завданням, яке неможливо вирішити за допомогою традиційних інструментів IT-безпеки. Промислові процеси не можна зупинити, щоб встановити патч. Збої можуть мати руйнівний вплив на людські життя та навколишнє середовище. Ще більше ускладнює ситуацію те, що атаки буває важко виявити, оскільки вони часто виконуються на замовлення і виглядають як легітимні технолочні інструкції. Тому тема кваліфікаційної роботи є актуальною.

Об'єкт дослідження – процес захисту промислових IoT від кібератак.

Предмет дослідження – технологія захисту промислових IoT із використанням Cisco Cyber Vision.

Мета роботи – розробити варіант захисту промислових організацій від загроз, щоб вони могли контролювати ризики кібербезпеки, за допомогою Cisco Cyber Vision та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз питання щодо векторів атак та загроз безпеки для промислових IoT;
- проаналізувати способи захисту систем і пристроїв, можливості і напрямки вирішення проблеми безпеки;
- розробити варіант для промислових організацій, щоб забезпечити безперерівність, стійкість і безпеку їхньої діяльності за допомогою Cisco Cyber Vision та рекомендації щодо застосування цієї технолгії.

Методи дослідження - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, їх порівняння, моделювання технології захисту промислового IoT із використанням Cisco Cyber Vision.

Практичне завдання одержаних результатів полягає в розробці технології захисту промислових IoT за допомогою Cisco Cyber Vision та рекомендації щодо застосування цієї технології для створення безпечної інфрастрктури, забезпечення безперервності процесу, моніторінгу даних в режимі реального часу.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки»

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ IoT

1.1. Призначення, структура, функції промислового IoT

Інтернет речей - це система мільярдів взаємопов'язаних обчислювальних пристроїв, цифрових і механічних машин, людей або об'єктів, які підключені до Інтернету і можуть передавати і обмінюватися даними через Інтернет. Основні рівні IoT виступають в якості основи систем IoT для розробки ефективної багаторівневої архітектури IoT. Ці рівні розглядаються нижче і узагальнені в Таблиці 1.1.

Таблиця 1.1.

Представлення IoT за допомогою семирівневої архітектури

Рівень	Надана послуга
Рівень сприйняття	Приводи, датчики, пристрої, контролери, машини
Транспортний рівень	Протоколи, комунікації, WiFi, мережі, Bluetooth
Рівень обробки	Накопичення даних
Прикладний рівень	Інтелектуальні додатки, програмне забезпечення для прийняття рішень, послуги моніторингу та управління пристроями, рішення на основі штучного інтелекту та машинного навчання
Граничний рівень	Попередня обробка на локальних серверах, шлюзах та інших пограничних вузлах мережі

Продовження таблиці 1.1.

Представлення IoT за допомогою семирівневої архітектури

Рівень	Надана послуга
Бізнес рівень	Бізнес-моделі, CRM, програми бізнес-аналітики
Рівень безпеки	Безпека пристроїв, безпека з'єднань, хмарна безпека

Розглянемо кожний рівень окремо.

Рівень сприйняття: це фізичний рівень, який складається з датчиків, приводів, пристроїв і машин. Датчики, лічильники і зонди збирають інформацію про промислове середовище IoT. Приводи, що використовуються в лазерах, контролерах двигунів, перетворюють електричні сигнали від систем IoT у фізичні дії.

Транспортний рівень: цей рівень транспортує дані датчиків між рівнем сприйняття і рівнем обробки за допомогою таких технологій, як WiFi, LPWAN, Ethernet і ZigBee.

Рівень обробки: відповідає за збір інформації з транспортного рівня та її обробку [1].

Прикладний рівень: відповідає за безпосередню взаємодію з кінцевими користувачами. Він складається з різних додатків, таких як мобільні додатки, програмне забезпечення для моніторингу пристроїв, сервіси бізнес-аналітики тощо. Всі додатки мають свої протоколи прикладного рівня.

Граничний рівень: виконує попередню обробку даних на периферії. Це відбувається на локальних серверах, шлюзах та інших периферійних вузлах мережі.

Бізнес-рівень: рівень, на якому підприємства на основі зібраних даних можуть приймати рішення.

Рівень безпеки: охоплює всі вищезгадані рівні IoT. Він включає в себе безпеку пристроїв, безпеку з'єднань і хмарну безпеку.

В основі Індустрії 4.0 лежать кіберфізичні системи, тобто інтелектуальні машини. Ці системи використовують сучасні системи управління з вбудованими програмними системами, які підключаються до Інтернету речей через інтернет-адреси. Таким чином, виробництво і продукти підключаються до мережі і можуть спілкуватися, що сприяє створенню цінності, оптимізації в реальному часі та новим способам виробництва. Метою є моніторинг процесів та активів у режимі реального часу, що дозволяє процесам приймати автономні рішення та задовольняти потреби клієнтів. Індустрія 4.0 характеризується наступним чином: забезпечує більшу автоматизацію в порівнянні з третьою промисловою революцією; перехід від централізованих систем управління промисловістю до систем, де інтелектуальні продукти визначають етапи виробництва; подолання розриву між цифровим і фізичним світом за допомогою кіберфізичних систем; замкнуті системи управління та моделі даних. Індустрія 4.0 - це "Зв'язок". Зв'язок уможливить інтелектуальне виробництво завдяки поширенню IIoT, хмарних технологій та великих даних. Розумні пристрої можуть збирати різні дані про місцезнаходження в приміщенні, зовнішнє положення, інформацію про стан, моделі використання клієнтів тощо. Вони можуть не лише збирати інформацію, але й обмінюватися нею з іншими користувачами. Це буде корисно для побудови ефективного виробничого процесу в промислових умовах, а також для допомоги в плановому профілактичному обслуговуванні обладнання. Інша перевага полягає у якнайшвидшому виявленні помилок на виробничому конвеєрі, оскільки це є важливим фактором зниження виробничих витрат і витрат на технічне обслуговування. Індустрія 4.0 також зосереджується на проблемах оптимізації в промисловості, використовуючи розумні пристрої для використання послуг на основі даних. Індустрія 4.0 використовуються для спільного виконання складних завдань, прийняття рішень на основі зібраних даних та віддаленого доступу до обладнання. Масштабне підключення речей та можливість збору/обміну даними робить безпеку основною вимогою до концепцій Індустрії 4.0.

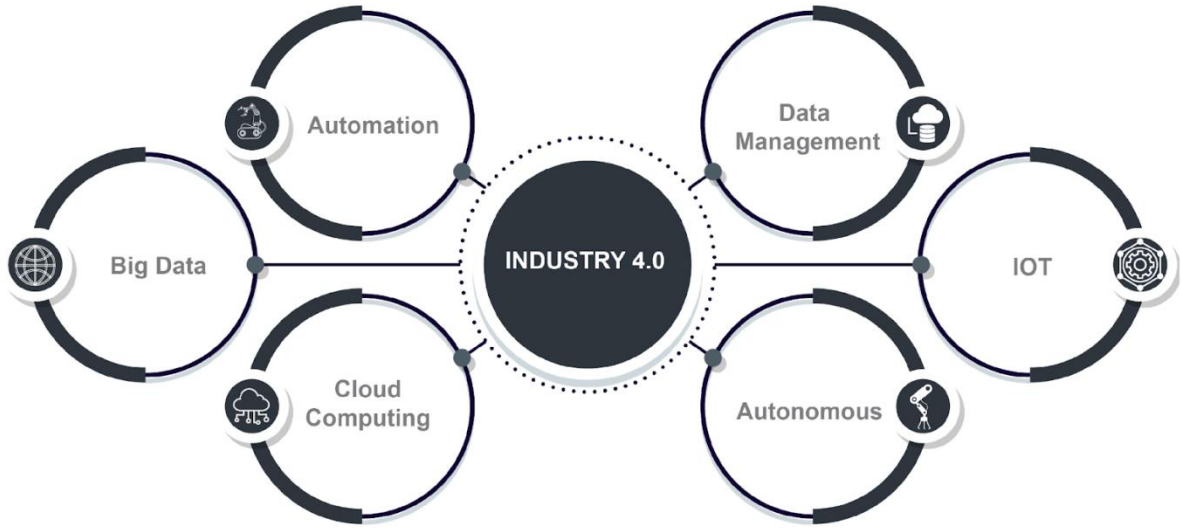

Рисунок 1.1.1. Індустрія 4.0 та нові технології для покращення промислового виробництва

Як показано на рисунку 1.1.1. Індустрія 4.0 - також відома як четверта промислова революція - є прикладом безпрецедентної промислової еволюції і доповнює різні нові технології і системи, такі як CPS, MCC, IoT, AI, CC, великі дані і туманні обчислення, з метою підвищення адекватності промисловості з точки зору підтримки гетерогенних даних, автоматизації, високої продуктивності та інтеграції знань [2,3]. Кількість вбудованих систем, що використовуються в промислових додатках, стрімко зросла завдяки доступності монтажу, можливостям і ціновій доступності датчиків, комунікаційних модулів і процесів [4]. Це викликало підвищений інтерес до використання IIoT в таких промислових сферах, як "розумні міста", транспорт, охорона здоров'я, мікромережі та "розумні" заводи, що призвело до появи Індустрії 4.0 на основі CPS.

Промисловий IoT відноситься до використання IoT в промисловому секторі та бізнес-середовищі. Промисловий IoT - це перетин операційних технологій (OT) та інформаційних технологій (IT). Машина генерує завчасне повідомлення про наближення поломки; хмарні інтелектуальні заводські цехи отримують інформацію про стан конвеєрного виробництва або просування сировини в режимі реального часу. Промислова система управління відноситься до апаратних пристроїв і програмної інтеграції, які підтримують і контролюють критично важливі інфраструктури. Вона включає в себе програмований логічний контролер

(ПЛК), віддалений термінал (RTU), інтелектуальний електронний пристрій (IED), сервер управління, розподілену систему управління (DCS), диспетчерський контроль і збір даних (SCADA) і датчики [5].

Компоненти промислового IoT можуть відрізнятися залежно від застосування. Однак, як правило, вони поділяються на три категорії, які розглядаються нижче і показані на рисунку 1.1.2.

Рисунок 1.1.2. Компоненти промислового IoT

Периферійні пристрої або пристрої керування (Front-End Edge Devices), відповідають за збір даних і дії на основі даних. Дані можуть бути показаннями температури, акселерометра або відеопотоку. Датчики/пристрої можуть використовуватися як окремі одиниці або кілька датчиків, об'єднаних разом, а також датчики можуть бути вбудовані в пристрої, які виконують більше завдань, ніж просто зчитування даних. Технологія підключення (Connectivity Technology): після того, як дані зібрані, наступним кроком є відправка даних до хмари. Аналогічно, хмара надсилає назад команди до промислової системи IoT. Промислові системи IoT в основному покладаються на бездротові технології, включаючи Bluetooth, Mesh-мережі, WiFi і LPWAN. Аналіз даних платформи промислового IoT (Industrial loT Platform for Data Analysis): промислова система IoT містить промислове програмне забезпечення IoT для аналізу отриманих і переданих даних. Промислове програмне забезпечення IoT також може приймати рішення і передавати команди назад на периферійні пристрої управління. Промисловий Інтернет речей - це інноваційна спроба створити розумне виробниче

середовище, використовуючи переваги Інтернету речей в управлінні промисловими процесами. Промисловий Інтернет речей зосереджується на міжмашинних комунікаціях (M2M), машинному навчанні та великих даних, щоб дати можливість підприємствам і галузям підвищити надійність і ефективність своєї діяльності. Використання промислового Інтернету речей революціонізує сегментацію фабрик і промисловості, демонструючи її перевагу. Промисловий Інтернет речей стрімко розвивається і охоплює кілька послуг і галузей, як показано на рисунку 1.1.2. В індустрії гостинного господарства Інтернет речей може бути корисним для розуміння контексту гостей і прогнозування їхніх потреб завдяки інтелекту і вбудованим датчикам. У секторі охорони здоров'я можливості Інтернету речей безмежні. Система телемедицини базується на IoT. Це практика надання медичної допомоги за допомогою передачі даних та інтерактивних аудіовізуальних засобів. Освітні заклади також користуються перевагами різних додатків Інтернету речей. Наприклад, IoT використовується в e-learning, m-learning та u-learning. Сектор фінансових послуг також береться за IoT. Страхові компанії використовують телематичні додатки для прогнозування та оцінки можливих ризиків, які можуть призвести до претензій з боку клієнта. Енергетичні компанії використовують розумні мережі для збору аналітики, підвищення безпеки та швидкого відновлення після збоїв в електропостачанні. Інтернет речей змінює роботу ринку роздрібної торгівлі. Автоматизовані каси встановлюються на фасадній стороні магазинів. Це рішення дозволяє працівникам зосередитися на бізнес-можливостях і потребах замість того, щоб витрачати час на роботу касира. Одним з найкращих прикладів галузей, які впроваджують додатки Інтернету речей, є обробна промисловість. Виробники використовують IoT для відстеження виробничого потоку. Завдяки даним, зібраним з пристроїв Інтернету речей, виробники можуть вимірювати якість продукції. Удосконалення технологій обробки великих даних і потокової передачі даних дозволило організаціям ширше використовувати продукти штучного інтелекту (ШІ) і машинного навчання (МН) в Індустрії 4.0. Застосування ШІ та МН з'являються в охороні здоров'я, освіті, обороні, безпеці, промисловості тощо. Багато технологічних гігантів вкладають

мільярди доларів у розробку продуктів ШІ, таких як автономні автомобілі (самокеровані машини). Google, NVIDIA та інші розробляють алгоритми самокерованого водіння на основі комп'ютерного зору, а також розпізнавання пішоходів, виявлення зіткнень тощо. Автомобільні компанії, такі як Ford, General Motors, Nissan, Tesla, Mercedes та інші, інвестували мільярди в дослідження і розробки. Сотні інших невеликих компаній створюють радари, камери, обчислювальні та комунікаційні системи, інші датчики тощо.

1.2. Аналіз проблеми захисту промислових мереж і пристроїв

Проблемою для галузей є безпека. Це питання є надзвичайно важливими через зростаючу вразливість до атак та витоків даних. У контексті промислового інтернету речей дані вважатимуться критично важливими і конфіденційними, оскільки вони охоплюватимуть різні аспекти промислової діяльності, в тому числі дуже конфіденційну інформацію про продукти, бізнес-стратегії та компанії. Перехід до більш вразливих і відкритих мереж і можливостей обміну даними в Інтернеті речей підвищує ризики в промислових галузях. Витік конфіденційних даних може призвести до значних збитків і втрат. Існує багато викликів, які впливають на безпеку пристроїв Інтернету речей. Оскільки ідея об'єднання пристроїв Інтернету речей не є новою, безпеці не надається великого значення на етапі проектування пристроїв. Крім того, враховуючи той факт, що ринок Інтернету речей тільки зароджується, багато виробників пристроїв все більше прагнуть якнайшвидше вивести свої пристрої на ринок, замість того, щоб знайти спосіб включити заходи безпеки на самому початку. Розглянемо основні проблеми і загрози.

Використання паролів за замовчуванням або жорстко закодованих паролів є однією з проблем, які можуть спричинити проломи в безпеці. Навіть якщо

користувачі змінюють паролі, вони зазвичай недостатньо надійні, щоб запобігти вторгненню [6].

Обмеженість ресурсів IoT-пристроїв - ще одна проблема. Багато пристроїв Інтернету речей не забезпечують або не можуть забезпечити просунуту безпеку. Наприклад, датчики моніторингу температури не можуть впоратися з найсучаснішим шифруванням або іншими заходами безпеки.

Спроби підключити застарілі активи, які насправді не призначені для підключення до Інтернету речей, є ще однією проблемою безпеки. Заміна інфраструктури цих об'єктів мережевими технологіями вимагає надмірних витрат. Однак шанси на атаку набагато вищі в цих застарілих активах через відсутність оновлень і відсутність захисту від сучасних загроз. Що стосується оновлень, велика кількість систем просто включає довідку на певний період часу. Для нових і застарілих ресурсів безпека може вислизнути, якщо не включити додаткову допомогу, оскільки численні пристрої Інтернету речей залишаються в мережі протягом тривалого часу. Безпека IoT також страждає від відсутності стандартів, визнаних індустрією[6]. Незважаючи на існування численних фреймворків безпеки IoT, жоден з них не є загальноприйнятим. Величезні організації та галузі можуть мати свої власні специфічні стандарти, в той час як певні частини, наприклад, промисловий IoT, мають обмежувальні, непослідовні стандарти. Безпека систем і гарантія сумісності між ними стали ще складнішими, оскільки різноманітність цих стандартів ускладнює захист систем. Виробники, постачальники послуг і кінцеві користувачі повинні навчитися розглядати безпеку як спільну проблему. Безпека і конфіденційність продуктів і послуг повинні бути пріоритетом для виробників і постачальників послуг. Кінцеві користувачі також повинні подбати про власну безпеку, часто змінюючи паролі, використовуючи доступне програмне забезпечення для захисту і встановлюючи патчі.

1.3. Мета та завдання управління захистом промислових IoT від кібератак

Компанії вважають безпечний обмін даними важливою вимогою безпеки. Крім того, деякі компанії не наважуються застосовувати підходи, засновані на обміні даними, такі як інтелектуальне обслуговування, виявлення і запобігання несправностей і хмарні сервіси, оскільки вони вважають, що дані, якими вони обмінюються з постачальниками послуг, можуть бути недостатньо захищені. Є організації, які не наважуються розгортати хмарні сервіси або залежать від хмарних провайдерів у питаннях зберігання та обміну даними з клієнтами. Ще одна серйозна проблема виникає, коли витік даних відбувається всередині організації. Існують і інші проблеми, пов'язані з пристроями, додатками та середовищами IIoT. Методи захисту даних повинні бути легкими, щоб їх можна було використовувати в пристроях IIoT з обмеженими ресурсами. Крім того, ці методи повинні мати можливість працювати на гетерогенних пристроях. Деякі критичні додатки IIoT вимагають повноцінного механізму захисту даних, тому неможливо реалізувати цей механізм на пристрої з обмеженими ресурсами (тобто, перевага надається периферійним вузлам). Безпека даних є важливою, оскільки в промислових умовах важливо обмінюватися даними для забезпечення різних інтелектуальних можливостей, а отже, дані зазвичай є чутливими. Пристрої IIoT генерують великі обсяги даних, ці дані повинні оброблятися за допомогою розподілених обчислень і зберігатися в одному або декількох вузлах для аналізу і пошуку. Це створює проблеми з безпекою та конфіденційністю, а також проблеми з масштабуванням. Для захисту конфіденційних даних та безпечного обміну даними необхідні ефективні протоколи. Середовища IIoT складаються з різних пристроїв, починаючи від крихітних вбудованих систем і закінчуючи повноцінними серверами. Важливо виділити проблеми безпеки на різних рівнях IIoT.

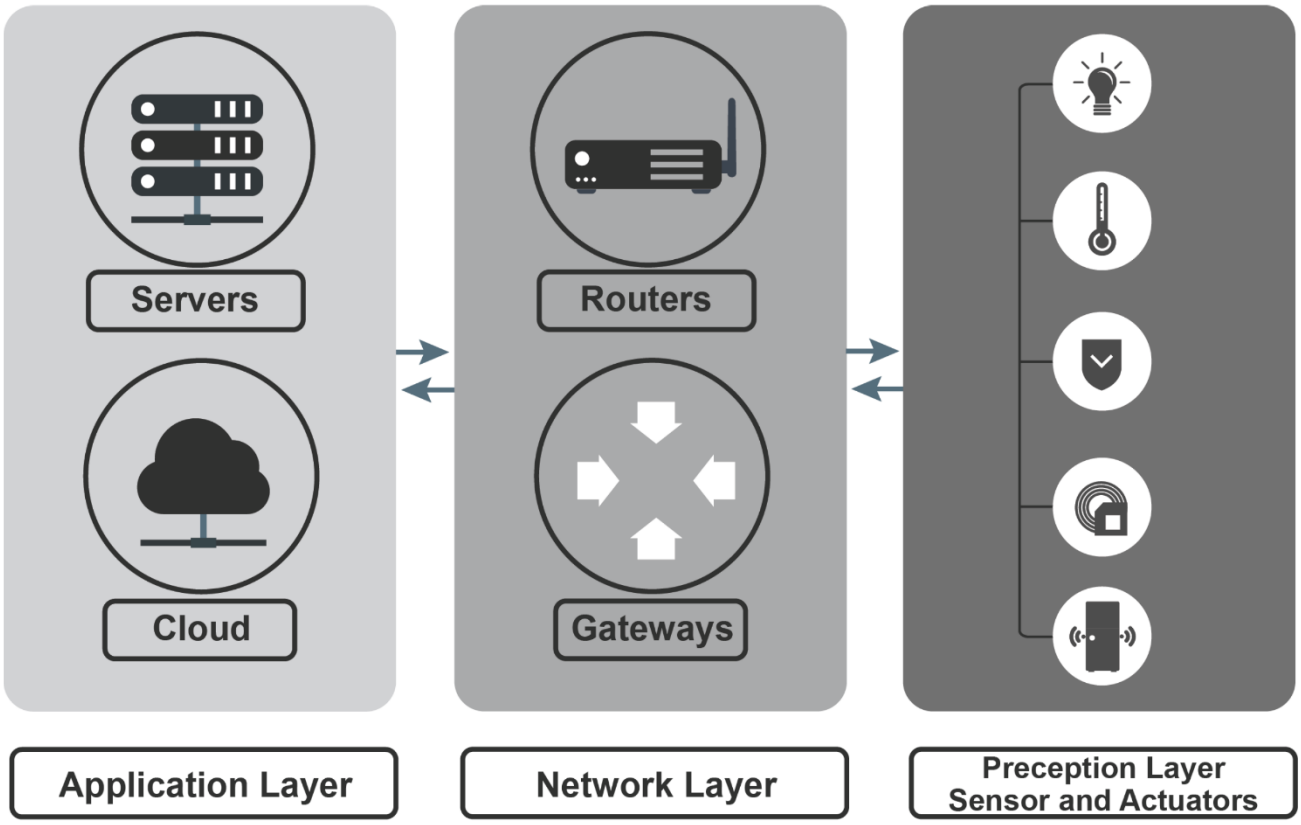

Рисунок 1.3. Структура трьох традиційних рівнів IIoT: сприйняття, мережа та додаток

Як показано на рисунку 1.3., традиційна архітектура рівня IIoT складається з трьох рівнів: рівень сприйняття (Preception Layer), мережевий рівень (Neywork Layer) і прикладний рівень (Application Layer). Кожен рівень має свої власні технології та унікальні особливості. Розглянем ці три рівні і проблеми, з якими стикаються додатки IIoT при застосуванні вимог безпеки в промислових середовищах [7]. У Таблиці 1.3 показані популярні атаки, які націлені на три рівні IIoT, а також їх загальні заходи протидії.

Таблиця 1.3.

Популярні загрози безпеці, та загальні заходи протидії їм

Рівень	Атака	Порушені вимоги	Загальні заходи протидії
Сприйнят-тя	Вузол захоплення	Конфіденційність, автентифікація	Знищення інформації, пов”язаної з захищеними ключами, після роз”єднання

Продовження таблиці 1.3.

Популярні загрози безпеці, та загальні заходи протидії їм

Рівень	Атака	Порушені вимоги	Загальні заходи протидії
	Глушіння	Доступність	Підвищення стійкості до перешкод за допомогою таких методів, як FHSS I D
	Позбавлення сну	Доступність	Забезпечення відсутності порушень політики безпеки за допомогою IDS
	Відтворення	Цілісність	Використання міток часу
Мережа	Мережева вибіркова переадресація	Доступність	Виявлення та запобігання з використанням комбінації IDS та IPS
	Підслуховування	Конфіденційність	Використання методів контролю доступу та шифрування даних
	Клонування ідентифікаторів	Автентифікація	Застосування методів фільтрації пакетів IDS та локалізації
	Червоточина	Конфіденційність, доступність	Розгортання безпечних методів виявлення сусідніх вузлів та вимірювання затримки виклику-відповіді та RTT
	Відмова в обслуговуванні	Доступність	Використання фільтрації трафіку, IDS і методів відстеження
	Людина посередині	Конфіденційність, автентифікація	Використання легких методів шифрування та розгортання

Продовження таблиці 1.3.

Популярні загорзи безпеці, та загальні заходи протидії їм

Рівень	Атака	Порушені вимоги	Загальні заходи протидії
Додатки	Впровадження шкідливого коду	Конфіденційність, автентифікація	Використання криптографії з приватним ключем, легкого шифрування
	Міжсайтовий або шкідливий скрипт	Конфіденційність, автентифікація	Впровадження IDSна основі підписів, а також методів аналізу контенту та шаблонів
	Впровадження шкідливого програмного забезпечення	Цілісність	Розгортання IDS, IPS та механізмів видалення шкідливого програмного забезпечення
	Спотворення даних	Цілісність та безпечний обмін даними	Використання контролю доступу, шифрування та відновлення, механізм резервного копіювання
	SQL injection	Конфіденційність, автентифікація	Використання параметризованих операторів IDS, контролю доступу та методів шифрування
	Програми вимагачі	Конфіденційність, автентифікація	Використання фільтрації трафіку, IDS, IPS та методів шифрування
	Побічний канал	Конфіденційність	Захист криптографічних методів, запобіганню аналізу трафіку та впровадження суворих політик контролю доступу

Продовження таблиці 1.3.

Популярні загрози безпеці, та загальні протидії їм

Атака	Порушені вимоги	Загальні заходи протидії
Авторизація та автентифікація	Автентифікація та контроль доступу	Використання методів контролю доступу та автентифікації

Атаки на рівень сприйняття. Рівень сприйняття (також відомий як рівень пристроїв) складається з пристроїв, оснащених різними об'єктами, такими як датчики, камери, роботи і розумні лічильники, як показано на рисунку 2.1. Цей рівень відповідає за ідентифікацію та збір інформації, пов'язаної з цільовим датчиком. Ця інформація включає вимірювання таких величин, як рух, хімічні речовини в конкретному середовищі, вібрації, тепло, прискорення або вологість. Зібрані дані передаються на нижній рівень (тобто мережевий рівень), а потім за допомогою керованого (наприклад, промислового кабелю Ethernet) або некерованого середовища (наприклад, WiFi) передаються до системи обробки інформації на периферії [8].

Атаки на захоплення вузлів. У цьому типі атак зловмисник може фізично отримати або замінити вузол IIoT або модифікувати певне обладнання. Цей тип зловмисних дій призводить до викриття конфіденційної інформації, пов'язаної з координацією цифрових прав, такої як криптографічні ключі або ключі доступу. Як тільки зловмисник отримує доступ до пристрою IIoT, він може діяти зловмисно, щоб завдати шкоди іншим пристроям в мережі [9]. Атаки глушіння. Цей тип атаки може порушити або попередити зв'язок пристроїв IIoT шляхом підробки або втручання в режим доступу до бездротового зв'язку. Таким чином, пристрої IIoT не зможуть успішно передавати дані іншим мережевим об'єктам [10]. Зловмисники можуть глушити бездротовий сигнал віддалено, використовуючи потужний пасивний передавач. Вони також можуть використовувати методи екранування, щоб обійти захисні механізми. Радіошум, який відповідає частоті певної системи, може бути використаний для зловмисного втручання в роботу систем RFID.

Атаки позбавлення сну. Це сімейство атак не дозволяє пристроям IIoT переходити в сплячий режим, вставляючи в пам'ять пристрою нескінченно циклічні коди або вносячи апаратні модифікації. За замовчуванням, пристрої IIoT працюють від батареї і залишаються в сплячому режимі, коли вони не передають і не отримують інформацію, щоб зберегти заряд батареї; однак ці атаки можуть розрядити батареї пристроїв IIoT, активно пробуджуючи їх, що в кінцевому підсумку призведе до їх повного вимкнення (це тип DoS-атаки) [11].

Атаки на відтворення. Без механізмів аутентифікації зловмисник може перехопити раніше легітимне повідомлення, передане з пристрою IIoT на інший об'єкт, а потім модифікувати і відтворити його в кінцевому пункті призначення [12]. Цей вид атаки можливий, коли аутентифікація застосовується в певному середовищі IIoT. Зловмисник може підслуховувати бездротовий канал, перехоплювати повідомлення, клонувати і використовувати код автентифікації в перехопленому повідомленні (тобто згенерований відправником).

Атаки на мережевому рівні. Як показано на рисунку 1.3., після того, як дані передаються з рівня сприйняття на мережевий рівень, він визначає шлях, яким повідомлення досягне одержувача (цей шлях включає перший прикордонний маршрутизатор, який відповідає за пересилання повідомлення до наступного маршрутизатора на маршруті) [13]. Мережевий рівень призначений для передачі мережевих пакетів (так званих дейтаграм) між гетерогенними мережами, що передаються різними пристроями IIoT. Ці мережеві пакети надсилаються інтерфейсом пристрою IIoT за допомогою протоколу зв'язку, проходячи через різні лінії зв'язку. Передані пакети від пристроїв IIoT зазвичай отримуються вузлами на периферії, такими як маршрутизатори або шлюзи, для обробки і пересилання в зовнішній світ [14]. Тому пристрої IIoT та прикордонні вузли є вразливими до атак на мережевому рівні.

Атаки на підслуховування. Цей тип атак дозволяє зловмиснику прослуховувати поточний обмін повідомленнями між пристроями IIoT в каналі зв'язку. Обмін повідомленнями може включати конфіденційну інформацію, в тому

числі паролі та банківську інформацію у відкритому вигляді, якщо не застосовується шифрування [15].

Атаки Sybil та ID-клонування. Відбувається, коли зловмисник викрадає ідентифікатор легітимного пристрою IIoT, щоб порушити зв'язок між пристроями. Зловмисник може заволодіти різними ідентифікаторами, щоб обдурити пристрої IIoT і змусити їх повірити, що в мережі знаходиться багато пристроїв IIoT . З іншого боку, атака з використанням ідентифікатора клону може бути визначена як підробка ідентифікатора легітимного вузла і вдавання, що зловмисник має ідентифікатор іншого легітимного вузла в мережі. Він може запустити цю атаку, щоб отримати доступ до більшої кількості пристроїв у мережі [16,17].

Атаки через червоточину. Цей тип атаки дозволяє двом зловмисникам створити віртуальний міжміський тунель, який створюється для того, щоб змусити інші пристрої в мережі передавати свої пакети через цей тунель. Крім того, інформація, якою обмінюються, може проходити через проміжні легітимні вузли, розряджаючи їхні батареї [18].

Атаки на відмову в обслуговуванні (DoS). Зловмисник може запустити цей тип атаки для саботажу пропускної здатності або мережевих ресурсів, що може бути досягнуто шляхом активної передачі великої кількості пакетів на пристрої/сервери, підключені до мережі, на невизначений або тимчасовий час, щоб зробити їх зайнятими і перешкодити їм виконувати свою звичайну діяльність. Ця атака може також розрядити батареї пристроїв IIoT, що призведе до їх повного вимкнення [19,20]. Інший підвид DoS-атак - DDoS, який компрометує звичайні пристрої IIoT, що не мають належного захисту, і перетворює їх на джерело атакуючого трафіку. Цю атаку можна класифікувати на логічну та затоплення. Логічна атака дозволяє зловмиснику передавати оманливі повідомлення, щоб ввести в оману звичайних користувачів і змусити їх повірити, що додаток або сервіс на машині, з якою вони зв'язуються, недоступний (тобто повністю зайнятий). Атака переповнення націлена на периферійні пристрої або сервери IIoT шляхом передачі великої кількості пакетів, що робить цільові пристрої нездатними обробляти ці пакети і в кінцевому підсумку робить їх недоступними для звичайних користувачів

мережі (тобто вони не можуть відповідати на звичайні запити від легітимних користувачів). Периферійні обчислення більш вразливі до DoS-атак, ніж хмарні, оскільки послуги надаються периферійними пристроями IIoT, які не можуть бути оснащені відповідними механізмами захисту через обчислювальні обмеження. Крім того, зловмисники націлені на периферійні пристрої і використовують їх як джерела для запуску атак на сусідні периферійні сервери; отже, атаки можуть бути більш серйозними, ніж при націлюванні на віддалені хмарні сервери (в цьому випадку трафік буде проходити через різні маршрутизатори і може бути заблокований ще до того, як досягне хмарного сервера).

Атака з вибірковою переадресацією є різновидом DoS-атаки. У цій атаці зловмисник може вибрати пересилання певних пакетів (наприклад, керуючих повідомлень RPL) і відкинути решту пакетів, щоб порушити маршрут. Ця атака може мати більш серйозні наслідки в поєднанні з іншими атаками, такими як sinkhole-атаки [21]. Зловмисник запускає цю атаку, щоб змусити мережеві об'єкти повірити, що він є вузлом-відстійником (тобто вузлом у мережі з більшими можливостями, ніж інші вузли в мережі), і перенаправити мережевий трафік на нього. Переадресований трафік в кінцевому підсумку передається зловмиснику і може не досягти цільового одержувача .Ця атака може бути запущена зловмисним вузлом, який діє як діра (вузол, який змушує інші мережеві об'єкти направляти пакети до нього і скидати переадресовані пакети), щоб знизити продуктивність мережі IIoT . Атаки «людина посередині». Зловмисник може запустити цю атаку, щоб стати "людиною посередині" поточної комунікації між двома легітимними вузлами IIoT. Зловмисник може відстежувати комунікацію в режимі реального часу, а також перехоплювати і змінювати повідомлення, якими вони обмінюються.

Атаки на рівні додатків. Як показано на рисунку 1.3, останнім рівнем в традиційній архітектурі рівнів IIoT є прикладний рівень. Рівень додатків представляє дані і надає користувачам IIoT різні додатки, такі як інтелектуальний транспорт, інтелектуальне виробництво і інтелектуальна логістика [22]. Останнім часом пристрої IIoT стали спокусливими цілями для атак на рівні додатків. Пристрої та аналітичні системи IIoT надають різноманітні переваги галузям, які

допомагають збільшити темпи зростання та ринкову капіталізацію. Однак будь-яка можливість раптового простою може призвести до значних збитків. Тому зловмисники вважають пристрої IIoT ідеальною мішенню для отримання прибутку, адже в разі успіху атак зловмисників, промисловість, швидше за все, заплатить викуп, щоб уникнути простою, який може статися через ці атаки. Пристрої IIoT вразливі до атак з вимогою викупу в деяких розгортаннях IIoT, таких як розгортання "Браунфілд-IIoT". У таких розгортаннях застарілі системи, розгорнуті на периферії, повинні бути підключені до інтернету. Ці системи вразливі до кількох проблем безпеки, оскільки вони зазвичай не підтримують належних заходів безпеки, таких як шифрування, оновлення та виправлення. Робочі станції на периферії, які використовують ці системи (особливо ті, що використовують неоновлені операційні системи), є середовищем, яке зловмисники можуть використовувати для поширення своїх атак в середовищі IIoT, оскільки вони мають прямі або опосередковані зв'язки з ICS. Зазвичай ICS використовують інтерфейси робочих станцій через протокол OLE для управління процесами. Крім того, інші процеси, такі як NetBIOS та SMB, використовуються ICS для впровадження та конфігурації. Після зараження робочої станції через шкідливий USB-накопичувач, шкідливе посилання або підозрілий файл, програма-вимагач може легко поширюватися на критично важливі ICS. В останні кілька років версія вірусу-здирника, відома як "WannaCry", використовувала інтерфейси робочих станцій для поширення атак в середовищах IIoT, що вплинуло на кілька галузей по всьому світу. Прикладний рівень вразливий до різних проблем безпеки, перелічених нижче:

Атаки впровадження шкідливого коду. Зловмисники можуть використовувати вразливості, пов'язані з модулями налагодження, для впровадження шкідливого коду. Після впровадження шкідливого коду зловмисник може виконувати небажані дії на ураженому пристрої . Він може здійснювати зловмисні дії у всій мережі через уражений пристрій [23]. А також пристрої IIoT можуть бути інфіковані під час оновлення прошивки програмного забезпечення за допомогою утиліти OTA. Зокрема, зловмисник може впровадити вірус в пристрій

IIoT, коли пристрій встановлює заплановане оновлення прошивки; отже, ця дія вимагає перезавантаження пристрою IIoT, щоб бути ефективною. Щоб захистити пристрої IIoT від таких атак, повинен існувати відповідний механізм аутентифікації та ідентифікації для периферійних пристроїв, а також забезпечення того, щоб оновлення та модернізації, які можуть бути встановлені на пристрої IIoT, були надійними (тобто не містили шкідливого програмного забезпечення).

Міжсайтові атаки або атаки шкідливих скриптів. Ці вразливості можуть бути використані зловмисниками через веб-сайти, які відвідують користувачі IIoT [24]. Підозрілі веб-сайти можуть бути оснащені шкідливими скриптами, які заманюють систему користувача до зараження, розкриваючи таким чином дані користувача. Такі шкідливі скрипти можуть бути створені за допомогою будь-якої мови сценаріїв, наприклад, JavaScript, як і будь-який інший легальний скрипт, і запущені будь-яким інтернет-браузером. Однією з можливих загроз міжсайтових і шкідливих скриптів є їхня здатність заманювати користувачів до завантаження даних навіть без перевірки.

Атаки впровадження шкідливого програмного забезпечення. У цьому типі атак зловмисник націлюється на сервісні запити прикордонного пристрою жертви, щоб впровадити шкідливе програмне забезпечення в систему або мережу цього пристрою [25]. Ця атака призводить до руйнівних загроз для безпеки системи та цілісності даних. До такого роду атак схильні як периферійні сервери, так і пристрої. Граничний сервер може бути атакований ін'єкційною атакою шкідливого програмного забезпечення, відомою як SSI. Цю атаку можна розділити на чотири класи: XML-ін'єкції, CSRF-ін'єкції, XSS-ін'єкції та SSRF-ін'єкції. Граничні пристрої схильні до атаки впровадження шкідливого програмного забезпечення, відомої як DSI (наприклад, RCE або reaper), в якій зловмисник впроваджує шкідливий код в цільовий пристрій IIoT.

Атаки спотворення даних. У цьому типі атак зловмисники підслуховують бездротовий канал, перехоплюють пакети, що передаються між мережевими об'єктами, спотворюють їх і пересилають одержувачу .

Атаки типу SQL Injection. Цей тип атак використовує вразливості додатків, які отримують і передають інформацію з баз даних і до них. Цей тип атак також може модифікувати SQL-запит, що виконується, шляхом зловмисного запуску фрагмента запиту, наприклад, через веб-форму. Таким чином, зловмисник може отримати доступ до бази даних і змінити схеми, таблиці, кортежі або атрибути бази даних.

Атаки з використанням програм-вимагачів. Атаки з вимогою викупу - це підгрупа сімейства атак зловмисного програмного забезпечення, де зловмисник викрадає пристрої або файли IIoT і вимагає компенсацію (зазвичай гроші) за відновлення доступу до пристроїв IIoT або розшифрування файлів, щоб пристрій-жертва міг знову ними користуватися. Кіберзлочинці, які здійснюють цей тип атак, зазвичай взаємодіють з жертвами і просять їх заплатити викуп в обмін на розшифровку файлів або відновлення доступу до пристроїв Інтернету речей [26]. Атаки побічних каналів. Цей тип атаки використовує загальнодоступні дані для вилучення конфіденційних даних, пов'язуючи їх з приватними даними користувача. Зловмисник використовує загальнодоступні дані в периферійній обчислювальній інфраструктурі та подає їх як вхідні дані для ML, DL або анонімних алгоритмів для отримання бажаного результату (наприклад, конфіденційної інформації). Атаки побічних каналів можуть бути спрямовані на будь-який об'єкт мережі, а зловмисники можуть використовувати різні методи для запуску атак побічних каналів, такі як атаки на синхронізацію, атаки на кеш і електромагнітні атаки . Атаки на авторизацію та аутентифікацію. У цих типах атак зловмисник використовує фальшиві облікові дані для отримання доступу до захищених ресурсів. Зазвичай, периферійні сервери і пристрої проходять аутентифікацію в периферійних обчисленнях, щоб дозволити периферійним пристроям отримати доступ до сервісів або ресурсів, розміщених на периферійних серверах. Ці типи атак можна розділити на чотири групи: загрози, які використовують методи аутентифікації, загрози, які націлені на протоколи авторизації, словникові атаки та атаки з використанням надмірних привілеїв [27]. При словниковій атаці зловмисник створює файл найбільш часто

використовуваних паролів і за лічені хвилини перебирає всі можливі паролі, щоб визначити правильні облікові дані, які дозволяють зловмиснику отримати доступ до ресурсів конкретного користувача. В атаках на протоколи автентифікації та авторизації зловмисник використовує вразливості авторизації або автентифікації, щоб розкрити облікові дані автентифікованого користувача, таким чином отримуючи доступ до ресурсів або послуг на периферійних серверах як авторизований користувач. В атаках з використанням надмірних привілеїв зловмисник може вимкнути систему або отримати доступ до неї як авторизований користувач, вставивши шкідливе програмне забезпечення. Ця атака може бути здійснена в різних формах, наприклад, шляхом зміни ключа від дверей розумного будинку, а також отримання та використання голосових записів користувача.

Висновок до 1 розділу. В цьому розділі був зроблений огляд Промислових Інтернет речей, його структура, функції, використання. Впровадження промислового Інтернету речей надає переваги, які варіюються від автоматизації та оптимізації до усунення ручних процесів і підвищення загальної ефективності, але, головним залишається питання безпеки. Відсутність надійних механізмів захисту і масштабність функцій безпеки є значними перешкодами для підвищення безпеки IIoT. За останні кілька років ми стали свідками тривожних атак з використанням вразливостей мережевих пристроїв IIoT. Більше того, зловмисники можуть також проникати вглиб мережі, використовуючи взаємозв'язки між вразливими місцями. Такі загрози мережевій безпеці призводять до того, що галузі та підприємства зазнають фінансових збитків, шкоди репутації та крадіжки важливої інформації.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПРОМИСЛОВИХ IoT

2.1. Промислові системи керування, призначення і функції

Промислові системи керування (ПСК) оточують нас повсюди: у водо-, газо- та електропостачанні, та розподільчих мережах, на електростанціях та критично важливих об'єктах інфраструктури, на виробничих лініях інфраструктури, у виробничих лініях та транспортних мережах тощо. Вони були створені та впроваджені за останні кілька десятиліть для того, щоб допомогти промисловим організаціям пілотувати свою виробничу інфраструктуру та критично важливі об'єкти. ПСК відповідають міжнародним стандартам, встановленим міжгалузевими вертикальними (МСА, МЕК) або галузевими організаціями (МАГАТЕ в атомній енергетиці, CENELEC у залізничному транспорті тощо).

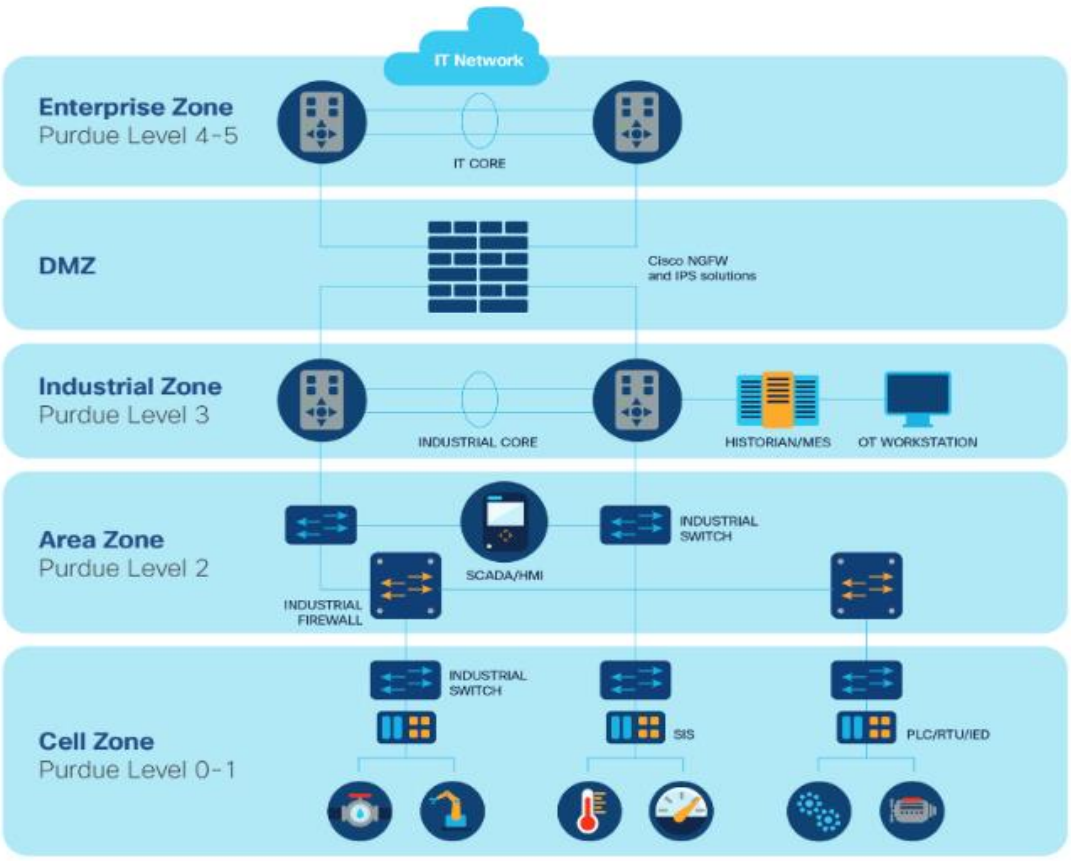

Рис. 2.1. Структура промислової системи керування

Рівень 0 (Cell Zone) - Польовий: датчики, виконавчі механізми, двигуни

Рівень 1 (Cell Zone) - Процес: пристрої автоматизації, системи безпеки, контролери

Рівень 2 (Area Zone) - Контроль: станції SCADA, операторські станції DCS, інженерні станції

Рівень 3 (Industrial Zone) - Виробничі операції: MES, LIMS

IT - рівні 4 і 5 (Enterprise Zone)- бізнес: офіс, ПК, обмін повідомленнями, інтернет

Часто буває важко класифікувати мережі, які вважалися б IT, якщо дивитися лише на їхні технічні характеристики. Насправді, починаючи з 2000-х років промислові системи інтегрують традиційні IT-компоненти (Microsoft Windows, Ethernet, IETF, TCP/IP тощо) у свої мережі ІКС, що робить розрізнення ще більш складним. Однак, існує спосіб точно визначити промислову мережу управління;

якщо принаймні 4 з 5 характеристик, наведених нижче, то це промислова мережа управління:

- Вона спрямована на пілотування та контроль фізичного процесу

- Вона розгорнута в середовищі, що вимагає певної стійкості обладнання (до 70°C, живлення 12В або 24В постійного струму, пилонепроникність, рівень захисту IP від 20 до 80 і т.д.).

- Використовує стандартизовані протоколи зв'язку IEC або пропрієтарні протоколи від визнаних виробників (див. список виробників пристроїв ICS

виробників пристроїв ICS нижче)

- Складається в основному з низькошвидкісного зв'язку "машина-машина" зв'язку (локальні мережі від 10 до 100 Мбіт/с, 512 кбіт/с віддалені мережі)

- Використання IT-технологій (наприклад, протоколів HTTP IETF) зарезервовано для операцій управління: веб-адміністрування, SNMP, або ICMP-моніторингу. І навпаки, немає ніяких "користувацьких" комунікацій (веб-серфінг, обмін повідомленнями тощо)

У традиційному IT-світі ризик включає в себе загрози, які можуть підірвати конфіденційність, цілісність та доступність даних і систем. Вплив переважно фінансовий, наприклад, випадки вимагання (вірус Cryptolocker), банківське шахрайство або атаки на відмову в обслуговуванні, що поширюються на веб-сервери, які використовуються сайтами електронної комерції.

Промислові системи управління керують фізичним світом, де використовуються операційні технології (так звані OT). Ризик в середовищах ICS включає в себе загрози, які можуть підірвати операційну безпеку.

На відміну від споживчих мереж, де основними векторами загроз є Інтернет, в ІКС існує побоювання, що шкідливі програми можуть бути вставлені через USB-носії або шляхом бічного переміщення шкідливого програмного забезпечення на станції які пілотують ICS. Дистанційна діагностика і дистанційне обслуговування

вимагають віддаленого доступу до мереж і промислових систем управління. Віддалений доступ є ще більш серйозним вектором загрози, оскільки він об'єднує мережі різної критичності, а іноді й за участю третіх осіб. Робочі станції віддаленого доступу підключаються до серця критично важливих промислових систем управління для виконання операцій, які можуть мати значний вплив (наприклад, оновлення програмного забезпечення або завантаження нової прошивки). Їх не можна просто заборонити, але їх потрібно контролювати за допомогою ефективних механізмів моніторингу. Всі ці вектори загроз здебільшого характерні для індустріального світу. Заходи безпеки, що впроваджуються в промислових системах контролю повинні враховувати оперативну реальність, яка необхідна персоналу ОП для того, щоб продовжувати експлуатувати об'єкти і працювати ефективно. Вони не можуть просто заборонити весь віддалений доступ або покладатися виключно на контроль доступу та організаційні заходи.

Крім того, промислові системи управління ніколи не були розроблені для боротьби із загрозами кібербезпеки. Вони створюються з метою забезпечення операційної безпеки та безперервності роботи, і вони часто не не враховують можливість того, що мотивований зловмисник може отримати доступ до їхніх цифрових інтерфейсів. Ось чому поки що продукти автоматизації мають лише кілька функцій кібербезпеки. В більшості випадків функції кібербезпеки не активуються промисловими операторами.

Промислові системи побудовані на наборі протоколів, які дозволяють обмінюватися комунікацій між компонентами в мережах. Існують деякі стандарти, такі як MODBUS або PROFINET, але протоколи для перепрограмування або модифікації систем керування здебільшого є власницькими і закриті. Більшість з них (Siemens, Schneider, ABB, Rockwell Automation та ін.) не планують відкривати свої протоколи з законних причин, пов'язаних з інтелектуальною власністю. Тому застосування таких IT-технологій, як перевірка протоколу на відповідність стандарту для всіх повідомлень. Ця методика залишається корисною для тих частин повідомлень (заголовки протоколів), які відповідають відкритим

стандартам (наприклад, MODBUS наприклад), але її було б дуже важко застосувати до закритого протоколу.

Для побудови ефективної стратегії кібербезпеки ICS дуже важливо визначити події безпеки, які є найбільш вірогідними. Це дозволить зосередитися на впровадженні відповідних заходів для захисту активів, які з найбільшою ймовірністю можуть бути атаковані, і підвищити безпеку чутливих активів, які зловмисник може використати для проникнення.

У сфері промислової кібербезпеки, побоювання з точки зору безпеки включають в себе кібератаку на промислову інформаційну систему, яка може завдати значної шкоди операціям компанії, виробничим інструментам, випуску продукції або навіть її працівникам чи клієнтам. Ці події матимуть суттєвий вплив у фізичному світі. У деяких випадках вони можуть призвести до кримінальних справ проти керівництва компанії.

Для кодифікації сценаріїв кібератак та деталізації їхніх різних етапів використовується концепція кібер-ланцюга вбивств. Ця концепція дозволяє детально описати структуру складної спроби вторгнення, характерної для нових атак. Етапи кібер-ланцюга вбивства такі: розпізнавання, озброєння, доставка, операції встановлення, командування і контроль, а також дії по досягненню цілей.

Особливо важливо розуміти, як зловмисник буде зламувати промислову мережу своєї цілі. Існує багато вразливих точок, які слід враховувати при розробці процесу моніторингу. Вони поділяються на такі групи класифіковані за ймовірністю:

Захоплення промислової станції

Зловмисник використовує цілеспрямовані IT-механізми розповсюдження (тобто шкідливе програмне забезпечення зв'язується з "командно-контрольним" сервером зловмисника) для поширення шкідливого програмного забезпечення в цільовій мережі, поки воно не досягне робочої станції в промисловому домені. Основними цілями є системи диспетчерського контролю та збору даних (SCADA)

та інженерні станції, оскільки вони містять важливу інформацію про процес (задані значення, змінні, що використовуються в програмуванні тощо).

Підміна авторизованого віддаленого доступу для третьої сторони

Зловмисник використовує авторизований віддалений доступ для третьої сторони, наприклад, субпідрядника. Це може бути ADSL або VPN-з'єднання, залишене відкритим або використовуване лише для певних IP-адрес. Такий віддалений доступ часто надає доступ до самого серця промислового об'єкта промислового об'єкта, забезпечуючи "якісну" точку входу для зловмисника.

Захоплення бездротового зв'язку

Зловмисник використовує загальнодоступну або власну вразливість бездротового бездротового зв'язку (відомі атаки на WEP або WPA). Таким чином, він може підключитися до промислової мережі управління. Після цього він отримує прямий доступ до серця системи на інженерних станціях, станціях SCADA і ПЛК.

Отримання доступу до польової мережі об'єкта

Зловмисник має прямий фізичний доступ до польової мережі об'єкта мережі об'єкта для здійснення атаки, наприклад, маючи доступ до комп'ютерної шафи вздовж розподільчої осі (трубопроводу в каналізації або вздовж кабелепроводу). Польова мережа дає прямий доступ до обладнання ICS, що використовується для керування модулями вводу/виводу. Це особливо важливо в транспортному секторі.

Встановлення стороннього фізичного компонента для модифікації мережу віддалено.

Щоб скористатися перевагами свого фізичного доступу без необхідності бути фізично присутнім у вразливому місці, зловмисник встановлює в промислову мережу модуль дистанційного керування: наприклад, мініатюрний Raspberry Pi з акумулятором і 4G-модемом модемом, що дає змогу дистанційно керувати системою.

Промислові мережі управління часто є географічно розгалуженими і складаються з багатьох "малих мереж" з невеликою кількістю компонентів. Щоб контролювати все це без розгортання складної і дорогої інфраструктури, система виявлення зазвичай складається з:

- Датчики, розташовані близько до процесу, які витягують дані зв'язку між пристроями

- Центрального сервера, який збирає, зберігає та аналізує дані, зібрані датчиками

Важливо розуміти, що так зване "просте управління контролером" надає зловмисникам безліч можливостей. З точки зору виявлення необхідно знати, як виявляти ці команди в мережі.

Для вилучення інформації, необхідної для моніторингу промислової системи

кібербезпеки промислової системи, платформа повинна декодувати потоки додатків, зібрані в промисловій мережі. Ці потоки можуть використовувати кілька типів мережевих протоколи:

- Відкриті протоколи, специфікації яких відомі та доступні. Ці протоколи були стандартизовані міжнародними організаціями

- Власні розширення відкритих протоколів. Ці розширення використовують відкриту область даних і включають власні, недокументовані структури даних структури

- Закриті протоколи, специфікації яких не є загальнодоступними.

2.2. Способи захисту систем і пристроїв промислових інтернет речей

Існують різні способи захисту систем і пристроїв Інтернету речей в залежності від місця в екосистемі Інтернету речей і конкретного застосування Інтернету речей. Загальними заходами безпеки IoT є наступні:

- Проактивні міркування щодо безпеки: розробники IoT повинні враховувати питання безпеки на початку розробки будь-якого пристрою.

- Уникання жорстко закодованих облікових даних: розробник повинен переконатися, що жорстко закодовані облікові дані необхідно змінити до того, як пристрій почне функціонувати.

Іноді продукт має облікові дані за замовчуванням, які слід замінити надійним паролем або вжити інших заходів, таких як розпізнавання відбитків пальців тощо.

- Безпека API: має фундаментальне значення для забезпечення достовірності інформації, яка передається від об'єктів IoT до внутрішніх систем. Крім того, важливо гарантувати, що тільки авторизовані пристрої або об'єкти можуть здійснювати будь-який зв'язок з API.

- Унікальна ідентифікація: надання кожному пристрою унікального ідентифікатора є життєво важливим для розуміння того, що це за пристрій, за допомогою яких засобів він діє, з якими пристроями він з'єднується, а також належних заходів безпеки, які слід вжити для цього пристрою.

- Шифрування: надійне шифрування має вирішальне значення для забезпечення безпечного зв'язку між пристроями. Для захисту даних слід використовувати алгоритми шифрування.

- Безпека в Інтернеті: дуже важливо забезпечити безпеку мережі IoT . Це можна зробити, переконавшись, що системи регулярно оновлюються і виправляються, забезпечуючи безпеку портів, не відкриваючи порти без необхідності, використовуючи такі функції, як брандмауери, а також виявляючи і блокуючи несанкціоновані IP-адреси.

- Шлюзи: шлюзи виступають посередником між Інтернетом та об'єктами IoT і зазвичай мають більшу пропускну здатність, пам'ять та пропускну здатність порівняно з самими об'єктами IoT. Тому вкрай важливо виконувати такі речі, як брандмауери, які гарантують, що зловмисники не зможуть дістатися до об'єктів IoT.

- Виправлення: дуже важливо постійно оновлювати програмне забезпечення та пристрої або автоматично або через мережеве з'єднання.

IIoT має свої власні проблеми безпеки, загрози та вразливості, на додаток до того, що він успадковує всі проблеми безпеки IoT. Крім того, якщо IIoT включає в себе хмарні обчислення, він також додає всі хмарні загрози і вразливості.

2.3. Вимоги до безпеки ПоТ, можливості та напрямки

Загальні вимоги безпеки, яким повинна відповідати кожна система зв'язку, включаючи середовища IIoT, при розгортанні пристроїв IIoT для периферійних обчислень.

Тріада ЦРУ. Модель інформаційної безпеки, відома як тріада ЦРУ, може розглядатися як будівельний блок для вимог або цілей безпеки. Набір механізмів безпеки також належить до цих трьох вимог, які коротко визначаються наступним чином: конфіденційність стосується захисту інформації в будь-якій формі. Методи, що використовуються для забезпечення конфіденційності, включають контроль доступу, шифрування, мережеву ізоляцію та приватність. Цілісність має на меті забезпечити суб'єктам IIoT узгодженість, автентичність і точність, а також дозволяє побудувати довіру з іншими суб'єктами. Доступність гарантує, що система працює ефективно в будь-який час. Для забезпечення доступності використовуються різні методи, такі як децентралізація та резервування. Традиційно модель ЦРУ використовувалася в сфері інформаційної безпеки, маючи на увазі, що ця модель пов'язана виключно з інформацією. Тим не менш, модель CIA рівномірно адаптується і в інших сферах, в тому числі і в CPS[28] . Традиційно в промислових середовищах основна увага приділяється доступності, потім цілісності і, нарешті, конфіденційності. Тим часом, з використанням пристроїв, підключених до Інтернету, ця концепція повинна бути переглянута таким чином, щоб усі три вимоги розглядалися однаково. Таким чином, з розвитком Індустрії 4.0 та парадигми Інтернету речей, цілісність і конфіденційність повинні розглядатися

рівнозначно з доступністю. Хоча модель безпеки ЦРУ забезпечує хорошу основу і залишається надзвичайно важливою, коли вимоги безпеки визначаються для певної системи, вона не завжди є корисною для зведення суворих вимог до елементів цієї моделі безпеки, якщо вже є більше (наприклад, контекстної) інформації, яка може дозволити вивести конкретну вимогу безпеки. Наприклад, ми можемо просто задекларувати, що ми повинні зберігати конфіденційність даних у стані спокою; однак, така мета безпеки може не передбачати станів, яким повинен відповідати конкретний механізм конфіденційності. Крім того, це може бути відкритим для інтерпретації.

Автентифікація Основною проблемою в різних комунікаційних середовищах, таких як IIoT, є автентифікація віддалених об'єктів (наприклад, машин, користувачів і додатків) . У контексті додатків IIoT автентифікація стає більш складним завданням через природу пристроїв IIoT, які мають обмежені можливості через обмеження потужності, а також обмежені можливості зберігання і обробки даних [29]. Таким чином, для подолання цих обмежень слід розробити полегшений механізм автентифікації з такими характеристиками, як невеликі обчислювальні витрати і мінімальний розмір передачі даних. Іншою важливою проблемою, пов'язаною з автентичністю даних, є забезпечення можливості перевірки їхньої цілісності та недопущення зміни даних під час передачі . Крім того, це стосується конфігураційних файлів, які повинні бути перевірені на предмет того, що вони були створені уповноваженими суб'єктами і не були змінені з моменту їх створення. З огляду на природу пристроїв IIoT, середовища IIoT вимагають рішень для автентифікації, які задовольняють компроміс між легкістю і секретністю, оскільки відомі механізми автентифікації не можуть бути прийняті в таких середовищах. У середовищах IIoT, які використовують периферійні обчислення, автентифікація на основі блокчейну є підходящим рішенням для автентифікації віддалених об'єктів і забезпечення цілісності даних. Є полегшена система автентифікації повідомлень на основі блокчейну, яка забезпечує безпеку повідомлень, використовуючи при цьому мінімальні обчислювальні витрати для пристроїв IIoT з обмеженими ресурсами. Ця система використовує периферійні

сервери, щоб зобов'язати пристрої IIoT виконувати міждоменну автентифікацію та ефективно зменшити надлишковий зв'язок між цими пристроями. Секретність цієї моделі аналізується за допомогою схеми випадкового оракула, що доводить її стійкість до декількох атак.

Контроль доступу та авторизація має важливе значення в різних обставинах. Пристроям в середовищах IIoT слід надавати дозвіл на доступ до ресурсів периферійної мережі на основі їх привілеїв. Наприклад, системним адміністраторам буде надано більше дозволів ніж звичайним користувачам. У деяких ситуаціях пристрої IIoT працюють у двох режимах: адміністратор і звичайний користувач. Контроль доступу зазвичай розглядається як залежний від автентифікації, оскільки необхідно автентифікувати користувачів перед застосуванням політики доступу. Таким чином, механізми контролю доступу зазвичай схожі на механізми автентифікації. Контроль доступу може споживати ресурси пристроїв IIoT, оскільки пристрої IIoT повинні взаємодіяти з серверами авторизації на периферії, перш ніж отримати доступ до певних ресурсів. На контроль доступу певним чином впливає доступність, особливо в середовищі IIoT (тобто, воно дуже розподілене); таким чином, політики контролю доступу завжди повинні бути доступними для пристроїв IIoT [30]. Функція контролю доступу виступає в якості агента між конкретним користувачем або одним з процесів пристроїв IIoT і системними або граничними мережевими ресурсами, включаючи операційні системи, брандмауери, маршрутизатори, додатки і бази даних. Якщо певна сторона хоче отримати доступ до ресурсу, вона повинна спочатку пройти автентифікацію. Механізм автентифікації вирішує, чи дозволено цій стороні в цілому отримати доступ до системи, чи ні. Після цього конкретний запит, ініційований стороною, дозволяється або забороняється функцією контролю доступу. Адміністратор мережі або співробітники служби безпеки зазвичай створюють і підтримують базу даних авторизації, що містить інформацію, яка визначає тип доступу, дозволений даному користувачеві. Механізм контролю доступу надає базі даних авторизації право вирішувати, чи дозволити доступ цій стороні . Для захисту сервера ресурсів має бути включений спеціальний сервер

авторизації. Ресурси повинні бути зареєстровані на сервері авторизації сервером реєстрації та мати відповідні політики для користувачів або процесів. Користувач або процес має отримати дозвіл на доступ, надіславши запит на сервер ресурсів. Щоб видати тікет процесу, дозвіл повинен бути зареєстрований сервером ресурсів на сервері авторизації. Потім процес розкриває квиток серверу авторизації для надання дозволу. Якщо сервер авторизації дає дозвіл, процесу видається RPT. Процес може отримати доступ до запитуваного ресурсу, використовуючи RPT.

Звичайні середовища IIoT використовують TTP як проміжне програмне забезпечення для аутентифікації пристроїв перед застосуванням політик контролю доступу. Оскільки використовується TTP, збереження конфіденційності даних є великою проблемою. Крім того, через використання TTP з'являються інші проблеми, такі як SPOF, довіра і вразливості. Тому пристрої IIoT повинні проходити колективну та спільну автентифікацію децентралізовано, наприклад, за допомогою технології блокчейн.

Стійкість і ремонтопридатність визначається ICS у своїй концепції безпеки IIoT як механізм, що розвивається, оснащений системою, яка нормально виконує покладені на неї завдання, навіть якщо вона стикається з несприятливими умовами. Ця система повинна уникати, поглинати і динамічно координувати свої дії, щоб працювати належним чином і виконувати поставлені завдання. Після зараження система повинна бути здатна відновити свої оперативні можливості. Ця термінологія схожа за концепцією з іншими термінами безпеки, такими як надійність, безпека та достовірність. Стійкість є однією з найбільш важливих проблем безпеки в середовищах IIoT [31] . Мережі IIoT повинні забезпечувати певні механізми, які гарантують, що операції в системах IIoT будуть виконуватися нормально, навіть якщо частина системи буде скомпрометована. Це можна зробити в мережах IIoT шляхом перенаправлення деяких поточних завдань із зараженої частини на іншу частину системи або навіть на іншу систему. Цей метод зазвичай називають різноманітністю, надмірністю або зміцненням . Ця концепція застосовується у WSN, в яких розгортається достатня кількість сенсорів для забезпечення надмірності. Такий сценарій має на меті ізолювати скомпрометовані

датчики, коли відбувається зараження, перенаправляючи нові вимірювання на інші датчики в мережі, поки проблема не буде вирішена. Ремонтопридатність можна описати як здатність конфігурувати та оновлювати систему або частину системи. Ця вимога безпеки має вирішальне значення в парадигмі IIoT, оскільки програмне забезпечення в пристроях IIoT повинно мати можливість оновлюватися, щоб бути захищеним від раніше невідомих кібератак. Оновлення програмного забезпечення вважається цінним контрзаходом проти різних загроз, оскільки воно допомагає постійно змінювати конфігурації брандмауерів на кордоні мережі, як тільки IDS виявляє нові загрози. Крім того, вразливості в програмному забезпеченні можна відновити, використовуючи виправлення в регулярних оновленнях програмного забезпечення. Різні пристрої IIoT взаємодіють один з одним та іншими традиційними пристроями через інтернет, який за своєю структурою є незахищеним. Тому регулярне оновлення пристроїв IIoT та виправлення їхніх вразливостей є важливим для підтримки їхньої стійкості до кібератак. Іноді використовують технологію блокчейн для забезпечення безпечних і надійних оновлень для пристроїв IIoT. Є протокол стимулювання, в якому певний агент постачає оновлення і використовує смарт-контракт для створення обіцянки надати фінансовий стимул вузлам, які передають оновлення на пристрої IIoT. Щоб отримати фінансову винагороду, вузли, з якими співпрацюють, повинні надати агенту підтвердження доставки. Вузли, що співпрацюють, повинні використовувати DAPS через підпис на основі атрибутів для здійснення справедливого обміну та отримання підтвердження доставки.

Конфіденційність є важливою вимогою безпеки для приватних осіб, компаній та урядів. У зв'язку зі зростанням попиту на послуги хмарного зберігання даних, збереження конфіденційності стало критично важливим питанням [32]. Сучасні пристрої генерують різні обсяги даних, що робить користувачів вразливими до порушень конфіденційності, коли на основі згенерованих даних можуть бути створені детальні профілі користувачів без їхнього дозволу. Крім того, додатки можуть порушувати конфіденційність, розкриваючи особисту інформацію про звички, пересування та взаємодію користувача з іншими користувачами,

наприклад, місцезнаходження користувача може бути відстежено одним із додатків, які він встановлює на своєму пристрої.

Деякі веб-сайти збирають інформацію про користувачів, таку як попередні відвідування товарів, кошики для покупок і навіть інформацію про кредитні картки. Зібрана інформація може бути передана іншим компаніям без дозволу користувача. Ще однією проблемою є збір даних під час транспортування, який може розкрити особисту інформацію про людей та об'єкти. Надлишковість даних в середовищах IIoT можна вирішити за допомогою механізмів, які зберігають дані в стані спокою. Однак захист конфіденційності та безпека даних є двома основними проблемами для збережених даних. За допомогою деяких методів шифрування, таких як шифрування з можливістю пошуку на основі атрибутів, збережені дані можна зашифрувати та отримати, не порушуючи конфіденційність користувачів.

Моніторинг безпеки поведінки систем забезпечується відомими інструментами, відомими як IDS. Ці інструменти можуть виявляти загрози, спрямовані на мережі, і забезпечувати необхідну процедуру реагування [33]. Для будь-якої мережі, в тому числі і для середовищ IIoT, важливим є моніторинг комунікацій, виявлення загроз та реагування на відомі та невідомі вторгнення. Однією з причин важливості IDS є те, що до мережі можуть підключатися старі та менш захищені пристрої (тобто ті, які важко виправити для усунення відомих вразливостей), що вимагає безперервного моніторингу безпеки. Ці пристрої можуть стати мішенню DDoS-атаки. Потім вони можуть стати частиною ботнету, який може здійснювати атаки на інші легітимні пристрої IIoT в мережі. Захоплення і дослідження обмінюваних даних, мереж і сервісів за допомогою пасивних систем моніторингу та аналізу мережевого трафіку мають першорядне значення для координації мереж і своєчасного виявлення проблем безпеки. IDS можна визначити як інструмент, який контролює мережевий трафік для виявлення атак. IDS може працювати в три етапи. Перший етап відповідає за моніторинг трафіку або даних, що залежить від датчиків на базі хоста або мережі. Другий етап відповідає за аналіз перехопленого мережевого трафіку або зібраних даних. На цьому етапі для виконання завдання використовуються методи вилучення ознак або ідентифікації

шаблонів. Третій етап передбачає виявлення загроз за допомогою двох відомих підходів: виявлення зловживань і виявлення аномалій. Методи виявлення вторгнень на основі зловживань збирають відомі сигнатури і шаблони відомих загроз в базі даних і порівнюють вхідний трафік із записами в базі даних для виявлення атак. Методи виявлення вторгнень на основі зловживань мають недоліки, такі як висока вартість зіставлення сигнатур, збільшення кількості хибних сповіщень та перевантаження мережевих датаграм. Крім того, обмеженість пам'яті пристроїв IIoT ускладнює реалізацію IDS на основі зловживань на цих пристроях через велику кількість записів підписів у базі даних. Також бази даних, призначені для підписів і шаблонів атак, повинні періодично оновлюватися. IDS, засновані на зловживаннях, вимагають попередніх знань, щоб мати можливість ідентифікувати підозрілі дії. Таким чином, невідомі атаки можуть бути не виявлені цим типом IDS. Методи IDS на основі аномалій підтримують ситуацію, в якій справжні пристрої генерують нормальні дані в мережі і відповідно оцінюють відстежувано дані для виявлення аномалій (тобто відхилень, які відрізняються від нормальних даних). Ці відхилення зазвичай генеруються шумом або іншими інцидентами, які можуть бути наслідком використання хакерських інструментів. Таким чином, незвичні дії, що є наслідком існування зловмисників, залишають сліди в зараженій мережі і атаки (в тому числі невідомі) можуть бути виявлені IDS на основі аномалій за цими слідами. Метод IDS на основі аномалій створює шаблон нормальних даних, що генеруються легітимними пристроями в мережі, періодично оновлює цей шаблон, відстежує мережевий трафік в режимі реального часу і порівнює відстежуваний трафік з нормальним шаблоном; якщо існує будь-яке відхилення від нормального шаблону, це може вказувати на зловмисника. Відкрита природа підключення та широке використання пристроїв IIoT роблять їх вразливими до кібератак. Крім того, поширеність і неоднорідність пристроїв IIoT ускладнюють створення централізованого методу виявлення кібератак. Таким чином, пропозиція децентралізованих підходів у безпосередній близькості до середовищ IIoT для виявлення кібератак є життєво важливою.

Безпечний обмін даними. Безпека даних важлива в цифрових парадигмах, в тому числі в IIoT. Однак цілісність і доступність мають кількісно вимірюваний економічний ефект і, отже, вважаються більш важливими, ніж конфіденційність даних в традиційних промислових умовах. Завдяки розвитку ІКС як невід'ємної частини парадигми Інтернету речей, важливість конфіденційності даних стала зрозумілою через взаємодію в ІКС між пристроями та користувачами, які генерують приватні дані [33]. Нові технології, такі як штучний інтелект і периферійні обчислення, надають різні можливості при інтеграції в безпечне середовище IIoT. Однак масштабованість і стійкість периферійних і туманних обчислень пов'язані з різними проблемами безпеки і конфіденційності. Розглянемо деякі можливості та виклики для безпечного розгортання пристроїв IIoT на периферії, включаючи безпечний обмін даними, моніторинг безпеки, аутентифікацію та контроль доступу. Є ідеї щодо того, як можна підвищити безпеку IIoT за допомогою периферійних/туманних обчислень і штучного інтелекту.

По – перше – безпечний обмін даними. Пристрої IIoT генерують величезний обсяг даних в режимі реального часу; таким чином, інтелектуальний аналіз даних дозволяє галузям приймати правильні рішення і неминуче підвищує ефективність виробництва Традиційно дизайн IIoT в основному вертикально забезпечується закритими додатками, які дозволяють промисловості вдосконалювати виробничі процеси на одному майданчику. Таким чином, острови даних - це форми, які необхідно розділити за допомогою периферійних обчислень, щоб підвищити їх гнучкість. Безпечний обмін даними є складним питанням. Обмін даними за допомогою периферійних обчислень стикається з двома ключовими проблемами: обмежена продуктивність периферійних пристроїв, що ускладнює застосування надійних методів безпеки, і неминучі величезні обсяги даних, які можуть призвести до більш серйозних наслідків (наприклад, знищення і кібератаки). Дані, що генеруються пристроями IIoT в периферійних обчисленнях, можуть безпечно обмінюватися за допомогою блокчейну. Вони можуть бути оснащені достатніми обчислювальними (для роботи зі складними методами шифрування) і

накопичувальними можливостями, які дозволяють пристроям IIoT зберігати дані і безпечно обмінюватися ними. Також периферійні обчислювальні вузли можуть бути розподілені близько до пристроїв IIoT, що зменшує пов'язану з ними затримку. Навіть коли з пристроїв IIoT генеруються великі дані, периферійний обчислювальний вузол може виступати в якості сервера для пристроїв IIoT і клієнта для серверів хмарних обчислень, полегшуючи зберігання і обробку даних (периферійний вузол також може прозоро шифрувати або розшифровувати дані, що зберігаються на хмарному сервері). Крім того, оскільки периферійні вузли знаходяться близько до пристроїв IIoT (тобто в одній локальній мережі), дані, що передаються між пристроями IIoT і периферійними вузлами, ніколи не покинуть межі мережі, тому складні механізми шифрування не потрібні. Таким чином, пристрої IIoT будуть вважати, що послуга надається периферійним вузлом, і їм не потрібно знати про відповідні методи безпеки або зберігання даних. Периферійні вузли можуть виступати в якості шлюзів між пристроями IIoT і зовнішніми пристроями, промисловість може захищати і контролювати потік даних на зовнішні пристрої і з них. Створення периферійного вузла дозволяє підтримувати високі стандарти безпеки, здійснювати взаємну аутентифікацію з зовнішніми пристроями і долати обмежену пропускну здатність пристроїв IIoT; отже, пристроям IIoT потрібно обробляти тільки безпечний зв'язок з периферійними вузлами. Крім того, граничний вузол може активувати стратегію потоку даних, щоб отримати доступ до вмісту повідомлення при обробці трафіку, що проходить через нього. Розподілена сервісна природа периферійних і туманних обчислень може призвести до витоку даних, тому необхідно запобігти розголошенню несанкціонованими сторонами збережених або транзитних даних. Тому для захисту переданих даних, що зберігаються в розподілених місцях, від розкриття можна використовувати легкі методи шифрування, такі як криптографічне хешування і гомоморфне шифрування. Зашифровані дані запобігають розголошенню, навіть якщо зловмисник перехоплює дані під час передачі або отримує доступ до захищених даних, що зберігаються на певних серверах. Дані, якими обмінюються між пристроями IIoT або між пристроями IIoT і

периферійними вузлами, повинні передаватися безпечно, щоб зловмисники не змогли модифікувати або змінити дані навіть у разі перехоплення. Системи перевірки криптографічного підпису є важливими методами, які використовуються для забезпечення цілісності даних, що обмінюються. Цілісність даних має першочергове значення для пристроїв IIoT при використанні послуг периферійних обчислень, оскільки в цій ситуації зв'язок між мережевими об'єктами повністю залежить від мережі.

По-друге – це моніторінг безпеки. Платформи периферійних обчислень можуть бути оснащені різними можливостями, щоб задовольнити потреби середовищ IIoT. Таким чином, вони можуть служити потужною системою, здатною відстежувати потенційні загрози безпеці. Периферійний вузол може бути оснащений IDS, здатним зберігати сигнатури відомих атак, таким чином, маючи можливість виявляти вторгнення з перехопленого трафіку на основі цих сигнатур. У випадку, якщо IDS базується на машинному навчанні/глибокому навчанні і для навчання алгоритму машинного навчання необхідно використовувати ряд зразків атак, для навчання алгоритму можна використовувати хмарний сервер, а ваги передавати на периферійний вузол для виявлення вторгнень; таким чином, можна вирішити проблему затримки, пов'язану з хмарними рішеннями. Оскільки датчики передають свої вимірювання безпосередньо на периферійні вузли, вони можуть застосовувати механізми виявлення аномалій, щоб переконатися, що вимірювання знаходяться в прийнятному діапазоні. Може бути розгорнута повна система моніторингу безпеки для моніторингу даних, що проходять через периферійні обчислювальні платформи до і з середовища IIoT, що дозволяє виявляти і стримувати загрози. Також можуть бути вжиті заходи на основі трафіку, що проходить через них, з метою пом'якшення DoS або DDoS-атак, спрямованих на середовища IIoT або інфраструктуру периферійних обчислень. DoS-атаки є однією з основних проблем, що обмежують доступність послуг з авторизованих пристроїв IIoT. Ці проблеми можуть бути частково вирішені за допомогою периферійних/туманних обчислень через розподілену природу обчислювальних ресурсів. Однак DDoS може погіршити роботу авторизованих пристроїв IIoT або

перешкодити їм отримати доступ до цих сервісів. Середовища IIoT можуть розгортати інтелектуальні служби дозволу DNS, WAF та інші інтелектуальні методи моніторингу та фільтрації мережевого трафіку, щоб забезпечити постійну доступність послуг.

По-третє - аутентифікація і контроль доступу. Граничні обчислення можуть бути застосовані для заміни рішень, які потребують сторонніх серверів. Граничний вузол не обмежений в ресурсах і може виконувати складні обчислювальні завдання, отже, має можливість виступати в якості стороннього сервісу для забезпечення пристроїв IIoT необхідним механізмом автентифікації. Однією з переваг периферійних вузлів перед сторонніми серверами є їх локальне розміщення, що забезпечує пристроям IIoT низьку затримку при обміні повідомленнями автентифікації між пристроями та периферійними вузлами. Крім того, периферійний вузол може виступати в якості центру сертифікації для пристроїв IIoT. Таким чином, периферійні вузли можуть формувати однорангову мережу для створення єдиної та потужної ключової інфраструктури. Граничні вузли також можуть слугувати шлюзами, додаючи нові пристрої IIoT, видаляючи існуючі та відповідаючи за повторне введення ключів. Вони також можуть стати заміною такого сервера і можуть бути приєднані до датчиків, діючи як проксі-сервери для сенсорних вимірювань. При цьому масштабованість може бути розширена, оскільки більше вузлів туману може бути розподілено таким чином, щоб вони були доступні для близьких пристроїв IIoT. Таким чином, якщо є нагальна потреба застосувати автентифікацію для оновлення пристроїв за допомогою ключів NFC або біометричних даних, то знадобиться лише вузол туману і його прив'язка до відповідного ключа, а не пошук кожного пристрою, пов'язаного з ключами, незалежно. Подібно до можливостей, пов'язаних з аутентифікацією, контроль доступу може бути покращений при інтеграції з периферійними обчисленнями для авторизації пристроїв IIoT. Пристрої IIoT використовують безпечні та надійні сервіси, що надаються периферійними і туманними обчисленнями.

В четверте - обслуговування та відмовостійкість. Промислові системи можуть отримати вигоду від периферійних обчислень з точки зору

ремонтопридатності. Оскільки більшість важливих промислових систем підключені до Інтернету, це дозволяє швидко керувати програмним забезпеченням та оновлювати його. Однак слід використовувати периферійні обчислювальні пристрої для перевірки достовірності цих оновлень і проведення ретельних тестів. Пристрої периферійних обчислень можуть виступати в якості концентраторів для промислових систем, де промислові пристрої можуть переглядати інформацію про програмне забезпечення, включаючи номер версії та необхідні оновлення, або керувати конфігураційними файлами промислових пристроїв. Оскільки пристрої периферійних обчислень можуть забезпечити легкодоступне місце для зчитування міток NFC або інших модулів автентифікації, поліпшення процедур обслуговування промислових систем і інших факторів автентифікації можливо без необхідності фізичного відвідування кожного пристрою для технічного обслуговування окремо. Граничні вузли здатні відключати та ізолювати скомпрометоване промислове програмне забезпечення. Така практика дозволяє мережевим адміністраторам або співробітникам служби безпеки ретельно перевіряти уражене програмне забезпечення, поки промислові пристрої виконують інші рутинні завдання. Крім того, периферійні обчислення можуть подолати перебої в інтернет-з'єднанні з хмарними сервісами. Периферійні пристрої можуть бути забезпечені зручними процесами, які зазвичай виконуються в хмарі і часто запитуються промисловими системами. Периферійний вузол може надавати послуги, якщо з'єднання з хмарним сервером обривається. Промислові пристрої іноді відправляють дані в хмару для обробки, і тому переривчасте підключення може стати проблемою. Таким чином, периферійний вузол може буферизувати інформацію навіть за відсутності інтернет-з'єднання і передавати буферизовану інформацію, коли інтернет-з'єднання відновлюється. Таким чином, промислові пристрої будуть мінімально зачеплені переривчастим з'єднанням.

Висновок до 2 розділу. В цьому розділі були розглянуті методи захисту промислового IoT. Виклики безпеки були класифіковані за трьома категоріями на основі рівня безпеки IIoT: загрози на рівні додатків, загрози на рівні мережі та

загрози на рівні сприйняття. Кожна атака була пов'язана з вимогою безпеки, яку вона порушує, і загальними контрзаходами, які можна вжити для запобігання атаці. Були розглянуті рішення для виявлення і запобігання цих атак для загального підвищення безпеки IIoT. Крім того, були детально розглянуті виклики, з якими стикаються в сфері IIoT при впровадженні периферійних обчислень. Хоча периферійні обчислення надають різні переваги середовищу IIoT, вони створюють значні витрати для обслуговуючого персоналу. Це може вимагати спеціального навчання для більшої кількості мережевих адміністраторів, що належать до організації, що робить периферійні обчислення дорожчими, ніж хмарні, які можуть підтримуватися експертами на стороні постачальника послуг.

3 РОЗРОБЛЕННЯ ВАРІАНТУ ТЕХНОЛОГІЇ ЗАХИСТУ ПРОМИСЛОВИХ IoT ІЗ ВИКОРИСТАННЯМ CISCO CYBER VISION

3.1. Розроблення варіанту захисту промислових мереж із використанням Cisco Cyber Vision

Глибша інтеграція між IT, хмарними та промисловими мережами робить системи промислового контролю вразливими до кібератак. Коли отримуєш переваги від оцифрування галузі та розгортання технології промислового Інтернету речей (IIoT) важливо мати рішення з кібербезпеки, яке допоможе забезпечити безперервність, стійкість і безпеку промислових операцій [34].

Cisco Cyber Vision було спеціально розроблено для промислових організацій, щоб забезпечити повну видимість їхніх промислових мереж, цілісність процесів, будувати безпечні інфраструктури, відтворювати відповідність нормативним вимогам і впроваджувати політики безпеки для контролю ризиків.

Cisco Cyber Vision поєднує в собі унікальну архітектуру периферійного моніторингу та глибоку інтеграцію з провідним портфелем рішень Cisco для забезпечення безпеки. Вбудоване в промислове мережеве обладнання Cisco може бути легко розгорнуте для моніторингу промислових активів і потоків їхніх додатків у режимі реального часу. Це ідеальне рішення для забезпечення операційного центру IT-безпеки (SOC) з контекстом OT, щоб побудувати уніфіковану архітектуру кібербезпеки IT/OT.

Таблиця 3.1.

Функції та переваги Cisco Cyber Vision

Функції	Переваги
Комплексна видимість	Cyber Vision дає детальну видимість промислових активів в режимі реального часу, їх комунікаційні схеми та потоки додатків.

Продовження таблиці 3.1

Функції і переваги Cisco Cyber Vision

Функції	Переваги
Оперативна інформація	Cyber Vision підтримує операції працювати більш ефективно і з меншим ризиком.
Виявлення вразливостей	Cyber Vision попереджає вас про вразливості обладнання та програмного забезпечення, які необхідно усунути.
Виявлення вторгнень (IDS)	Виявляє загрози кібербезпеці, що надходять IT-мережі. Cyber Vision виявляє відомі та нові загрози.
Виявлення аномалій	Захищає ICS від невідомих атак. Виявляє нелегітимні модифікації промислових активів і процесів, такі як неочікуване завантаження програм або зміни даних.
Гранична архітектура	Легко розгорнути систему безпеки ICS в масштабах. Cyber Vision вбудовано у мережеве обладнання для зменшення витрат на обладнання та мінімального впливу на промислову мережу управління
OT-теги	Можна одразу розуміти, що робить кожен пристрій. Cyber Vision переводить кожен потік додатків у зрозумілі теги, щоб розуміти, що відбуваєтьсяою.
Попередньо встановлені перегляди	Легкий вибір даних за допомогою попередньо встановлених переглядів, які виділяють те, що дійсно важливо.

Продовження таблиці 3.1

Функції і переваги Cisco Cyber Vision

Функції	Переваги
Вигляд мапи	Cyber Vision пропонує кілька типів карт для відображення активів та їхніх комунікацій. Швидко виявляє загрози тааномалії завдяки кольоровому кодуванню.
Глибока перевірка пакетів (DPI)	Відстежує вміст усіх потоків додатків. Cyber Vision "розуміє" протоколи ICS, які використовуються, і тому може профілювати промислові активи і виявляти несправності.
Бортовий самописець OT	Відповідає вимогам відповідності. Cyber Vision зберігає історію всіх подій і потоків додатків, включно зі змінними доступом, щоб легко запускати криміналістичний пошук і створювати звіти про інциденти.
Глибока інтеграція IT-безпеки	Cyber Vision надає платформам IT-безпеки контекст OT, щоб впроваджувати політики безпеки, не зупиняючи виробництво.

Cisco Cyber Vision побудована на дворівневій архітектурі, що складається з декількох сенсорних пристроїв, які виконують глибоку перевірку пакетів, аналіз протоколів і виявлення вторгнень на периферії, аналітику, поведінковий аналіз, звітність. Він може працювати на апаратному пристрої або, як віртуальна машина VMware, а датчик працює на промисловому обчислювальному шлюзі Cisco IC3000.

Таблиця 3.2.

Платформи для продуктів Cyber Vision

Компоненти продукту	Підтримувані платформи
Апаратний прилад Cyber Vision Sensor	Cisco IC3000 Industrial Compute
Апаратне обладнання Cisco Cyber Vision	Cisco UCS® C220 M5 Rack Server
Програмне забезпечення Cisco Cyber Vision	VMware ESXi 6.x or later

Архітектура периферійних обчислень Cisco Cyber Vision вбудовує компоненти моніторингу безпеки в промислове мережеве обладнання, як показано на рисунку 3.1.[35] Більше не потрібно купувати спеціальні пристрої, не потрібно будувати велику мережу, щоб надсилати потоки промислової мережі на центральну платформу безпеки. Cyber Vision дозволяє промисловій мережі збирати інформацію, необхідну для забезпечення комплексної видимості, аналітики та виявлення загроз, має унікальну простоту і низьку вартість.

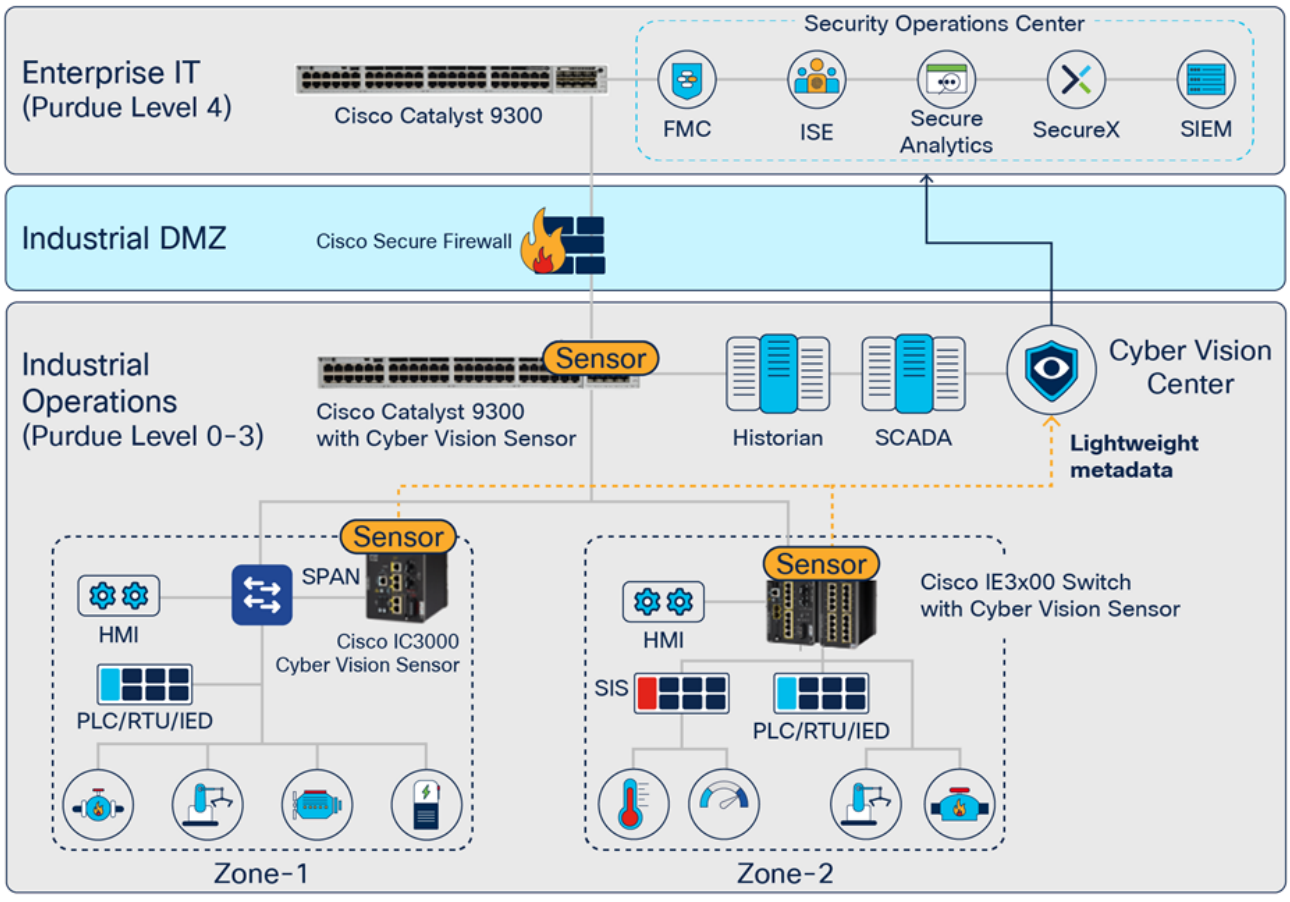

Рисунок 3.1. Мережеві датчики Cyber Vision

Cyber Vision використовує пасивні та активні механізми виявлення, щоб ідентифікувати всі активи, їхні характеристики та зв'язки. Запити активного виявлення є надзвичайно точними і непорушними. Вони використовують семантику використовуваних протоколів, щоб зібрати детальну інформацію про всі промислові активи, включаючи системи на базі Windows. Оскільки запити ініціюються з датчиків Cyber Vision, вбудованих в мережеве обладнання Cisco, що формує промислову мережу, вони не блокуються брандмауерами або межами NAT, що забезпечує всеосяжну видимість.

До цієї величезної кількості інформації про активи, карти комунікацій, оперативні події та події безпеки можуть отримати доступ місцеві співробітники відділів експлуатації та IT-команди. Вона також може бути задіяна в Глобальному центрі кібервізії, що дозволяє великим організаціям отримати глобальну видимість на всіх об'єктах і сприяти управлінню і дотриманню нормативних вимог.

Cisco Cyber Vision автоматично виявляє найдрібніші деталі виробничої інфраструктури: посилання на постачальників, версії прошивки та обладнання, серійні номери, конфігурацію слотів у стійці тощо. Він визначає взаємозв'язки між активами, схеми зв'язку тощо. Інформація відображається в різних типах карт, таблиць і звітів. Cisco Cyber Vision дає інженерам OT в режимі реального часу уявлення про фактичний стан промислових процесів, таких як несподівані зміни показників або модифікації контролерів, щоб вони могли швидко вирішувати виробничі проблеми і підтримувати безперебійну роботу. Кібер-експерти можуть легко зануритися в усі ці дані, щоб розслідувати події, пов'язані з безпекою. Керівники служб інформаційної безпеки мають всю необхідну інформацію для документування звітів про інциденти та забезпечення дотримання нормативних вимог. Продукт використовує теги для виділення ролей активів і контекстів зв'язку, щоб будь-який член команди OT і IT-команди міг легко зрозуміти промислову інфраструктуру і операційні події, незалежно від бренду активу або посилань на нього.

Детальна інвентаризація активів і видимість подій, пов'язаних з операційною діяльністю, надають цінність як для операційних команд, так і для команд IT-

безпеки. Готові інтеграції з портфелем рішень безпеки Cisco, а також з широким набором рішень сторонніх виробників розширюють можливості Cyber Vision для моніторингу ризиків і дотримання нормативних вимог, звітності, впровадження політики безпеки та багато іншого.

Cyber Vision легко інтегрується з провідними SIEM-системами, такими як IBM QRadar або SPLUNK, тому аналітики з безпеки можуть відстежувати промислові події в своїх існуючих інструментах і починати співвідносити події OT/IT. Використовуючи багатий API Cyber Vision, IT- та OT-команди можуть забезпечити будь-який існуючий інструмент глибокими знаннями про промислові активи, мережевий трафік і стан безпеки.

3.2. Технології виявлення і усунення загроз за допомогою Cisco Cyber Vision

У традиційному IT-світі ризик включає в себе загрози, які можуть підірвати конфіденційність, цілісність та доступність даних і систем. Вплив переважно фінансовий, наприклад, випадки вимагання (вірус Cryptolocker), банківське шахрайство або атаки на відмову в обслуговуванні, що поширюються на веб-сервери, які використовуються сайтами електронної комерції.

Промислові системи управління керують фізичним світом, де використовуються операційні технології. Ризик в середовищах ICS включає в себе загрози, які можуть підірвати операційну безпеку (фізичну безпеку товарів і людей, вплив на навколишнє середовище), а також доступність або навіть фізичну цілісність виробничого інструменту. Також існує загроза крадіжки критично важливих промислових даних. Наслідки мають не лише економічний, але й соціальний характер; цивільна та кримінальна відповідальність керівників.

Розглянемо конкретні та ідентифіковані вектори загроз.

На відміну від споживчих мереж, в яких основні вектори загроз пов'язані з Інтернет, в ICS існує побоювання, що шкідливі програми будуть вставлятися через USB-носії або шляхом бічного переміщення шкідливого програмного забезпечення до станцій які пілотують ICS.

Дистанційна діагностика і дистанційне обслуговування вимагають віддаленого доступу до мереж і промислових систем управління. Віддалений доступ є ще більш серйозним вектором загрози, оскільки він об'єднує мережі різної критичності, а іноді й за участю третіх осіб. Робочі станції віддаленого доступу підключаються до серця критично важливих промислових систем управління для виконання операцій, які можуть мати значний вплив (наприклад, оновлення програмного забезпечення або завантаження нової прошивки). Їх не можна просто заборонити, але вони повинні контролюватися ефективними механізмами моніторингу.

Промислові системи управління ніколи не були розроблені для боротьби з загрозами кібербезпеки. Вони створюються з метою забезпечення операційної безпеки та безперебойної роботи, і вони часто не не враховують можливість того, що мотивований зловмисник може досягти їхніх цифрових інтерфейсів. В більшості випадків функції кібербезпеки не активуються промисловими операторами. Промислові системи побудовані на наборі протоколів, які дозволяють обмінюватися комунікацій між компонентами в мережах. Існують деякі стандарти, такі як MODBUS або PROFINET, але протоколи для перепрограмування або модифікації систем керування здебільшого є приватними і закриті. Більшість з них (Siemens, Schneider, ABB, Rockwell Automation та ін.) не планують відкривати свої протоколи з законних причин, пов'язаних з інтелектуальною власністю. Застосування таких IT-технологій, як протокол, не є можливим.

Для побудови ефективної стратегії кібербезпеки ICS дуже важливо визначити події безпеки, які є найбільш вірогідними. Це дозволить зосередитися на

впровадженні відповідних заходів для захисту активів, які є найбільш вразливими і підвищити безпеку чутливих активів, які зловмисник може використати для проникнення в систему Інтернетом або електронною поштою. Особливо важливо розуміти, як зловмисник буде зламувати промислову мережу своєї цілі. Існує багато вразливих місць, які слід враховувати при розробці процесу моніторингу. Вони поділяються на такі групи:

Захоплення промислової станції. Зловмисник використовує цільові IT-механізми розповсюдження щкідливого програмного забезпечення в цільовій мережі, поки воно не досягне робочої станції в промисловому домені. Основними цілями є системи диспетчерського контролю та збору даних (SCADA) та інженерні станції, оскільки вони містять важливу інформацію про процес.

Підміна авторизованого віддаленого доступу для третьої сторони. Зловмисник використовує авторизований віддалений доступ для третьої сторони, наприклад, субпідрядника. Це може бути ADSL або VPN-з'єднання, залишене відкритим або використовуване лише для певних IP-адрес. Такий віддалений доступ часто надає доступ до самого серця промислового об'єкта, забезпечуючи вхід для зловмисника.

Перехоплення бездротового з'єднання. Зловмисник використовує загальнодоступну або власну вразливість бездротового з'єднання. Таким чином він може підключитися до промислової мережі управління. Після цього він отримує прямий доступ до серця системи на інженерних станціях.

Отримання доступу до польової мережі об'єкта. Зловмисник має прямий фізичний доступ до польової мережі об'єкта, мережу для своєї атаки, наприклад, маючи доступ до комп'ютерної шафи вздовж розподільчої осі. Польова мережа дає прямий доступ до обладнання ICS, яке використовується для управління модулями вводу/виводу. Це особливо важливо в транспортному секторі.

Встановлення стороннього фізичного компонента для модифікації

віддалено модифікувати мережу. Щоб скористатися своїм фізичним доступом без необхідності бути фізично присутнім в компрометуючому місці, зловмисник встановить у промислову мережу модуль дистанційного керування: наприклад, мініатюрний Raspberry Pi з акумулятором і 4G-модемом, що дає змогу дистанційно керувати системою. Мотивами зловмисника можуть бути кібертероризм, конкурентне позиціонування або навіть акт війни між двома країнами.

Після того, як зловмисник отримав доступ до програм контролера, він модифікує їх і повторно вводить їх у контролери, щоб впливати на промисловий процес. Можна також діяти безпосередньо на значення змінних або модифікувати програмне забезпечення, що взаємодіє з промисловим обладнанням. Промислові мережі управління часто є географічно розгалуженими і складаються з багатьох "малих мереж" з невеликою кількістю компонентів. Щоб контролювати все це без розгортання складної і дорогої інфраструктури, система виявлення зазвичай складається з:

- Датчиків, які розташовані близько до процесу, які витягують дані зв'язку між пристроями;

- Центрального сервера, який збирає, зберігає та аналізує зібрані дані за допомогою датчиків;

Для того, щоб покрити вищезгадані ризики, система виявлення аналізує

властивості компонентів, контрольні повідомлення та різні маркери:

- Ідентифікаційні властивості: MAC-адреса, ідентифікатор протоколу, TCP-порт, UDP-порт

- Інвентарні властивості: назва виробника, назва ПЛК, назва проекту, версія проекту, назва моделі, версія мікропрограми, версія апаратного забезпечення, апаратне забезпечення серійний номер, розташування / слот субмодуля, код продукту, компонент роль (SCADA, інжиніринг)

- Просте керування контролерами/ПЛК: завантаження програм з/до ПЛК, команди зупинки/запуску, зміни годинника, оновлення прошивки

- Розширені контролери / управління ПЛК: моніторинг вмісту програм ПЛК програм, метаданих програм (список програмних блоків, мітка часу, розмір), дані аутентифікації (логін і паролі), зміна залишкових бази даних, стирання пам'яті, перехід в режим обслуговування, перехід в режим діагностики

- Керування процесом: команди запису та читання, список змінних/регістрів - Індикатори компрометації (IOK): DNS-запити, зроблені промисловими станціями, або метаданими HTTP чи FTP; ці IoC можуть вказувати на діяльність командного сервера, що взаємодіє зі зловмисним програмним забезпеченням встановлених на промислових станціях.

Важливо розуміти, що так зване "просте управління контролером" надає зловмисникам безліч можливостей. Необхідно знати, як виявляти ці команди на мережу. Щоб отримати інформацію, необхідну для моніторингу кібербезпеки промислової системи, платформі потрібно декодувати потоки додатків, зібрані в мережі. Ці потоки можуть використовувати кілька типів мережевих протоколи:

- відкриті протоколи, специфікації яких відомі та доступні. Ці протоколи були стандартизовані міжнародними організаціями.

- власні розширення відкритих протоколів. Ці розширення використовують відкриту область даних і включають власні, недокументовані дані структури.

- протоколи, специфікації яких не є загальнодоступними.

Cisco Cyber Vision поєднує в собі аналіз протоколів, виявлення вторгнень, виявлення вразливостей і поведінковий аналіз, щоб допомогти зрозуміти стан системи безпеки. Він автоматично розраховує оцінки ризиків для кожного компонента, пристрою та будь-якої конкретної частини операцій, щоб виділити критичні проблеми, визначити пріоритети, які потрібно виправити. Кожна оцінка супроводжується рекомендаціями, як зменшити вразливість, щоб діяти на випередження і побудувати процес вдосконалення для усунення ризиків.Cisco

Cyber Vision була спеціально розроблена для промислових організацій, щоб отримати повну видимість своїх промислових мереж, щоб вони могли забезпечити цілісність процесів, створювати безпечні інфраструктури, забезпечувати відповідність нормативним вимогам, і впроваджувати політики безпеки для контролю ризиків. Поєднання унікальної архітектури периферійного моніторингу та глибоку інтеграцію з провідним портфоліо рішень Cisco для забезпечення безпеки, Cisco Cyber Vision можна легко розгортати в масштабі.

Механізм виявлення Cyber Vision використовує дані про загрози від Cisco Talos, однієї з провідних світових дослідницьких команд з кібербезпеки та офіційного розробника сигнатурних файлів Snort. База знань про загрози Cyber Vision оновлюється щотижня, включаючи найновіші списки вразливостей активів та сигнатур IDS.

Cisco Cyber Vision - рішення, яке не вимагає придбання додаткових пристроїв або створення нових мереж. Промислове середовище все частіше підключається до IT-інфраструктур, Інтернету та хмарних технологій, а оперативні команди потребують інформації, яку надає обладнання. Однак доступ до даних у режимі реального часу вважається фактором ризику для компаній у виробничій сфері, енергетичних операторів, постачальників комунальних послуг тощо.

Розглянемо фактори ризику в промисловому середовищі

Неоднорідність інфраструктури. Промислові мережі постійно розвиваються, і через кілька років експлуатації вони стають конгломератом старого обладнання та IoT-рішень від різних виробників.

Низька видимість. Небагато компаній сьогодні володіють детальною інформацією про все обладнання, що входить до складу промислових мереж, і знають, які пристрої взаємодіють один з одним.

Труднощі з виявленням атак. Технології автоматизації та захисту відносно старі і не відповідають сучасним вимогам, а промислові системи управління (PLC, RTU, IED, DCS тощо) використовують протоколи, які не розуміють IT-рішення з безпеки.

Брак комунікації між IT та операційними відділами. Часто ці дві команди не розмовляють однією мовою і мають різні пріоритети, працюють окремо, з наборами даних, які не мають спільного доступу.

Такі обмеження є поширеними, особливо у випадку, коли в інфраструктурі є 10-20-річне обладнання працює разом з рішеннями автоматизації та управління на основі IP-технологій нового покоління на периферійних ділянках мережі. Cisco випустила Cyber Vision - рішення безпеки, спеціально розроблене для забезпечення безперервності процесів і безпеки даних з дотриманням існуючих вимог. Основною конкурентною перевагою Cisco Cyber Vision є те, що воно аналізує локальний прямий трафік в мережевому обладнанні.

Інтеграція технології глибокого аналізу пакетів в обладнання Cisco вигідна для IT-відділів. Вони можуть захистити мережу без необхідності купувати, встановлювати, налаштовувати, керувати та обслуговувати інші пристрої. У той же час, це плюс для операційних команд, оскільки розширена видимість дозволяє їм активно втручатися в усунення ризиків.

Як працює Cyber Vision для усунення загрози кібератаки.

Автоматично виявляє та ідентифікує обладнання в промисловій мережі. Cyber Vision створює реєстр підключених пристроїв, надаючи інформацію про модель, версію прошивки, конфігурацію, потенційні вразливості тощо.

Складає комунікаційну карту. Визначає взаємозв'язки між мережевим обладнанням і моделями зв'язку між ними. Cyber Vision переводить згенеровані потоки даних в систему тегів, що дозволяє швидко розібратися в ситуації без необхідності глибоких знань в області комунікаційних протоколів.

Виявляє загрози. Збирає та корегує дані про трафік і виконує контекстний аналіз, що дозволяє виявляти аномалії, які можуть сигналізувати про потенційну атаку. Рішення створює на основі історичних даних з використанням технологій AI та ML еталонну модель мережі та дозволяє налаштовувати правила та оповіщення.

Надає корисну інформацію. Рішення Cisco відстежує зміни конфігурації, фіксує події в області систем управління та надає корисні рекомендації щодо усунення потенційних ризиків.

Спрощує процес аудиту. Cyber Vision автоматично генерує докладні звіти, які допомагають організаціям проводити аудит на відповідність чинним нормам. Для того, щоб розширити захист на багаторівневому рівні, Cisco Cyber Vision інтегрується з усім портфелем рішень безпеки Cisco, а також з додатками сторонніх виробників за допомогою API-інтерфейсів.

3.3. Розроблення рекомендацій щодо застосування Cisco Cyber Vision у промислових мережах

Розгортання кібербезпеки ОТ може швидко стати дуже складним, особливо якщо промислова мережа розкидана по всій країні або має багато віддалених промислових об'єктів. Для того, щоб проєкт кібербезпеки ОТ був успішним, треба мати можливість легко і за розумну ціну розгоргути його в масштабах всієї організації [36]. Cisco Cyber Vision використовує унікальну архітектуру периферійних обчислень, яка дозволяє здійснювати моніторинг безпеки на промисловому мережевому обладнанні Cisco. Не потрібно купувати окремі пристрої та думати про те, як їх встановити. Захист інфраструктури ОТ починається з отримання точного уявлення про інвентаризацію активів, схеми зв'язку і топології мережі. Cisco Cyber Vision надає командам ОТ і мережевим менеджерам повну видимість у свої активи та потоки додатків, щоб вони могли впроваджувати найкращі практики безпеки, керувати проектами сегментації мережі та підвищувати операційну стійкість. Cisco Cyber Vision автоматично виявляє найдрібніші деталі виробничої інфраструктури: посилання на постачальників, версії прошивки та обладнання, серійні номери, конфігурацію слотів для ПЛК в стійці тощо. Він визначає взаємозв'язки між активами, схеми зв'язку, зміни показників і багато іншого. Це багатство інформації відображається в різних типах карт, таблиць і звітів, які підтримують повну інвентаризацію у промислових активах, їхні взаємовідносини, вразливості та програми, які вони виконують.

Оперативна інформація Cisco Cyber Vision дає інженерам з експлуатації в режимі реального часу уявлення про те, що відбувається на об'єктах, про фактичний стан промислових процесів, таких як несподівані зміни показників або модифікації контролерів, щоб вони могли вжити заходи для підтримки цілісності системи і безперервності виробництва. Кібер-експерти можуть легко зануритися в усі ці дані, щоб проаналізувати атаки і знайти їх джерело. Керівники служб інформаційної безпеки мають всю необхідну інформацію для документування своїх звітів про інциденти. Cisco Cyber Vision "розуміє" власні протоколи OT, що використовуються обладнанням для автоматизації, тому може відстежувати аномалії процесів, помилки, неправильні конфігурації та несанкціоновані промислові події. Вона також реєструє ці події, стаючи "бортовим самописцем" промислової інфраструктури. Продукт використовує теги для виділення ролей активів і контекстів зв'язку, так що будь-який член команди OT та IT-спеціалістів може легко зрозуміти промислову інфраструктуру та операційні події, незалежно від бренду або посилань. Після цього IT-команди можуть співпрацювати з персоналом OT, щоб впроваджувати найкращі практики, такі як виправлення вразливих активів, відстеження стандартних вразливих активів, відстеження використання паролів за замовчуванням, покращення сегментації мережі тощо.

Промислові мережі все більше пов'язані з IT-мережами, їх захист від звичайних IT-загроз, таких як шкідливе програмне забезпечення або вторгнення, стає все більш важливим. А оскільки атаки на промислові мережі зазвичай виглядають як легітимні інструкції до активів, потрібно виявляти ці небажані модифікації процесів. Щоб захистити промислову мережу, потрібні різноманітні механізми виявлення загроз. Cisco Cyber Vision поєднує в собі аналіз протоколів, виявлення вторгнень і поведінковий аналіз для виявлення будь-якої атаки. Такий комплексний підхід допомагає гарантувати, що Cyber Vision може виявляти як відомі, так і невідомі атаки, а також зловмисну поведінку, яка може бути попереджувальною ознакою атаки. Cyber Vision інтегрується з IT SOC, щоб аналітики з безпеки могли відстежувати промислові події в своїх системах управління інформацією про безпеку та подіями (SIEM).

Головна перевага Cisco Cyber Vision - видимості безпеки. Прозорість системи безпеки є ключовим компонентом загального підходу до кібербезпеки для промислової автоматизації та управління. Це дозволяє виробникам краще розуміти ризики у виробничому середовищі та керувати ними, допомагаючи їм:

- розвинути відчуття ризику безпеки шляхом ідентифікації активів і пристроїв, підключених до мережі, і їх стану безпеки шляхом порівняння з відомими ризиками до мережі, а також їх стан безпеки, порівнюючи з відомими ризиками та загрозами:

- розвинути глибоке розуміння промислових комунікаційних потоків у виробничій системі, на основі яких може бути розроблена політика безпеки. Моніторинг підключених активів і комунікаційних потоків на предмет змін або аномалій, які можуть свідчити про компрометацію.

- створити інвентаризації активів у вашій промисловій мережі в режимі реального часу.

- підвищити операційну ефективність, побачивши актуальний стан зв'язку між активами, що допомагає швидше вирішувати проблеми.

- Інтегрувати виробниче середовище в процеси і процедури безпеки підприємства, що полегшує управління ризиками в корпоративних процесах та процедурі безпеки.

- Розгорнути та експлуатувати в масштабі і з мінімальними витратами завдяки використанню мережі.

Виявлення ризикованих активів і пристроїв дозволяє виробникам визначати пріоритети оновлення під час вікон технічного обслуговування. Розуміння комунікаційних потоків дозволяє розробляти і розгортати політики безпеки, які додатково захищають системи промислової автоматизації від загроз. Здатність виявляти зміни або аномалії в комунікаціях допомагає швидко ідентифікувати загрози, щоб можна було вжити відповідних заходів реагування.

Ці переваги допомагають підтримувати безперебійність виробництва, безпеку продукції та працівників і зменшити витрати, коли вони все ж таки трапляються. Випадки використання видимості безпеки:

- Видимість активів
- Стан безпеки
- Оперативна інформація
- Виявлення вторгнень

Видимість активів. Cisco Cyber Vision використовує унікальну комбінацію пасивного і активного виявлення для ідентифікування всіх активів, їх характеристики та комунікації. Cisco Cyber Vision дозволяє промисловій мережі збирати інформацію, необхідну для забезпечення комплексної видимості, аналітики та виявлення загроз.

Стан безпеки. Cisco Cyber Vision поєднує в собі аналіз протоколів, виявлення вторгнень, вразливостей виявлення та поведінковий аналіз, для забезпечення системи безпеки. Він автоматично розраховує оцінки ризиків для кожного компонента, пристрою та будь-якої конкретної частини операцій, щоб виділити критичні проблеми і можна було визначити пріоритетність того, що потрібно виправити. Кожна оцінка супроводжується рекомендаціями, як зменшити вразливість, щоб діяти на випередження і побудувати процес вдосконалення для усунення ризиків.

Оперативна інформація. Cisco Cyber Vision автоматично виявляє найдрібніші деталі виробничої інфраструктури. Про фактичний стан зв'язку промислових процесів, наприклад, про те, що трафік вводу/виводу зупинився або нещодавно були виконані модифікації контролера, так що виробничий персонал міг швидко вирішувати проблеми та підтримувати безперебійну роботу. Кібер-експерти можуть легко зануритися у всі ці дані і розслідувати події, пов'язані з безпекою. Керівники служби інформаційної безпеки мають всю необхідну інформацію для

документування звітів про інциденти та дотримання нормативних вимог виявлення вторгнень.

Cisco Cyber Vision інтегрує систему виявлення вторгнень (IDS) Snort в деякі платформи, використовуючи правила підписки Talos для виявлення відомих і нових загроз, таких як зловмисне програмне забезпечення або шкідливий трафік. (рисунок 3.2)

Датчики вторгнень - це системи, які виявляють активність, що може скомпрометувати конфіденційність, цілісність або доступність (CIA) інформаційних ресурсів, обробки, або систем. Система виявлення вторгнень (IDS) може аналізувати трафік від канального до прикладного рівня, щоб виявити такі речі, як мережеві атаки, наявність шкідливого програмного забезпечення та неправильну конфігурацію сервера. Система запобігання вторгненням (IPS) може виявляти, зупиняти та блокувати атаки. Перевага розгортання IDS над IPS полягає в тому, що вони не створюють ризику виведення з ладу IACS. Ця перевага може бути пов'язана з "хибними спрацьовуваннями", коли IDS або IPS виявляє стан, який, на їхню думку, є аномалією або атакою, тоді як насправді це критично важливий для бізнесу трафік. Оскільки системи IDS, як правило, не є вбудованими, вони не мають ніякого впливу на статистику продуктивності мережі, таку як затримка поширення і коливання затримки. Інший ризик рішень IPS полягає в тому, що катастрофічний збій системи IPS може призвести до повної відсутності зв'язку. Рекомендується, щоб мережі OT використовували гібридне розгортання IDS/IPS.

Візуалізація безпеки є критично важливим фактором для корпоративних мереж з часів широкого впровадження стандартних мереж. IT-стандарти, інструменти та додатки були розроблені для моніторингу, дослідження та оцінки мережевого зв'язку в корпоративних системах. Ці інструменти та можливості мають відношення до систем заводу - особливо там, де IT-сервери працюють під управлінням додатків commonOS (наприклад, MS Windows). Вони ідентифікують пристрої в мережі. Системи промислової автоматизації та управління, системи OT,

містять різні пристрої працюють за протоколами, які не зустрічаються в IT-мережах, і мають суттєво відмінні комунікаційні потоки.

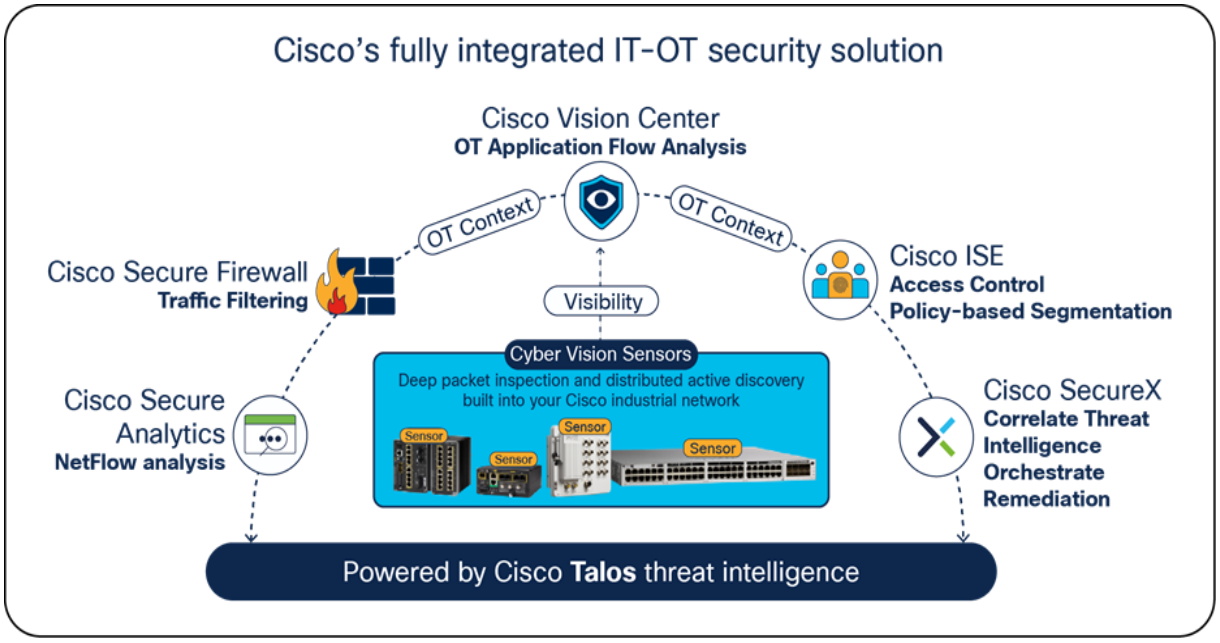

Рисунок 3.2. Інтегроване рішення Cisco для захисту IT-OT

Тому потрібні інструменти, які розуміють пристрої IACS та їх зв'язок.

Забезпечення видимості безпеки OT за допомогою Cisco Cyber Vision. Візуалізація безпеки працює завдяки інструментам промислової кібербезпеки, що забезпечують видимість безпеки, по суті, збирають глибокий аналіз пакетів (Deep Packet Inspection, DPI), контролюють трафік. На основі цього аналізу вони можуть визначити деталі того, що підключено до мережі, які пристрої або програми взаємодіють з кожним з них, а також те, що вони повідомляють.

Візуалізація безпеки – це видимість активів, стан безпеки, оперативна інформація та виявлення вторгнень. DPI дозволяє збирати інформацію про пристрої, таку як модель, бренд, номери деталей, серійні номери, версії мікропрограми та апаратного забезпечення, конфігурації слотів у стійці та іншу інформацію, щоб надати інформацію про підключені ресурси. На основі знання відомих ризиків і загроз можна оцінити стан безпеки. DPI декодує всі комунікаційні потоки і витягує вміст повідомлень і заголовки пакетів, забезпечуючи видимість шаблонів зв'язку для оперативного аналізу та підґрунтя для створення політик

безпеки для їх захисту. Це дозволяє зрозуміти, що передається через мережу. Наприклад, можна побачити, чи намагається хтось завантажити нову прошивку на пристрій або змінити параметри, що використовуються для запуску промислового процесу. Щоб досягти повної видимості, необхідно перевіряти весь мережевий трафік. В промисловій мережі більша частина трафіку відбувається в межах зони Cell/Area, тому що саме там розміщені контролери, датчики і виконавчі пристрої. Відносно невеликий трафік надходить до додатків рівня сайту або виробництва.

При зборі мережевих пакетів для виконання DPI постачальники рішень безпеки зазвичай налаштовують SPAN-порти на мережевих комутаторах і використовують одну з трьох архітектур:

- Надсилати весь трафік на центральний сервер, який виконує DPI.

-Розгортання спеціальних сенсорних пристроїв на кожному комутаторі промислової мережі.

- Надсилання трафіку на спеціальні сенсорні пристрої, розгорнуті в різних точках мережі.

Хоча ці підходи забезпечують прозорість мережі, вони також створюють нові проблеми. Налаштування мережевих комутаторів для відправки трафіку на центральний сервер вимагає дублювання мережевих потоків. Для транспортування цього додаткового трафіку, як правило, потрібна нова позасмугова мережа, що може бути складно і дорого. Це може бути прийнятним для невеликого промислового об'єкта, вартість розгортання такої "телеметричної" мережі на більшості об'єктів коштує дорожче, ніж сама виробнича мережа. Підключення сенсорних пристроїв до мережевих комутаторів вирішує проблеми, пов'язані з дублюванням мережевого трафіку в існуючих або нових "телеметричних" мережах. Прилад збирає та аналізує мережевий трафік локально і лише надсилає телеметричні дані на сервер для додаткового аналізу та зберігання. Встановлення, управління та обслуговування спеціального обладнання призводить до проблем з вартістю та масштабуванням. Оскільки більшість промислового трафіку є

локальним, отримання повної видимості вимагає розгортання приладів на кожному комутаторі мережі, що ускладнює процес масштабування мережі. Чим більше трафіку в мережі, тим повільніше вона працює, що призводить до перевантажень, підвищеної затримки і/або джиттера - часто неприйнятного компромісу в промислових мережах, де процеси повинні працювати швидше, а машини повинні бути своєчасно синхронізовані.

Кращий спосіб досягти повної видимості мережі - вбудувати можливості DPI (датчики) в існуюче мережеве обладнання. Комутатор промислового класу з вбудованою підтримкою DPI усуває необхідність дублювати мережеві потоки і розгортати додаткові пристрої.

Отримання функцій видимості і безпеки - це просто питання активації функції на мережевому комутаторі, маршрутизаторі або шлюзі. Комутатор з підтримкою DPI аналізує трафік локально, щоб витягти значущу інформацію. Він лише надсилає легкі метадані на центральний сервер, який виконує аналітику та виявляє аномалії. Трафік настільки легкий, що може передаватися через промислову мережу, не викликаючи перевантажень і не вимагаючи додаткової пропускної здатності. Вбудовування DPI в мережеве обладнання надає як IT, так і OT унікальні переваги. IT-спеціалісти можуть використовувати існуючу мережеву інфраструктуру для захисту промислових операцій без необхідності шукати, розгортати та керувати додатковим обладнанням. Оскільки ці мережеві елементи бачать весь промисловий трафік, вбудовані датчики можуть забезпечити аналітичну інформацію про кожен компонент промислових систем управління. В результаті, OT може отримати доступ до інформації про операції, якої раніше ніколи не мала.

Активне виявлення. Повне виявлення активів важливо для мереж IACS, щоб отримати розуміння всіх пристроїв в мережі і пов'язаних з ними ризиків безпеки. Щоб пасивне виявлення було ефективним, розміщення датчиків має важливе значення. Отримання повної картини вимагає часу і може бути визначено лише на основі інформації, яка передається об'єктом. Активне виявлення - це механізм

отримання інформації про об'єкт на вимогу. Воно працює шляхом надсилання точних і непорушних запитів у семантиці специфічних протоколів IACS. Постачальників IACS розробили дійсні команди протоколу, що підтримуються промисловими активами. Ці команди схожі на управління активами і не завдають шкоди.

Вразливості та ризики промислових пристроїв зазвичай імпортуються за допомогою інструменту ICS (Cyber Vision) і порівнюються з виявленими активами. Вразливість - це слабке місце в системі або її дизайні. Вразливості іноді можна знайти в самих протоколах.

Загроза - це будь-яка потенційна небезпека для активів. Загроза реалізується, коли хтось або щось виявляє певну вразливість і використовує її, створюючи вразливість. Якщо вразливість існує теоретично, але ще не була використана, загроза є латентною і не була реалізована. Суб'єкт, який використовує вразливість, відомий як агент загрози або вектор загрози. Контрзахід - це засіб захисту, який зменшує потенційний ризик. Контрзахід зменшує ризик, усуваючи або зменшуючи вразливість, або зменшуючи ймовірність того, що агент загрози може успішно використати ризик. Ризик - це функція ймовірності того, що певне джерело загрози скористається певною потенційної вразливості, і, як наслідок, впливу цієї несприятливої події на Cisco Cyber Vision Center - це центральна платформа, яка збирає дані з усіх периферійних Sensors і виступає в якості платформи моніторингу, виявлення та управління. Він може бути розгорнутий як програмний або апаратний пристрій в залежності від вимог мережі. Для розгортань, з якими не впорається один екземпляр Cisco Cyber Vision, або для організацій, які бажають об'єднати кілька сайтів в один глобальний центр Cisco Cyber Vision може об'єднувати до 20 локальних центрів Cisco Cyber Vision. Cisco Cyber Vision Global Center використовується для моніторингу безпеки на декількох об'єктах, надаючи консолідоване уявлення про компоненти, вразливості і подій, як показано на рис.3.3.

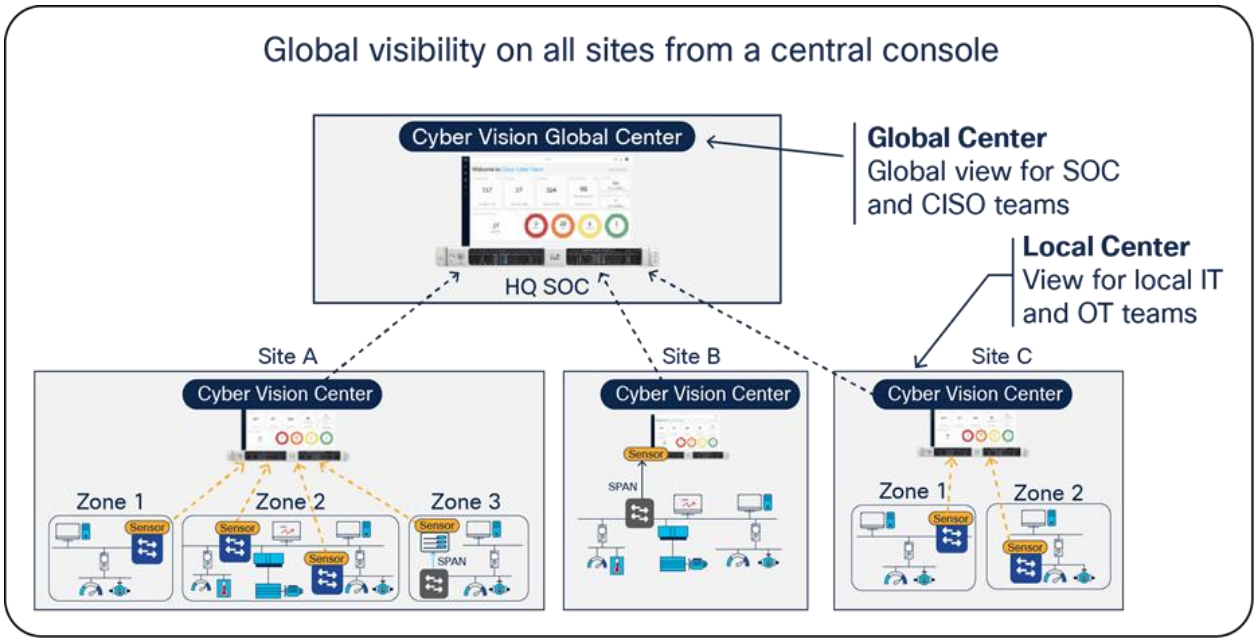

Рисунок 3.3. Cyber Vision та периферійна архітектура

Датчики Cisco Cyber Vision вбудовуються в певне мережеве обладнання Cisco/Stratix. Ці датчики пасивно захоплюють і декодують мережевий трафік, використовуючи DPI промислових протоколів управління. Оскільки датчики Cisco Cyber Vision декодують трафік промислових мереж на кордоні, вони відправляють тільки легкі метадані в центр Cisco Cyber Vision, додаючи лише 2-5% навантаження на промислову мережу. Датчики Cisco Cyber Vision також мають можливість активного виявлення. Ці активні запити на виявлення надходять від датчика, глибоко в мережу IACS, тому ці повідомлення не блокуються брандмауерами і надходять за межами мережі. Cyber Vision Center може працювати без будь-якого з'єднання з промисловою зоною.

Висновок до 3 розділу. В цьому розділі було розглянуто захист промислових IoT за допомогою Cisco Cyber Vision, який забезпечує безпрецедентний масштаб і простоту промислової безпеки. Дає рішення з кібербезпеки, яке допоможе забезпечити безперервність, стійкість і безпеку промислових операцій. Cisco Cyber Vision надає власникам активів повну видимість своїх промислових мереж і їх безпеки OT. Розширені можливості моніторингу OT надають інформацію для

підвищення ефективності мережі та пришвидшують усунення несправностей операційних проблем. Поєднання унікальної периферійної архітектури, яка впроваджує OT функції безпеки в промислову мережу. Cyber Vision можна легко розгортати в масштабі, щоб дати можливість IT- і OT-командам працювати разом над створенням інноваційних промислових операцій, забезпечуючи при цьому безпеку глобального підприємства. Cisco Cyber Vision поєднує в собі аналіз протоколів, виявлення вторгнень, виявлення вразливостей і поведінковий аналіз, щоб контролювати стан безпеки і допомагати діяти на випередження, щоб зменшити вразливість до кіберзагроз. Повністю інтегрований з портфелем рішень Cisco для забезпечення безпеки, розширює IT SOC до домену OT. Оперативна інформація для OT: покращення продуктивності мережі та скорочення часу простою виробництва. Cisco Cyber Vision розуміє промислові протоколи, щоб відстежувати події, що відбуваються у промислових мережах, тому можна підвищити ефективність мережі, швидше усувати несправності та скоротити час простою.

ВИСНОВОК

Безпека є головним пріоритетом кожного підприємства в сучасному світі, а захист архітектури підприємства дозволить захистити бізнес-цінності та результати. Таким чином, критично важливим елементом успіху будь-якої мережі є забезпечення і підтримка безпеки - це вимога, яка застосовується до всіх мереж і мережевих пристроїв для Інтернету речей. Прагнучи спростити кібербезпеку і підвищити видимість пристроїв в системах, в області Інтернету речей, Cisco представляє Cisco Cyber Vision - програмне рішення для кібербезпеки. Cisco Cyber Vision надає організаціям можливість отримати огляд промислового середовища, включаючи повну інформацію про те, які активи знаходяться в мережі, як ці активи взаємодіють, а також розуміння операційної інформації на рівні додатків. В результаті Cisco Cyber Vision надає уявлення і можливості, включаючи інтеграцію, які можуть бути використані командами безпеки, командами IT-інфраструктури та операційними командами для забезпечення цілісності системи і захисту від кібер-ризиків.

Cyber Vision - це рішення для моніторингу промислових мереж. Воно покладається на потужний стек DPI для декодування різних промислових протоколів. Потім Cyber Vision будує карту спостережуваної мережі. Це дозволяє знаходити неправильні конфігурації, виявляти аномалії та проблеми з безпекою. Сильною стороною рішення є те, що "датчики", які виконують роботу DPI, фактично вбудовані в деякі промислові маршрутизатори, комутатори та точки доступу Cisco, тому можна використовувати наявне обладнання. Cisco Cyber Vision забезпечує повну видимість ІКС, включаючи динамічну інвентаризацію активів, моніторинг мереж управління і технологічних даних в режимі реального часу, а також комплексну аналітику загроз, що дозволяє створювати безпечні інфраструктури і впроваджувати політики безпеки для контролю ризиків. Поєднуючи унікальну архітектуру периферійного моніторингу та глибоку інтеграцію з провідним портфелем рішень Cisco Cyber Vision можна легко

розгортати в масштабах, щоб забезпечити безперервність, відмовостійкість і безпеку промислових операцій.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ ПРИ НАПИСАННІ МАГІСТЕРСЬКОЇ РОБОТИ

Характеристика джерела	Джерело
Один автор	6.Ismail Butun, Industrial IoT Challenges, Design Principles, Applicftion and Security, 2020.
Два автори	18. Bhosale, S.A.; Sonavane, S.S. Wormhole attack detection system for IoT network: A hybrid approach. *Wirel. Pers. Commun.* **2022**, *124*, 1081–1108.
Три автори	10. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET Inf. Secur.* **2020**, *14*, 368–379. 14. Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based internet of things. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 794326. 22. Donta, P.K.; Srirama, S.N.; Amgoth, T.; Annavarapu, C.S.R. Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. *Digit. Commun. Netw.* **2022**, *8*, 727–744.
Чотири і більше авторів	1.Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796. 2.Basir, R.; Qaisar, S.; Ali, M.; Aldwairi, M.; Ashraf, M.I.; Mahmood, A.; Gidlund, M. Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors* **2019**, *19*, 4807. 3. Stefanescu, D.; Galán-García, P.; Montalvillo, L.; Unzilla, J.; Urbieta, A. Industrial Data Homogenization and Monitoring Scheme with Blockchain Oracles. *Smart Cities* **2023**, *6*, 263–290. 9. Kumar, S.; Sahoo, S.; Mahapatra, A.; Swain, A.K.; Mahapatra, K.K. Security enhancements to system on chip devices for IoT perception layer. In Proceedings of the 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Bhopal, India, 18–20 December 2017; pp. 151–156. 27. Ansari, M.S.; Alsamhi, S.H.; Qiao, Y.; Ye, Y.; Lee, B. Security of Distributed Intelligence in Edge Computing: Threats and countermeasures. In *The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge*

	Computing; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 95–122.
Тези доповідей, матеріали конференцій	8. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37. 13. Kakkar, L.; Gupta, D.; Saxena, S.; Tanwar, S. IoT architectures and its security: A review. In Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI, Jaipur, India, 23–24 December 2020; pp. 87–94. 15. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 28–31 October 2020; pp. 0406–0413. 20. Jazzar, M.; Hamad, M. An Analysis Study of IoT and DoS Attack Perspective. In Proceedings of the International Conference on Intelligent Cyber-Physical Systems: ICPS 2021, Victoria, BC, Canada, 10–12 May 2022; pp. 127–142. 23. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A review of Internet of things (IoT) security issues, challenges and techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Online, 23–24 December 2019; pp. 1–6. 28. Hassanzadeh, A.; Modi, S.; Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 795–800. 33. Lesjak, C.; Ruprechter, T.; Bock, H.; Haid, J.; Brenner, E. ESTADO—Enabling smart services for industrial equipment through a secured, transparent and ad-hoc data transmission online. In Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), London, UK, 8–10 December 2014; pp. 171–177.

Статті із продовжуваних та періодичних видань	4.Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. 5.Karmakar, A.; Dey, N.; Baral, T.; Chowdhury, M.; Rehan, M. Industrial Internet of Things: A Review. In Proceedings of the 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 18–20 March 2019; pp. 1–6. 7. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors* **2021**, *21*, 3654. 11. Ahmad, I.; Niazy, M.S.; Ziar, R.A.; Khan, S. Survey on IoT: Security threats and applications. *J. Robot. Control. (JRC)* **2021**, *2*, 42–46. 12. Kalinin, E.; Belyakov, D.; Bragin, D.; Konev, A. IoT Security Mechanisms in the Example of BLE. *Computers* **2021**, *10*, 162. 16. de Oliveira, G.H.; de Souza Batista, A.; Nogueira, M.; dos Santos, A.L. An access control for IoT based on network community perception and social trust against Sybil attacks. *Int. J. Netw. Manag.* **2022**, *32*, e2181. 17. Morales-Molina, C.D.; Hernandez-Suarez, A.; Sanchez-Perez, G.; Toscano-Medina, L.K.; Perez-Meana, H.; Olivares-Mercado, J.; Sanchez, V.; Garcia-Villalba, L.J. A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. *Sensors* **2021**, *21*, 3173. 19. Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Alimi, O.A. Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things. *J. Sens. Actuator Netw.* **2022**, *11*, 32. 21. Ding, J.; Zhang, H.; Guo, Z.; Wu, Y. The DPC-based scheme for detecting selective forwarding in clustered wireless sensor networks. *IEEE Access* **2021**, *9*, 20954–20967. 24. Acar, G.; Huang, D.Y.; Li, F.; Narayanan, A.; Feamster, N. Web-based attacks to discover and control local IoT devices. In Proceedings of the 2018 Workshop on IoT Security and Privacy, Budapest, Hungary, 20 August 2018; pp. 29–35. 25. Watson, M.R.; Marnerides, A.K.; Mauthe, A.; Hutchison, D. Malware detection in cloud computing infrastructures. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 192–205. 26. Humayun, M.; Jhanjhi, N.Z.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* **2021**, *22*, 105–117.

	29. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for Internet of things: A comprehensive survey. *Secur. Commun. Netw.* **2017**, *2017*, 6562953. 30._Stallings, W.; Brown, L. *Computer Security Principles and Practice*, 3rd ed.; Pearson: Upper Saddle River, NJ, USA, 2015. 31. Hameed, S.; Khan, F.I.; Hameed, B. Understanding security requirements and challenges in Internet of Things (IoT): A review. *J. Comput. Netw. Commun.* **2019**, *2019*, 9629381. 32. Bakhshi, Z.; Balador, A.; Mustafa, J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Proceedings of the 2018 33. Zhou, L.; Yeh, K.H.; Hancke, G.; Liu, Z.; Su, C. Security and privacy for the industrial internet of things: An overview of approaches to safeguarding endpoints. *IEEE Signal Process. Mag.* **2018**
	Інші видання
Електронні ресурси	34.Cisco Cyber Vision http://cdn.cnetcontent.com/78/55/78555758-3873-41ed-af7b-b87ec438abd2.pdf (дата звернення: 21.10.23) 35. Cisco Cyber Vision Data Sheet https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html (дата звернення 25, 28.10.23) 36. Cisco Cyber Vision Bringing unprecedented scale and simplicity to industrial security https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/cyber-vision-aag.pdf (дата звернення 01.11.23)