Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження вразливостей цифрових двійників виробничих ліній металообробних підприємств

Виконав: студент VI курсу, групи СБм-61

спеціальності 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

_____ Копач М.А.
(підпис) (прізвище та ініціали)

Керівник _____ Скоренький Ю.Л.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Тимощук Д.І.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Копачу Максиму Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження вразливостей цифрових двійників виробничих ліній металообробних підприємств

Керівник роботи Скоренький Юрій Любомирович, к.ф.-м.н., доцент кафедри фізики
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_20_» _листопада_ 2024 року № _4/7-1112_

2. Термін подання студентом завершеної роботи 13 грудня 2024р.

3. Вихідні дані до роботи Наукові публікації про особливості функціонування та вразливості іцифрових двійників Індустрії 4.0

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Область застосування та основи роботи цифрових двійників, 1.1 Принципи та особливості платформ Індустрії 4.0, 1.2 Типи та функції цифрових двійників Індустрії 4.0, 1.3 Процеси та цифрові двійники в металообробці, 1.4 Висновки до першого розділу, 2 Вразливості цифрових двійників, 2.1 Віртуалізація систем промислового інтернету речей, 2.2 Вразливості, характерні для цифрових двійників Індустрії 4.0, 2.3 Можливі атаки на IDT, 2.4 Кіберінциденти, пов'язані з платформами розумного виробництва, 2.5 Висновки до другого розділу, 3 Планування та проведення заходів з протидії вразливостям, 3.1 Принципи кібербезпеки платформ розумного виробництва, 3.2 Виявлення вразливостей промислової інформаційної платформи, 3.3 Планування та проведення заходів з протидії вразливостям, 3.4 Висновки до третього розділу, 4 Охорона праці та безпека в надзвичайних ситуаціях, 4.1 Охорона праці, 4.2 Безпека в надзвичайних ситуаціях, Висновки, Перелік використаних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2 Актуальність. Мета. Завдання дослідження. 3. Процеси та агенти розумного виробництва. 4. Типи та призначення DT, 5. Схема процесів виробничої лінії, 6. Процеси та дані, необхідні для IDT металообробного підприємства. Обробка даних у IDT, 7. Принципи кібербезпеки в застосуванні до розумних виробництв, 8. Діаграма потоку даних для IDT металообробного виробництва, 9. Загрози безпеці та заходи протидії для IDT, 10. Вразливості та засоби пом'якшення для IDT виробничого процесу, 11. Використання інструментів AWS IoT Core для захисту IDT, 12. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Стручок В.С., к.т.н., доцент		

7. Дата видачі завдання 21 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.11.2024-22.11.2024	*Виконано*
2.	Підбір наукових джерел про цифрові двійники	22.11.2024-25.11.2024	*Виконано*
3.	Переклад та опрацювання наукових джерел щодо		
	аналізу вразливостей цифрових двійників	26.11.2024-28.11.2024	*Виконано*
	організації інфраструктури та безпеки публічної		
	вразливостей цифрових двійників	29.11.2024-03.12.2024	*Виконано*
5.	Оформлення розділу «Область застосування та		
	основи роботи цифрових двійників»	04.12.2024-05.12.2024	*Виконано*
6.	Оформлення розділу « Вразливості цифрових		
	двійників Індустрії 4.0»	06.12.2024-07.12.2024	*Виконано*
7.	Оформлення розділу «Планування та проведення		
	заходів з протидії вразливостям»	08.12.2024-09.12.2024	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	09.12.2024-10.12.2024	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2024-11.12.2024	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2024-13.12.2024	*Виконано*
11.	Нормоконтроль	16.12.2024-17.12.2024	*Виконано*
12.	Перевірка на плагіат	13.12.2024	*Виконано*
13.	Попередній захист кваліфікаційної роботи	20.12.2024	*Виконано*
14.	Захист кваліфікаційної роботи	26.12.2024	

Студент _____ Копач М.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скоренький Ю.Л.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження вразливостей цифрових двійників виробничих ліній металообробних підприємств // Кваліфікаційна робота освітнього рівня «Магістр» // Копач Максим Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 77, рис. – 13, табл. – 4, додат. – 1, бібліогр. – 52.

Ключові слова: інформаційна безпека, промисловий інтернет речей, цифрові двійники, вразливості.

Кваліфікаційна робота присвячена дослідженню вразливостей платформ промислових цифрових двійників металообробних підприємств.

У першому розділі проаналізовано типи, призначення та особливості цифрових двійників як інструментів для оптимізації виробництва шляхом цифровізації процесів.

В другому розділі з метою оцінки ризиків для цифрових двійників проводено ретельний аналіз інформації щодо загроз для конкретних цифрових двійників і притаманних їм вразливостей, базуючись на розумінні процесів конкретного виробництва. Визначено атрибути кіберзагроз, які збільшують складність необхідних запобіжних заходів.

З метою виявлення та аналізу потенційних загроз та вразливостей, властивих промисловим цифровим двійникам, у третьому розділі дослідження було застосовано структуровану методологію моделювання загроз STRIDE. За допомогою цієї методології було проведено детальний аналіз кожного елемента діаграми потоку даних, що дозволило ідентифікувати специфічні типи загроз безпеки та розробити відповідні заходи протидії для мінімізації ризиків.

ANNOTATION

Research on vulnerabilities of digital twins in manufacturing lines of metalworking enterprizes // Qualification work of the educational level “Master” // Maksym Kopach // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBm-61 group // Ternopil, 2024 // P. 77, fig. - 13, tables - 4, annexes - 1, references - 52.

Key words: information security, industrial internet of things, digital twin, vulnerabilities.

Qualification work is dedicated to the study of vulnerabilities of the industrial digital twin platform of metalworking enterprises.

The first section analyzes the types, purposes and features of digital twins as tools for optimizing production through digitalization processes.

The second section, providing a risk assessment for digital twins, conducts a thorough analysis of information threats for specific digital twins and their inherent vulnerabilities, based on an understanding of specific production processes. Cyber threat attributes that increase the complexity of preventive measures are identified.

In the third section, the STRIDE threat modeling methodology is applied to identify and characterize threats and vulnerabilities inherent in industrial digital twins. Types of security threats were identified for each element of a specific group in the data flow diagram along with countermeasures that should be implemented to reduce security risks.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

C&C server — Command and Control Server (керуючий сервер).

CIA – Confidentiality, Integrity, Accessibility (тріада конфіденційності, цілісності та доступності).

CIM – Computer-Integrated Model (модель комп'ютерно-інтегрованого виробництва).

DCS – Distributed Control System (розподілена система управління).

DDoS – Distributed Denial of Service (розподілена атака на відмову в обслуговуванні).

DLC – Data Life Cycle (життєвий цикл даних).

DNS – Domain Name System (система доменних імен).

DoS – Denial of Service (відмова в обслуговуванні).

DT – Digital Twin (цифровий двійник).

NIST – National Institute of Standards and Technology

HTTP – HyperText Transfer Protocol (мережевий протокол прикладного рівня HTTP).

HTTPS – HyperText Transfer Protocol Secure.

IDT – Industrial Digital Twin (платформа промислового ціфрового двійника).

ICS – Industrial Control System (промислова система управління).

IoT – Internet of Things (інтернет речей).

IIoT – Industrial Internet of Things (промисловий інтернет речей).

IP – Internet Protocol.

IT – Information Technology (інформаційні технології).

OWASP – Open Worldwide Application Security Project (відкритий проєкт з безпеки вебзастосунків).

PaaS – Platfrom as a Service (платформа як послуга).

PDF – Portable Document Format.

PLC – Programmable Logic Controller (програмований логічний контролер).

RAT – Remote Access Trojan (троян віддаленого доступу).

TCP/IP – Transmission Control Protocol/Internet Protocol.

SCADA – Supervisory Control and Data Acquisition (диспетчерське управління і збір даних).

SM – Smart Manufacturing (розумне виробництво).

STRIDE – Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

SSH – Secure Shell protocol (мережевий протокол “безпечна оболонка”).

VPN – Virtual Private Network (віртуальна приватна мережа).

USB – Universal Serial Bus (універсальна послідовна шина).

ВДТ – Візуальні дисплейні термінали.

ДРПА – Детальний план відновлення після аварії.

ЕОМ – Електронно-обчислювальна машина.

ПЗ – програмне забезпечення.

НС – надзвичайна ситуація.

ШІ – штучний інтелект.

ЗМІСТ

ВСТУП

Актуальність теми. Поява Інтернету речей (IoT) проклала шлях до нових можливостей для вдосконалення промислових процесів за допомогою інтеграції та складного керування машинами та приводами, обладнаними датчиками. У технологічних процесах промисловий Інтернет речей дає виробникам можливість отримати всебічне уявлення про кожен етап виробничого процесу, сприяючи коригуванням у реальному часі для забезпечення безперебійного виробництва та зниження ймовірності дефектів і збоїв, спричинених людськими помилками, відповідно до принципів Індустрії 4.0. Позитивні наслідки інтелектуального виробництва виходять за рамки виробничих операцій, обладнання та оптимізації запасів. Цифрові двійники (DT), які широко використовуються в Індустрії 4.0 для моделювання та керування виробничими процесами [1], є віртуальними копіями фізичних об’єктів або систем. Перевага використання цифрових двійників для малого та середнього бізнесу полягає в можливості оптимізувати виробничі процеси, забезпечити навчання персоналу та розширити можливості моделювання, виправдовуючи розробку ресурсомісткого, але важливого програмного забезпечення, призначеного для моделювання та навчання.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є аналіз вразливостей промислових цифрових двійників, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Для досягнення поставленої мети було потрібно виконати наступні завдання:

- проаналізувати предметну область та з’ясувати типи та характерні особливості цифрових двійників промислового обладнання;
- проаналізувати способи запобігання загрозам для інформаційних процесів Індустрії 4.0;

- дослідити інформаційні процеси та побудувати діаграму потоків інформації для типового металообробного підприємства;
- провести аналіз вразливостей цифрового двійника виробничої лінії металообробного підприємства;
- зробити практичні висновки щодо можливих шляхів забезпечення безпеки даних Індустрії 4.0.

Об’єкт дослідження. Процеси захисту інформації, яка обробляється в системах цифрових двійників металообробних підприємств.

Предмет дослідження. Задача захисту інформації у платформах промислових цифрових двійників.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що проведено аналіз наявних даних щодо ризиків, вразливостей, типів атак, засобів захисту, що дозволить запобігати порушенню роботи промислових цифрових двійників і втраті чутливих даних. В ході дослідження виявлено вразливості нового інформаційного середовища — цифрового двійника виробничої лінії металообробки.

Практичне значення одержаних результатів. На основі проведеного аналізу реалізовано набір запропонованих заходів кіберзахисту за допомогою інструментарію платформи AWS IoT Core, що необхідна для мінімізації потенційних ризиків атаки.

Апробація результатів магістерської роботи. Основні результати роботи доповідались на XII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 17 – 18 грудня 2024 р.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку літератури із 52 найменувань та додатка. Загальний обсяг кваліфікаційної роботи складає 77 сторінки, з них 60 сторінок основного тексту, який містить 13 рисунків та 4 таблиці.

1 ОБЛАСТЬ ЗАСТОСУВАННЯ ТА ОСНОВИ РОБОТИ ЦИФРОВИХ ДВІЙНИКІВ

1.1 Принципи та особливості платформ Індустрії 4.0

Сучасне промислове виробництво переживає період цифрової трансформації, що ознаменований переходом до концепції Індустрії 4.0. Характерною рисою цього етапу є широке використання автоматизації та комп'ютеризації виробничих процесів, що сприяє підвищенню їхньої ефективності та гнучкості.

Виникнення Інтернету речей (IoT) створило нові можливості для покращення промислових процесів за допомогою інтеграції та керування машинами та приводами, обладнаними датчиками [1, 2]. У технологічних процесах промисловий Інтернет речей (IIoT) дає виробникам можливість отримати всебічне уявлення про кожен етап виробничого процесу, сприяючи коригуванням у реальному часі для забезпечення безперебійного виробництва та зниження ймовірності дефектів і збоїв, спричинених людськими помилками, відповідно до принципів Індустрії 4.0 [3, 4]. Позитивні наслідки інтелектуального виробництва виходять за рамки виробничих операцій, обладнання та оптимізації запасів. У поєднанні з підвищеною гнучкістю вузькоспеціалізованого виробництва, адаптованого для швидкої реконфігурації, цей фактор компенсує значні витрати, пов'язані зі створенням, експлуатацією та забезпеченням безпеки систем IIoT [5, 6].

У цьому випадку саме IoT забезпечує зв'язок між цифровою сферою, включно з новими аналітичними методами, і фізичною сферою підприємства та всередині ланцюга постачання. Це добре узгоджується з баченням Індустрії 4.0 про перетворення ланцюжків поставок у розумну мережу пов'язаних інтелектуальних і автономних об'єктів, які спілкуються та взаємодіють один з одним у режимі реального часу [7]. Індустрія 4.0

визначає центральну роль, яку відіграватиме IoT як ключовий фактор розвитку передового інтелектуального виробництва.

Розумне виробництво (SM) можна розглядати як складну систему, яка базується на взаємодії фізичних об'єктів (обладнання), цифрової інформації та інтелектуальних алгоритмів. Аналіз даних, отриманих з різних джерел, дозволяє створювати цифрові двійники виробничих процесів та продуктів, що відкриває нові можливості для оптимізації та прогнозування.

Як і у випадку з багатьма новими технологіями, не існує єдиного загальновизнаного визначення розумного виробництва. Суміш характеристик SM включає аспекти технології (візуальні технології, аналітика даних, інтелектуальне керування, IoT, CPS/CPPS та кібербезпека), аспекти процесу (3D-друк, хмарне виробництво, управління виробництвом на базі IT), аспекти введення, можливість повторного використання відстеження (розумні продукти/частини/матеріали), а також аспекти сталого розвитку (енергоефективність). Очевидно, що це не вичерпний перелік будь-якого з перерахованих вище – наприклад, використання енергії є звичайним, але рідко єдиним витратним матеріалом, який хочеться використовувати ефективно.

З точки зору безпеки, з цієї категоризації випливає кілька цікавих речей:

- Управління виробництвом на базі IT пов’язує системи планування в IT-сфері з CPPS, які поширюються на цех. Як наслідок, безпека повного інтелектуального виробничого процесу залежить від спільних і окремих властивостей безпеки IT-домену, домену CPPS і зв’язку, який повинен існувати між ними.
- Порушення процесу аналізу даних та інтелектуального (адаптивного та/або навченого) контролю шляхом отруєння даних, на основі яких виконується аналіз або навчання, може порушити цілісність установки або якість її продукції. Оскільки надані дані, як правило, є

багатовимірними, а невеликі зміни можуть мати значний вплив на методи навчання, які часто є більш крихкими, ніж зазвичай можна зрозуміти, такі проблеми надзвичайно важко виявити. Проблема посилюється тим фактом, що ми тільки починаємо досліджувати системи навчання, в яких зрозумілий для людини розповідь про те, що було вивчено, виникає в процесі навчання.

- Кібербезпека розглядається як характеристика, а не принцип дизайну. Це помилкове уявлення призвело до створення незахищених систем в Інтернеті. Безпека — це процес, який починається на стадії проектування або перед нею та має охоплювати всі аспекти створеної системи. Крім того, це безперервний процес: поява нових загроз може вимагати фундаментального перегляду безпеки всієї установки, що можна зрозуміти лише на етапі проектування системи.

Таблиця 1.1 – Характеристики, принципи проектування та передові технології, що визначають розумне виробництво (SM) [8]

Характеристики	Принципи проектування	Забезпечуючі фактори
Цифрові двійники	Композиційність	Інноваційні підходи та засоби
Адитивне виробництво		
Кіберфізичні системи	Модульність	
Аналітика даних	Врахування контексту	Системи та стандарти обміну даними
Хмарне виробництво	Сумісність	
Кібербезпека	Різнорідність	Кращі практики та передові стандарти в промисловості

Створення та впровадження аналітичної платформи є ключовим етапом у процесі оптимізації виробництва. Завдяки цій платформі стає можливим системний збір, обробка та аналіз даних, що описують матеріальні потоки, інформаційні потоки та операції виробництва (детально представлені на рис. 1.1). Для ефективного управління виробничими процесами, сценаріями, моделями споживання та параметрами виробництва необхідно

впровадити систему управління даними. Збір даних дозволяє ідентифікувати найбільш енергоємні та відходотвірні процеси, що є необхідною умовою для впровадження нових, даноорієнтованих підходів до оптимізації виробництва. Враховуючи різноманітність обладнання, умов роботи та виробничих графіків, споживання енергії різними елементами виробництва може значно відрізнятися. Тому систематичний збір даних про енергоспоживання за допомогою датчиків Інтернету речей, інтегрованих у виробниче обладнання, є критично важливим для досягнення енергоефективності виробничих ліній.

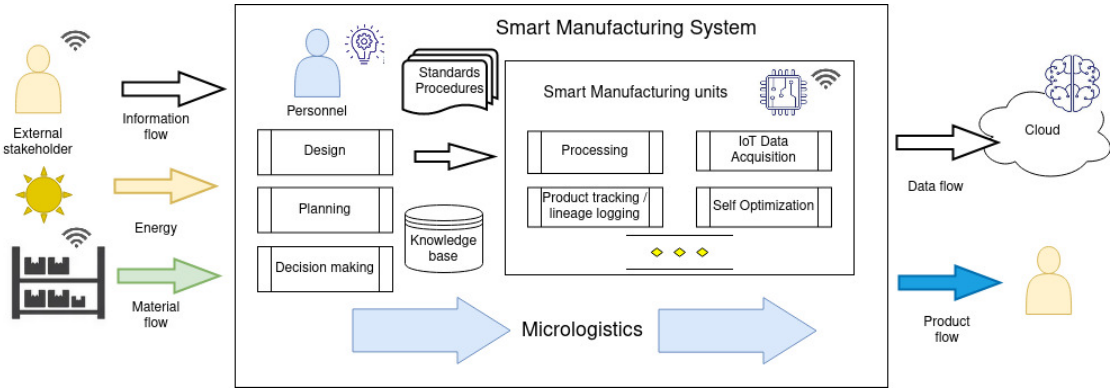

Рисунок 1.1 – Процеси та агенти розумного виробництва [6].

Постачальники обладнання традиційно розробляють власні приватні стандарти, щоб захистити свої права інтелектуальної власності та забезпечити відмінність від своїх конкурентів [9]. Фрагментований ландшафт власних стандартів допомагає цим постачальникам зберегти свою частку ринку, заблокувавши своїх клієнтів. Розробляючи та приймаючи відкриті стандарти, постачальники систем можуть відкривати нові ринкові можливості, зменшувати витрати на розробку, завойовувати визнання клієнтів і залучати нових клієнтів, захистити свої ноу-хау та права інтелектуальної власності, одночасно інтегрувавши відкриті стандарти для забезпечення взаємодії з іншими постачальниками. Незалежні від постачальника рішення забезпечують покращену сумісність у всьому ланцюжку створення вартості. Ці інструменти необхідні для забезпечення

повної оптимізації безперервності даних у промислових процесах. Безперервність даних – це процес, який протікає по всьому ланцюжку створення цінностей і даних. Він починається з фізичного об’єкта, який потім перетворюється на «цифровий артефакт», який потім завантажується на платформу (інтеграція даних). Потім набори даних і цифрові артефакти можуть циркулювати по ланцюжку створення вартості та через потоки даних на заводі.

1.2 Типи та функції цифрових двійників Індустрії 4.0

Впровадження Інтернету речей в промислове виробництво значно розширює функціональні можливості підприємств. Дистанційне обслуговування обладнання, взаємодія між машинами та створення кіберфізичних систем дозволяють підвищити ефективність виробництва, знизити витрати та поліпшити якість продукції. Крім того, Інтернет речей відкриває нові можливості для розробки інноваційних продуктів та послуг, що задовольняють потреби сучасного споживача. Індустрія 4.0 значною мірою спирається на використання віртуальних моделей кіберфізичних активів, які зазвичай називають цифровими двійниками (DT). Було запропоновано цифрові двійники для підтримки управління виробничими активами та життєвим циклом продукту, а також кількох варіантів використання, які можна класифікувати за типами використання як моніторинг, оптимізація та контроль. Цифрові двійники, які широко використовуються в Індустрії 4.0 для моделювання та управління процесами виробництва [10-13], є віртуальними копіями фізичних об’єктів або систем [4, 14]. Ці технології полегшують створення реалістичних 3D-моделей, які можуть взаємодіяти з реальним світом і пропонують безліч функціональних можливостей [15-17].

Інформація є критично важливим активом підприємства Індустрії 4.0, тому дані збираються з кожного елемента виробничої лінії, кожного мобільного пристрою та всіх підключених до мережі пристроїв. Ці дані необхідні для оптимізації виробництва в реальному часі, підвищення ефективності, економії енергії та ресурсів. DT з'явилися як відмінна риса інтелектуального виробництва [17-18], пропонуючи численні переваги. У промисловій сфері DT можна використовувати для моделювання, контролю та оптимізації виробничих процесів, забезпечення прогнозованого обслуговування обладнання [13, 19] і полегшення взаємодії між працівниками [20]. Цифровий двійник, який за визначенням [18] є динамічним віртуальним представленням фізичного об’єкта, частини реальної системи або цілої системи, може бути різних типів. Він може бути невеликим, дзеркальним відображенням окремого об’єкта, певної критичної частини обладнання. Це допомагає в контролі в реальному часі та в плановому обслуговуванні. Він також може являти собою процес або конвеєр, який дозволяє контролювати виробництво та відстежувати прогрес впродовж життєвого циклу виробу. Це також може бути повна віртуальна копія системи загалом, що охоплює виробничу лінію з усіма її елементами, замовленнями та ставленнями споживачів, ланцюг поставок, усі види зовнішнього середовища — промисловий цифровий двійник (IDT). Очевидно, що більший масштаб цифрового двійника, чим складніше програмне забезпечення, що залежить від даних, необхідне для моделювання, моніторингу та керування цифровим двійником, тим більш складні людино-машинні інтерфейси потрібно розробляти та розгортати.

Існують різні типи цифрових двійників залежно від рівня організації втробництва (див. рис. 1.2). Найбільша різниця між цими двійниками – область застосування. Зазвичай в системі чи процесі співіснують різні типи цифрових двійників [16-18, 21].

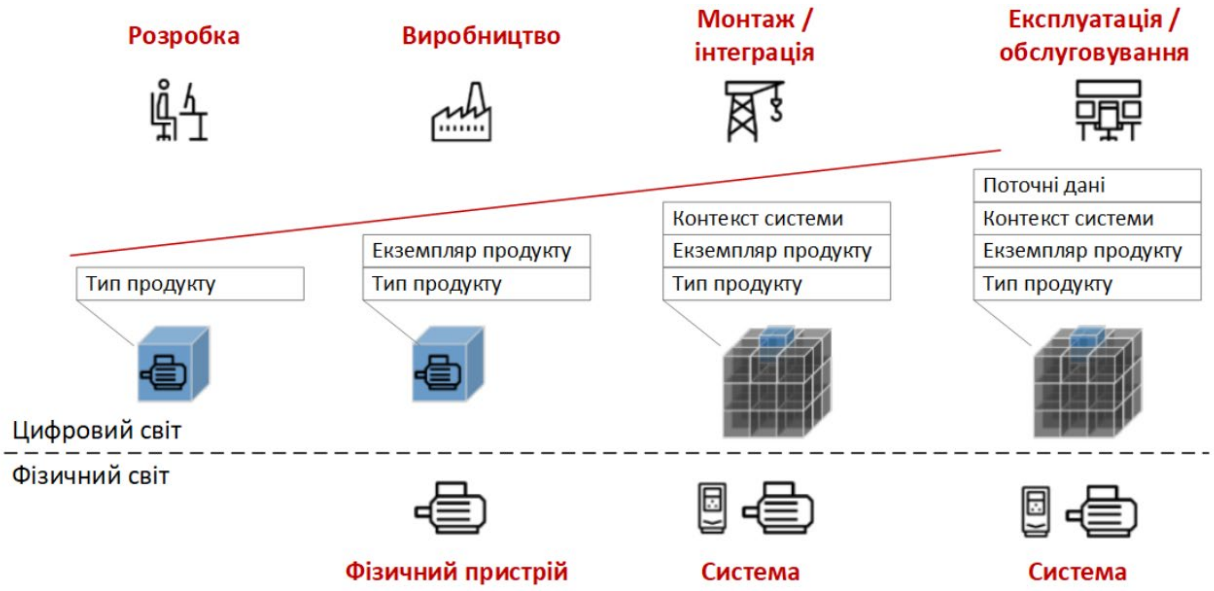

Рисунок 1.2 – Типи та призначення цифрових двійників [21].

Двійники компонентів (мікрорівень) є основною одиницею цифрового двійника, найменшим прикладом функціонуючого компонента. Коли два або більше компонентів працюють разом, вони утворюють сутність, яку називають активом. Двійники активів дозволяють вивчати взаємодію цих компонентів, створюючи величезну кількість даних про ефективність, які можна обробити, а потім перетворити на практичні висновки.

Наступний рівень включає двійники систем або блоків, які дозволяють побачити, як різні активи об'єднуються, щоб утворити цілу функціонуючу систему. Системні двійники забезпечують видимість взаємодії активів і можуть запропонувати покращення продуктивності.

Двійники процесів (макрорівень) показують, як системи працюють у виробничому підприємстві. Всі системи повинні бути синхронізовані, щоб працювати з максимальною ефективністю, оскількт затримки в одній системі вплинуть на інші. Двійники процесів можуть допомогти визначити точні схеми часу, які зрештою впливають на загальну ефективність.

Для будь-якого цифрового двійника є основні елементи, які дозволяють йому функціонувати. Це датчики, які є джерелами даних від периферійних пристроїв, програмне забезпечення, яке формалізує віртуальну

модель і дозволяє проводити прогнозну аналітику, а також інтерфейси для обміну інформацією. Датчики надають дані про різні аспекти функціонування фізичного об’єкта, такі як споживанана потужність, температура, тиск тощо. Потім ці дані передаються в систему обробки та застосовуються до цифрової копії. Отримавши такі дані, віртуальну модель можна використовувати для моделювання, вивчення проблем із продуктивністю та генерування можливих покращень з метою створення цінної інформації, яку потім можна застосувати до вихідного фізичного об’єкта. Різниця між цифровим двійником і симуляцією значною мірою залежить від масштабу: симуляція зазвичай вивчає один окремий процес, в той час як цифровий двійник сам може запускати будь-яку кількість корисних симуляцій для вивчення кількох процесів. Щоб розробити цифровий двійник, потрібно зрозуміти основні процеси та зібрати достатньо даних для розробки статистичних моделей на основі фізики або даних. Цифрові моделі та алгоритми є найефективнішими, якщо їх розгортати в усій промисловій IoT-екосистемі та постійно оновлювати, моделі налаштовувати з новими даними, а алгоритми штучного інтелекту навчаються в режимі реального часу. Коли кожен із активів представлено своїм цифровим двійником, належним чином спроектованим і функціонуючим, наступним природним кроком є розширення цифрового двійника до всієї системи.

Цифрові двійники можна використовувати для вирішення різних задач, з якими стикаються організації:

1. Вивчення вимоги до продукту. DT можуть гарантувати, що вимоги, які висуваються споживачем, зберігаються, перевіряються та перевіряються, коли продукт розвивається, створюється, вводиться в експлуатацію та остаточно виводиться з експлуатації, виводиться з експлуатації та переробляється.
2. Проектування виробів. Однією з переваг цифрового дизайну є можливість оцінювати альтернативи на етапах розробки ідей, а потім

швидко відкидати концепції, які не відповідають початковому наміру. Крім того, DT дизайну можна використовувати для моделювання та тестування дизайну перед початком будь-яких виробничих робіт. 3D-моделі можна візуалізувати для створення конфігурованого цифрового макета кінцевого продукту.

3. Планування проекту: DT для планування проекту можна використовувати для порівняння різних планів життєвого циклу на основі впливу інших цифрових двійників у міру їх розвитку, щоб допомогти в управлінні надзвичайними ситуаціями та стійкістю, щоб переконатися, що план досяжний.
4. Забезпечення надійності. Здатність цифрового відображення інформації з датчика реального екземпляра активу стала можливою із розвитком рішень промислового Інтернету речей. Можливість відстежувати продуктивність активів у реальному часі, наскільки це необхідно, означає, що інженери з надійності можуть приймати кращі рішення щодо обслуговування та заміни активів, таким чином покращуючи загальну продуктивність активів, підвищуючи ефективність системи та оптимізуючи поведінку активів, що дозволяє інженер з надійності для прогнозування та управління ризиками на основі високоякісних даних.
5. Навчання. Оскільки активи стають дедалі складнішими, а досвідчені працівники інформаційних технологій наближаються до виходу на пенсію, зростає корисність цифрового двійника як допоміжного засобу для навчання.
6. Прийняття рішень у реальному часі. DT дозволяють особам, які приймають рішення, швидко зрозуміти наслідки будь-яких змін, внесених до активу на будь-якому етапі його життєвого циклу. DT дає змогу організації виконувати симуляції, щоб відповісти на запитання

«що було б», з коригуванням параметрів, а не проходити через процес створення фізичних прототипів.

7. Виведення обладнання з експлуатації. У зв’язку з тим, що доступні лише обмежені рівні певних ресурсів, велика увага приділяється тому, як активи переробляються, виводяться з експлуатації чи здаються на металобрухт, щоб сприяти циркулярній економіці. Наприклад, у зв’язку з тим, що сталь є обмеженим ресурсом, основні виробники сталі приділяють велику увагу тому, щоб зрозуміти, де використовується їхня продукція, як довго вона використовуватиметься, як її підтримуватимуть і в якому стані вона перебуватиме. закінчення першого терміну служби, щоб гарантувати, що їх можна буде повторно використовувати (можливо, у нижчому класі) для майбутніх продуктів. Крім того, існують глобальні ініціативи щодо моніторингу пластику та інших небезпечних матеріалів для забезпечення безпечного використання та утилізації, що означає, що DT можна використовувати для покращення звітності та дотримання нормативних вимог.

1.3 Процеси та цифрові двійники в металообробці

Ефективне впровадження заходів кібербезпеки в інтелектуальне виробниче середовище вимагає ретельного проектування архітектури програмної платформи з особливим наголосом на швидкості та різноманітності даних, які збираються й обробляються, а також обмеженнях ресурсів компонентів IIoT, вбудованих у виробництво. Крім того, архітектурні міркування повинні враховувати необхідність бездоганної інтеграції пристроїв інтерфейсу з високим ресурсом і високим навантаженням, одночасно вирішуючи потенційні ризики кібербезпеки, що виникають внаслідок обробки конфіденційної інформації в рамках такої

різноманітної та взаємопов’язаної системи. Необхідно враховувати можливості обробки даних, оптимізацію ресурсів і заходи безпеки, таким чином уможливлюючи реалізацію ефективної промислової екосистеми.

Для дослідження вразливостей IDT металообробного підприємства було розглянуто виробничу лінію діючої компанії, яка спеціалізується на виготовленні металевих компонентів для агробізнесу, комбінуючи холодне штампування, зварювання та фарбування. В зв’язку з необхідністю оптимізації витрат та раціонального використання людського потенціалу компанія зацікавлена у цифровізації процесів. Найбільш ефективним способом такої цифровізації є побудова повнофункціонального IDT. Разом з тим, розробка IDT повинна спиратися на всебічний аналіз всіх аспектів його діяльності, загроз, вразливостей та обов’язкове планування заходів кіберзахисту вже на етапі дизайну архітектури IDT.

Основні виробничі процеси процеси показані на рис. 1.3. Метрологічні оцінки повинні проводитися на різних етапах виробничого процесу для забезпечення дотримання стандартів якості та технологічних умов. Початкова фаза (процес 00) передбачає перевірку форми та розміру заготовок шляхом оптичного контролю за допомогою систем камер і лазерного вимірювального датчика після завершення операцій обробки металу. Далі у внутрішньовиробничому сховиші (процес 01) кількість і сортамент заготовок обліковується на основі їх ваги та геометричних параметрів. Процедури зварювання, які виконуються робототехнічною системою Kuka (процес 03), вимагають перевірки зварних швів за допомогою мультиспектрального зображення та аналізу електропровідності. Після коригувального пресування (процес 04) заготовки оцінюються за попередньо визначеним шаблоном або за допомогою даних датчика лазерного вимірювання.

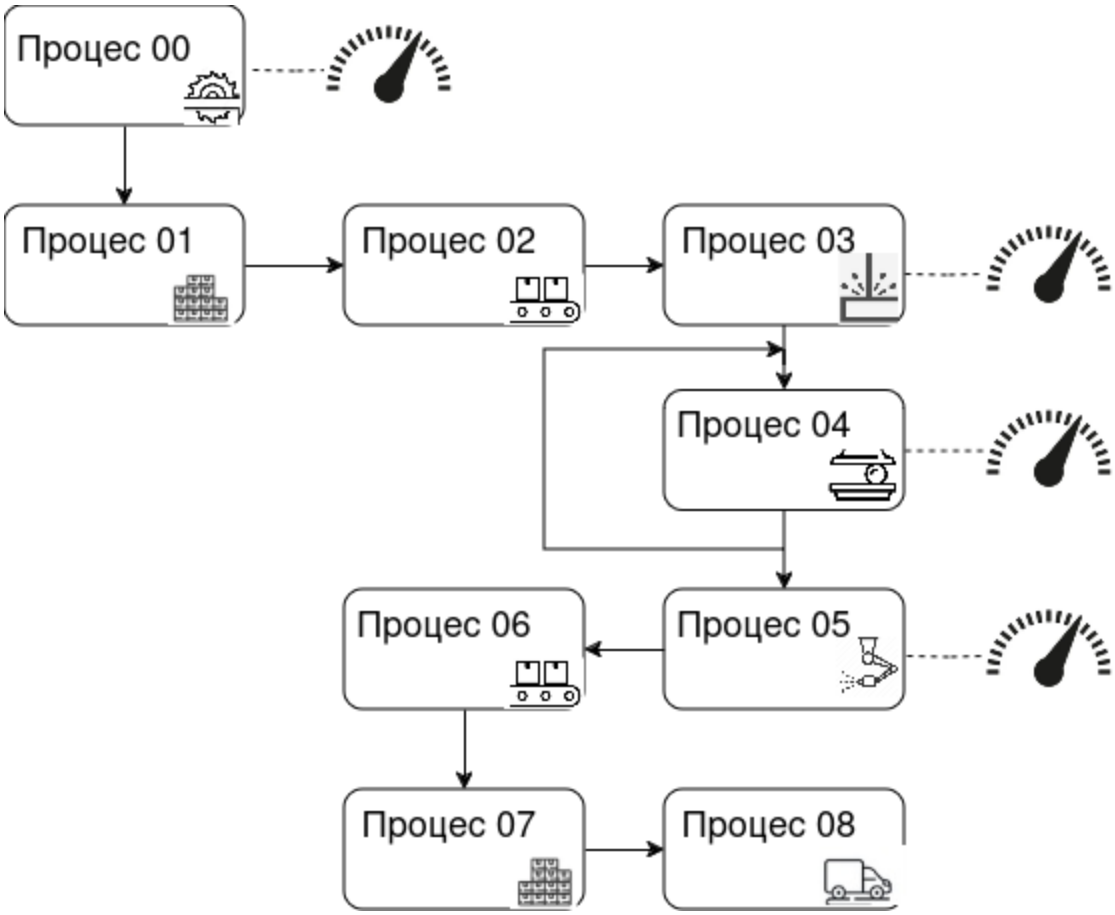

Рисунок 1.3 – Схема процесів для змодельованої виробничої лінії.

Після завершення процесу фарбування (процес 05) проводиться оцінка якості за допомогою ультразвукового вимірювача, готова продукція проходить візуальний контроль за допомогою фотокамери. Вимірювання та метрологічну оцінку слід виконувати після процедур 00, 03, 04, 05, однак внутрішня (процеси 02, 07) та зовнішня (процес 08) логістика також можуть вимагати додаткових вимірювань. Таким чином, складне металообробне виробництво можна розбити на процеси, кожному з яких відповідає цифровий двійник. В свою чергу, кожен з процесів використовує обладнання, яке можна моделювати комплексом цифрових двійників компоненрів, які обмінюються даними між собою та з зовнішніми пристроями. Оптимізація виробництва та управління можниві на рівні цифрового двійника всього підприємства.

Компоненти інтелектуальної виробничої лінії генерують значні обсяги різнотипних даних, характеристики яких представлено в таблиці 1.2. Відмінності у швидкості та обсязі генерації даних обумовлюють необхідність застосування різноманітних підходів до їх збору, передачі, попередньої обробки та зберігання. Зокрема, для ефективного управління даними, що надходять від кіберфізичних систем на основі пристроїв Інтернету речей з обмеженими ресурсами, необхідно розробити масштабовану платформу обміну даними [12], яка б забезпечувала безпеку та надійність передачі інформації.

Таблиця 1.2 – Процеси та дані, необхідні для цифрового двійника металообробного підприємства

Процеси	Характеристики
Експлуатація	Вимірювання температури, тиску, маси, швидкості
	Експлуатаційні показники
	Моделі оптимізації виробництва
Обслуговування	Вимірювання температури, тиску, маси, швидкості
	Дані щодо обслуговування пристроїв
	Прогностичні моделі
Безпека/керування	Вимірювання температури, тиску, маси, швидкості
	Дані та записи контролю
	Записи сертифікації

Різноманітність виробничих процесів вимагає застосування широкого спектру вимірювальних інструментів. Правильний вибір датчиків та виконавчих механізмів Інтернету речей є ключовим фактором для забезпечення ефективного збору даних та прийняття обґрунтованих рішень. Так, для оцінки температурного режиму обладнання можуть використовуватися як точкові термометри, так і термографічні системи, вибір яких залежить від специфіки об’єкта дослідження. Загалом, відповідність вимірюваних параметрів технологічним вимогам є необхідною умовою для забезпечення високої якості продукції та стабільності виробничого процесу.

Розробка та використання цифрового двійника, за послідовністю кроків, показаною на рисунку 1.4, дозволяє це забезпечити.

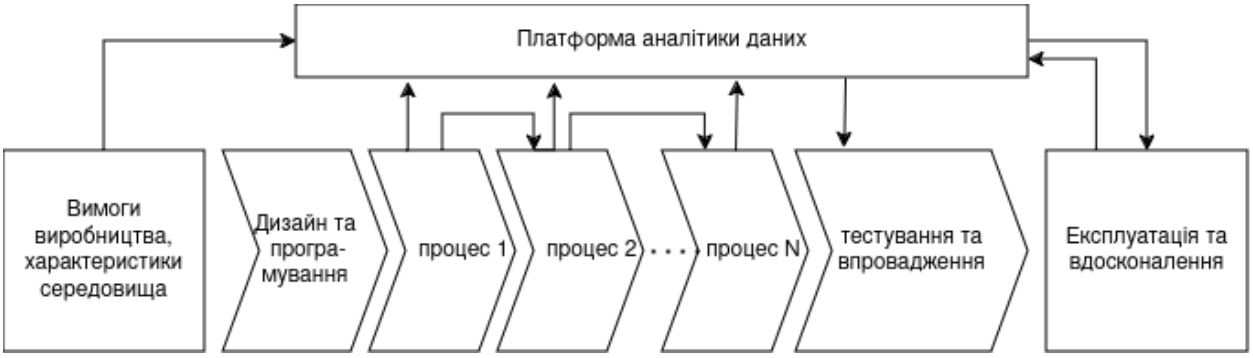

Рисунок 1.4 – Життєвий цикл IDT [22].

Діаграма, зображена на Рисунку 1.5, ілюструє обробку даних у IDT для виробника металевих деталей. Він складається з кількох блоків, які групують уніфіковані процеси або центри обробки даних з метою уникнення централізації обробки даних, обмеження поширення інформації всередині та за межами IDT і, зрештою, забезпечення швидкого розподіленого прийняття рішень для розумних виробництво. З точки зору виробника, найбільш фундаментальним блоком є оцифрована промислова платформа. Хоча існуюча інфраструктура спрощує подальшу розробку, вона також створює складності через необхідність забезпечення узгодженості системи, особливо коли застаріле обладнання взаємодіє з новими компонентами. У таких сценаріях наявність архітектурної схеми стає критичною вимогою для швидкого виявлення вузьких місць і вирішення проблем.

Вимоги підприємства до IDT полягали в тому, щоб уможливити навчання персоналу на місці та розширити можливості моделювання, виправдовуючи підключення до добре структурованої, розширюваної бази знань, яка може бути зовнішнім компонентом суб’єкта господарювання, але повинна бути частиною IDT. Хоча точаться дискусії щодо того, чи може зберігання даних у хмарі скомпрометувати конфіденційну інформацію та

відповідати національному законодавству, що гібридна інфраструктура даних може бути розроблена для пом’якшення таких ризиків.

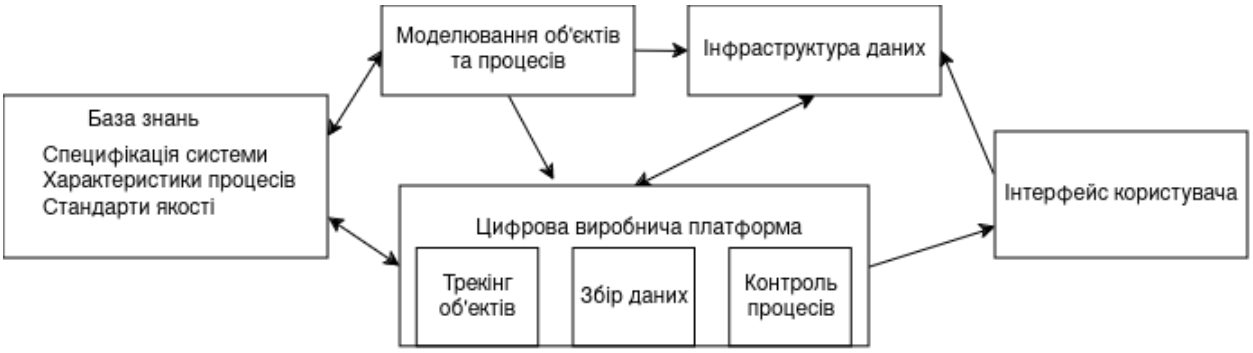

Рисунок 1.5 – Обробка даних у IDT.

Для описаної архітектури фактичний вибір периферійних електронних пристроїв і розробка програмного забезпечення вимагають специфікації моделі для циклу виробництва продукту, який слугуватиме інструментом для оптимізації процесу та моделлю потоку даних для цілей кібербезпеки. З точки зору оператора, модулі оцифрованої промислової платформи та модулі моделювання та навчання будуть нерозрізненими за умови, що сценарії навчання є дуже реалістичними та охоплюють усі можливі операції, несправності та що пристрої обробки даних мають достатню обчислювальну потужність.

На відміну від традиційного веб-орієнтованого цифрового двійника, у випадку платформи даних металообробного підприємства фізичні й віртуальні активи мають рівну цінність, що робить їх взаємозамінними для цілей моделювання. Цей підхід може забезпечити підвищену гнучкість і швидші цикли прийняття обґрунтованих рішень. Існує можливість уникнути критичних збоїв за допомогою цифрового двійника з підтримкою штучного інтелекту, вдосконалення якого стане природним продовженням поточної роботи. Таким чином, промисловий цифровий двійник дає операторам можливість приймати обґрунтовані рішення в реальному часі.

1.4 Висновки до першого розділу

Створення повнофункціонального IDT дозволяє бізнесу забезпечити оптимізацію витрат та раціональне використання людського потенціалу шляхом цифровізації процесів. Розробка IDT повинна спиратися на аналіз всіх аспектів його діяльності, загроз, вразливостей та обов’язкове планування заходів кіберзахисту вже на етапі дизайну архітектури IDT. Необхідно враховувати можливості обробки даних, оптимізацію ресурсів і заходи безпеки, щоб забезпечити ефективність промислової екосистеми.

З метою оцінки ризиків для цифрових двійників необхідно проводити ретельний аналіз інформації щодо загроз для конкретних DT і притаманних їм вразливостей, базуючись на розумінні процесів конкретного виробництва. Для забезпечення ефективного управління виробництвом необхідний комплексний підхід до збору даних, який передбачає правильний вибір, установку та інтеграцію датчиків та виконавчих механізмів IIoT.

2 ВРАЗЛИВОСТІ ЦИФРОВИХ ДВІЙНИКІВ ІНДУСТРІЇ 4.0

2.1 Віртуалізація систем промислового інтернету речей

Промислові системи управління (ICS) є частиною кіберфізичних систем. Ефективні ICS є міцною основою для успіху Індустрії 4.0. ICS - це категорія систем управління, які використовуються для управління та автоматизації промислових процесів [23], і вони повинні розглядатися як інтегральна частина IDT. З розширеним підключенням підвищується ризик кібератак, а це означає, що IDT потребуватиме кращого захисту. У минулому безпека виробничих систем досягалася за допомогою ізоляції на основі контролю фізичного доступу. Останнім часом, з міркувань вартості та зручності, Ethernet і стек протоколів IP стають основною частиною заводських і заводських мереж, внаслідок чого підключення таких мереж до більш широких корпоративних систем стає простіше і поширеніше. Подібним чином, щоб розширити мережеву інфраструктуру до віддалених районів, збільшити пропускну здатність зондування, керувати мобільністю та зменшити витрати на встановлення, спостерігається збільшення розгортання бездротових мереж [7].

Цифрові виробничі платформи дозволяють надавати виробничі послуги в широкому розумінні [24]. Цифрові платформи надають послуги, які можна використовувати для збору, зберігання, обробки та доставки даних. Ці дані описують весь контекст, який включає продукт, який виготовляється, виробничий процес, виробничі активи, працівника та всю мережу цінностей. Загалом, цифрова платформа для виробництва може забезпечити будь-яке «цифрове» розширення функціональних можливостей фізичних активів шляхом впровадження інформаційних технологій (IT). Цифрові платформи IDT відіграють вирішальну роль у створенні сценаріїв застосування цифрового виробництва [25]. Усі послуги спрямовані на оптимізацію

виробництва з різних точок зору, таких як ефективність, доступність, якість, продуктивність, гнучкість тощо. Цифрові платформи можуть бути розміщені на підприхємстві, у хмарі або в гібридній архітектурі.

Модель комп’ютерно-інтегрованого виробництва (CIM), показана на рис. 2.1, показує ієрархічну архітектуру комп’ютерних систем і комунікаційних з’єднань, які є в системах автоматизації виробництва. Це високоінтегрована модель, яка була використана та включена в багато інших моделей і стандартів у промисловості. Модель розділена на п'ять шарів, у яких мережеві протоколи загального призначення використовуються на вищих рівнях, а спеціальні протоколи використовуються на нижчих рівнях для забезпечення все менших затримок і більш спеціалізованих вимог. Як показано на рис. 2.1, на верхньому рівні, рівні підприємства/корпорації, приймаються рішення, пов’язані з оперативним управлінням, які визначають робочі потоки для виробництва кінцевого продукту. На рівні управління підприємством ці рішення приймаються локально в мережі керування підприємством. На наглядовому рівні здійснюється управління різними виробничими осередками, кожна з яких виконує різний виробничий процес. На рівні контролю клітини виконуються різні дії процесу. На нижньому рівні, на рівні датчика-приводу, контролери, датчики та виконавчі механізми інтегровані для виконання фізичного процесу. Ця модель вразлива до атак на безпеку, оскільки вона небезпечна за своєю конструкцією. Використані протоколи зв'язку для підтримки цієї інфраструктури, як-от Modbus, протокол розподіленої мережі (DNP3), PROFIBUS, мережа автоматизації та управління будівлями (BACnet), промисловий Ethernet, широко використовуються на рівні нагляду та керування для підключення пристроїв, шин або мереж. Ці протоколи зв’язку не були розроблені з урахуванням безпеки, і їм бракує механізмів для забезпечення автентифікації, цілісності, свіжості даних, неспростовності, конфіденційності та заходів для виявлення помилок і ненормальної поведінки.

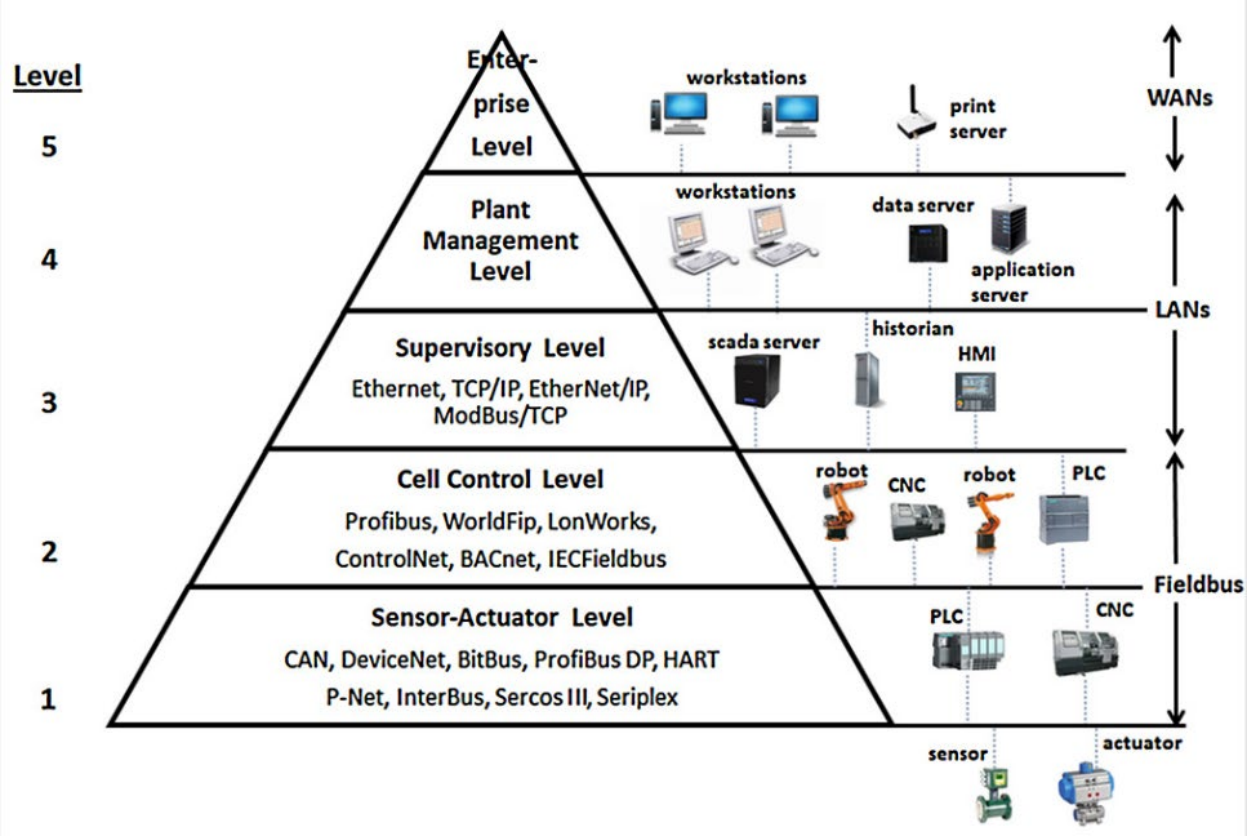

Рисунок 2.1 – Комп’ютерно-інтегрована виробнича модель (CIM) [7].

Концепція CIM відрізняється від бачення Індустрії 4.0, оскільки вона досить жорстко структурована. На нижніх рівнях (3-1) широко використовуються архітектури головний/підлеглий, у яких зв’язок зазвичай ініціюється головним. Індустрія 4.0 та інші подібні ініціативи для кіберфізичних систем пропонують більш децентралізовану архітектуру, у якій елементи моделі CIM є автономними. Автономні елементи знають своє оточення та можуть спілкуватися з іншими елементами, щоб контролювати те, що потрібно. Це призводить до децентралізованої автономної моделі, у якій продукти та машини стануть активними учасниками IoT, поводячи себе як автономні агенти протягом усього виробництва. Коли продукт рухається по виробничій лінії, він зв’язується з кожною машиною та повідомляє їй необхідний процес у цей момент, забезпечуючи гнучкий контроль між продуктами та машинами.

У рамках цього бачення ключовим є децентралізоване прийняття рішень, отримання даних та їх обробка на місці в режимі реального часу.

Самоврядування, обізнаність, самоорганізація, самообслуговування та самовідновлення – це деякі з атрибутів, які використовуються для опису можливостей компонентів і систем майбутніх фабрик і заводів.

Таке відкрите середовище схильне до широкого спектру як пасивних, так і активних атак безпеки, починаючи від звичайних атак підслуховування та відмови в обслуговуванні (DoS) до атак типу "людина посередині", які дещо змінюють якість або консистенцію кінцевого продукту. У порівнянні з атаками на звичайні мережі, наслідки атак на елементи виробничих систем можуть бути катастрофічними, оскільки вони мають здатність завдавати фізичної шкоди виробництву, людям і фізичному середовищу. Єдиний спосіб вирішити цю проблему – вбудувати аналіз безпеки (і постійне управління безпекою) на етапі проектування [26]. Відкритість архітектури, гнучкість у його реконфігурації та використання аналітики даних для здійснення внутрішніх змін призводять до складної динамічної поведінки, про яку важко пояснити. Зокрема, наразі неможливо чітко сформулювати очікувану поведінку в деталях, тому важко міркувати про джерело проблем або конкретний набір динамічних взаємодій, які призвели до проблем. Це означає, що діапазон можливих атак є більшим у моделі Індустрії 4.0, ніж у CIM, але ймовірність виявлення нижче, а підхід до пом’якшення неясний.

Безпека промислового цифрового двійника повинна бути закладена на етапі його розробки та супроводжувати систему протягом усього життєвого циклу. Це передбачає проведення аналізу ризиків, розробку політики безпеки, впровадження технічних заходів захисту та постійний моніторинг стану безпеки. Особливу увагу слід приділити захисту даних, що передаються по мережі, а також забезпеченню цілісності та доступності систем і додатків. Для досягнення високого рівня безпеки необхідно дотримуватися відповідних галузевих стандартів та найкращих практик.

2.2 Вразливості, характерні для цифрових двійників Індустрії 4.0

Вразливість – це відома слабкість у системі, яка може бути використана зловмисником для досягнення несанкціонованого доступу або пошкодження системи. Вразливості можуть бути різного типу: програмні (наприклад, помилки в коді), апаратні (недоліки фізичного обладнання), конфігураційні (неправильні налаштування системи) та людські (помилки персоналу).

Ризик – це ймовірність того, що вразливість буде експлуатована зловмисником, що призведе до певних негативних наслідків. Оцінка ризику включає в себе аналіз таких факторів, як цінність активу, ймовірність виявлення вразливості зловмисником, складність експлуатації вразливості та потенційні наслідки інциденту. Для ефективного управління ризиками інформаційної безпеки необхідно проводити регулярний аналіз вразливостей та загроз, розробляти та впроваджувати заходи захисту, а також здійснювати моніторинг стану безпеки системи.

Загрози для цифрових двійників активів металообробних підприємств можна класифікувати наступним чином :

Ботнети. Ботнет в IoT означає сукупність скомпрометованих або заражених пристроїв IoT, які знаходяться під контролем кіберзлочинців і використовуються для шкідливих дій, таких як запуск DDoS-атак або викрадення конфіденційних даних.

Загрози DNS. Цінність технології IoT полягає в її здатності підключати пристрої, збирати дані та приймати рішення на основі аналізу. Однак поточна система іменування, яка використовується для з’єднань пристроїв, відома як DNS, є застарілою та ненадійною для вимог масштабу, трафіку та безпеки сучасного Інтернету речей.

Програмне забезпечення-вимагач. Мета використання програм-вимагачів в галузі IoT полягає в тому, щоб вразити ціль у певний час і в певному місці, коли власники не можуть перезавантажити пристрій або протистояти впливу програм-вимагачів. Мета полягає в тому, щоб створити відчуття терміновості та заохотити жертву заплатити викуп.

Оскільки з використанням пристроїв Інтернету пов’язані кіберризики, наслідки для безпеки в зламаному пристрої призведуть до пошкодження об’єктів або обладнання та призведуть до простою виробництва. Деякі з поширених сценаріїв ризику в промислових умовах включають широкий спектр кібератак, наприклад, коли зловмисник встановлює шкідливі для системи програми, і в результаті вдається заблокувати всі форми логістики та виробничі операції. Виробництво, а також застосування потужності зазвичай ретельно перевіряються, що дозволяє контролювати дані програми та системи. У такому випадку найгірший сценарій включатиме неправильно скеровану машину, що може призвести до фізичних пошкоджень у всьому околиці [27]. В іншому випадку команди для промислових роботів надсилаються через імплантовану систему, яка пов’язана з запрограмованим логічним контролером, підключеним до Інтернету. Як наслідок, у такій ситуації зловмисник може встановити свої пакети даних, які можуть саботувати виробничу лінію певної галузі чи всю IT-інфраструктуру організації, а також зчитувати різні системні та прикладні дані. Третій сценарій стосується сектору соціальної інженерії, за якого зловмисники скористаються людськими вразливостями, такими як довіра, готовність допомогти, страх і цікавість, щоб змусити співробітника отримати доступ або отримати доступ до даних організації, уникаючи різних ситуацій безпеки або встановлення шкідливих програм на свої пристрої [28]. Загалом, їх мета полягає в тому, щоб здійснювати шкідливі діїс, поки вони залишаються непоміченими в мережі компанії.

Щоб зрозуміти ймовірні вектори атаки, потрібно розуміти вразливі місця промислових інформаційних систем загалом та цифрових двійників зокрема [7]. Виробничі системи, як правило, або розробляються без урахування безпеки, або з явним припущенням, що система ізольована і тому не піддається (стороннім) атакам. Практики розробки безпечного програмного забезпечення, спрямовані на запобігання вразливостям

програмного забезпечення, включаючи специфікацію вимог безпеки та реалізацію властивостей безпеки, включаючи тестування, перегляд коду та керування виправленнями, не розглядалися широко під час створення цих систем. Спроби модифікувати захист існуючих систем у світлі атак мають погані результати: з огляду на той факт, що система працює, важко гарантувати, що нові системи безпеки так само повністю протестовані, як оригінальний дизайн, і, як наслідок, вони часто надто консервативні в місцях, водночас не в змозі повністю захистити систему та вводячи нові помилки та вразливості. Таким чином, розгляд безпеки є життєво важливим на кожному етапі життєвого циклу системи [29].

Застосування готових комерційних продуктів, таких як відкриті протоколи та робочі станції під керуванням відомих операційних систем, таких як Microsoft Windows або Linux, зменшило витрати на інсталяцію та забезпечило кращий взаємозв’язок. Однак вони також успадковують уразливості цих продуктів і надають більше можливостей для атак на ці системи. Промислові системи управління використовують широкий спектр незахищених протоколів зв'язку, таких як Modbus, PROFINET, DNP3 і EtherCAT. Хоча Modbus і DNP3 починалися як послідовні протоколи, обидва вони були розширені для роботи з TCP/IP і Ethernet, і вони широко використовуються для підключення пристроїв до різних польових шин або мереж. Ці системи не мають механізмів безпеки для підтримки автентифікації (наприклад, будь-хто може маскуватися під головного й надсилати команди підлеглим пристроям), цілісності пакетів, захисту від відмови або повторного відтворення [30].

Вразливі місця часто з’являються у виробничих системах через погану політику та методи безпеки. Навіть сьогодні загальноприйняті та «очевидні» хороші практики, такі як відключення непотрібних з’єднань і зміна налаштувань з’єднання за замовчуванням і паролів, менш поширені в галузі, ніж можна було б розумно передбачити, враховуючи історію атак. Тому не

дивно, що, враховуючи новизну систем Інтернету речей і враховуючи невизначеність, внесену в ці системи динамічними змінами, які виникають через непрозору навчену поведінку, немає загальновизнаного погляду на те, якими можуть бути вразливості систем розумного виробництва. Без такого розуміння та без дій, які з нього випливають, частина яких, за загальним визнанням, може виникнути лише з досвіду, неминучий висновок полягає в тому, що такі системи є вразливими способами, які нам ще належить відкрити.

2.3 Можливі атаки на IDT

Відносно невелика кількість зареєстрованих атак [7], ймовірно, зумовлена деякою комбінацією чотирьох факторів: 1) атаки є складними: вони вимагають спеціальних знань про виробничі системи, які не є широко представленими серед потенційних зловмисників; 2) зловмисники уникають виробничих систем через власні соціальні причини: враховуючи аналогічний обсяг зусиль, може бути можливим здійснити атаку на IT-системи, яка має глобальне охоплення, і таким чином викликати більше похвали для зловмисника; 3) люди не усвідомлюють, що вони піддаються атаці, оскільки наслідки цих атак ледь помітні або тому, що не вдається пов’язати симптоми з можливістю нападу; 4) про атаки просто не повідомляється, оскільки це завдасть шкоди довірі до бізнесу. Протоколи комунікаційних мереж, що використовуються для промислової автоматизації, не були розроблені з урахуванням безпеки, і було проведено досить мало аналізу їхніх властивостей безпеки порівняно з аналогічними Інтернет-протоколами. Для проектування безпеки важливо розуміти, звідки виникають потенційні загрози. Атаки можуть здійснюватися по всіх мережевих з’єднаннях: через з’єднання підприємства, з’єднання через інші мережі на рівні контрольної мережі та/або з’єднання на рівні польових пристроїв.

Деякі з поширених атак:

1. Відмова в обслуговуванні (DoS): ця атака має на меті позбавити законних користувачів доступу до деяких активів, таких як мережа, системний пристрій або будь-яких інших обчислювальних ресурсів, таких як пам’ять, процес або файлова система. Розподілені атаки на відмову в обслуговуванні (DDoS) використовують кілька скомпрометованих систем, заражених шкідливим програмним забезпеченням для атаки на ціль. За останній рік кілька відомих ботнетів Інтернету речей, таких як ботнет Mirai, були відповідальними за деякі з найбільших DDoS-атак. Ці ботнети скомпрометували сотні тисяч пристроїв IoT, демонструючи невразливість. З’являються нові ботнети, схожі на Mirai, такі як ботнети Brickerbot [31] і Repaer [32], демонструючи небезпеку підходу «налаштував і забув» до пристроїв IoT.

2. Підслуховування (Eavesdropping attack): шляхом моніторингу мережі зловмисник може отримати конфіденційну інформацію про поведінку мережі (пасивна розвідка) для подальших атак. Аналіз мережевого трафіку, навіть зашифрованих пакетів, може виявити інформацію (наприклад, хто з ким і коли розмовляє) і порушити конфіденційність.

3. Атака "людина посередині" (Man-in-the-middle): у цій атаці супротивник сидить між пристроями, що спілкуються, і передає зв'язок між ними. Наприклад, це може саботувати протокол обміну ключами (багато промислових систем керування роблять це відкрито без будь-якого шифрування) між системою керування та виконавчим пристроєм.

4. Атака з впровадженням фальшивих даних (False data injection attack). Атака з фальшивим впровадженням — це атака введення в оману, під час якої зловмисник вводить неправдиву інформацію в мережу; наприклад, надсилаючи шкідливі команди на виконання.

5. Атака із затримкою часу (Time delay attack): зловмисник вводить додаткові затримки в вимірювання та контрольні значення систем, що може порушити стабільність системи та спричинити збій обладнання [33].

6. Атака зі фальсифікацією даних (Data tampering attack): атаки зі фальсифікацією даних призводять до неавторизованої зміни даних, які можуть перебувати в сховищі або передаватися. Наприклад, дані, що зберігаються на робочих станціях істориків даних та інженерів, можуть бути змінені, або мережеві пакети даних можуть бути змінені, що завдасть значної шкоди роботі заводу.

7. Атака відтворення (Replay attack): під час атаки відтворення зловмисник може повторно передати автентичні пакети. Це може статися кількома способами: автентичний, але скомпрометований вузол може надіслати дані, напр. зловмисник, якому вдалося перехопити повідомлення автентифікації.

8. Атака спуфінгу (Spoofing attack): коли вузол зловмисника видає себе за системну сутність. Відсутність відповідних механізмів контролю автентифікації означає, що суб’єкти можуть маскуватися один під одного, фальсифікуючи свою особу, щоб отримати нелегітимний доступ.

9. Атаки по бічному каналу (Side channel attacks) здійснюються з використанням різноманітних методів, які аналізують витік інформації з апаратного та програмного забезпечення, наприклад, аналіз споживання електроенергії, випромінювання світла, оптичного сигналу, потоку трафіку (наприклад, щоб отримати знання про топологію мережі), часу (наприклад, час, необхідний для виконання операції), електромагнітне, акустичне та теплове випромінювання від апаратних компонентів і несправності, що виникають у системі.

10. Атаки через приховані канали (Covert-channel attacks): використовує скомпрометований пристрій і законні канали зв’язку для

витоку конфіденційної інформації з безпечного середовища в обхід заходів безпеки [34].

11. Фізична атака (Physical attack): отримуючи фізичний доступ до обладнання виробничих систем, зловмисники можуть маніпулювати доступними пристроями, наприклад, декалібрувати датчики для зміни вхідних сигналів; зміна розташування пристрою (наприклад, датчика), що призводить до того, що отримані дані містять помилки; введення шахрайського пристрою в мережу для маскування під законний пристрій; а також атаки на фізичні властивості пристроїв (наприклад, через атаки збоїв, пов’язані з модифікацією годинника або джерела живлення чіпа для маніпулювання роботою системи).

12. Атаки на машинне навчання та аналітику даних: методи машинного навчання широко використовуються в безпеці від біометрії до моніторингу безпеки мережі. Для розумних виробничих систем аналіз даних лежить в основі переваг, які, ймовірно, принесе цей розумний підхід. У результаті, якщо процес машинного навчання може бути підірваний або безпосередньо, або через отруєння даних, на які він спирається, будуть наслідки. Враховуючи непрозорість процесу навчання, не завжди зрозуміло ні атакуваному, ні навіть нападнику, які можуть бути наслідки або як ідентифікувати таку атаку. Приклади атак на машинне навчання включають фільтрацію спаму [35] і системи біометричного розпізнавання [36]. Машинне навчання може бути піддано атакам на етапах навчання та висновків. Потенційні атаки під час навчання включають маніпулювання навчальною вибіркою для контролю точності моделі; атаки на доступність вибіркових даних для зниження достовірності моделі та атаки на конфіденційність, які розкривають інформацію про модель навчання.

2.4 Кіберінциденти, пов’язані з платформами розумного виробництва

З огляду на той факт, що розгорнута база інтелектуальних виробничих систем значно менша, ніж у звичайних виробничих систем, не дивно, що існує небагато повідомлень про атаки на них. Це не вказує на відсутність вразливостей у таких системах, а свідчить про їхню відносну новизну та складність. Це, у свою чергу, свідчить про те, що, за винятком, можливо, державних програм інформаційної війни, хакерська спільнота ще має отримати конкретні знання, які дозволили б їм здійснювати успішні атаки. Покладатися на те, що ця ситуація залишається такою, було б безглуздо так само, як виявилося покладатися на знеохочувальний ефект викликів у атаці на звичайні виробничі системи. З цією метою обізнаність про зареєстровані атаки на звичайні системи є важливою передвісником розуміння потенціалу атак на інтелектуальні виробничі системи.

Типові вузли IoT поєднують відносно малопотужний процесор із можливостями бездротової мережі, тому можуть бути атаковані безпосередньо особами в радіусі дії. Це підриває традиційну модель безпеки, в якій існує визначений периметр і пристрої (наприклад, брандмауери та системи виявлення вторгнень), які відповідають за безпеку цього кордону. Натомість кожен пристрій має принаймні частково відповідати за власну безпеку, завдання, яке ускладнюється через обмежені можливості обробки типового вузла IoT. Природно, це не допомагає, коли виробники не вміють оцінити масштабні наслідки нездатності належним чином захистити окремі пристрої, і гучний IoT ботнет Mirai [37], який спричинив найбільшу розподілену атаку на відмову в обслуговуванні, є прикладом такої невдачі.

Mirai виявляє вразливі пристрої IoT шляхом сканування тих, до яких можна отримати доступ через Інтернет. Після ідентифікації цих пристроїв виконується атака грубою силою за допомогою простої атаки за словником (що складається із заводських імен користувачів і паролів, таких як

admin/admin) [38]. Боти повідомляють ідентифіковані IP-адреси вразливих пристроїв на сервери звітів, які потім розподіляють уразливі пристрої на сервери завантаженнКіберінциденти, пов’язані з платформами розумного виробництвая. Сервер завантаження завантажує зловмисне програмне забезпечення, специфічне для операційної системи жертви. Після того, як пристрій запускає зловмисне програмне забезпечення, він стає ботом і отримує нові команди від керуючого сервера (C&C server) . Mirai також мав можливості знищити інші процеси зловмисного програмного забезпечення, закривши всі процеси, які використовують SSH, telnet і HTTP-порти, а також шукав і вимикав інші процеси ботнету, які могли працювати на пристрої. Сервер C&C спілкується з сервером звітів, щоб стежити за зараженими пристроями. Боти здійснюють розподілені атаки на відмову в обслуговуванні (DDoS) на цілі, вони продовжують сканувати та заражати нових жертв, а також отримують нові інструкції від C&C сервера.

Повідомлення про атаки, спрямовані на промислові та виробничі системи, демонструють реальність загроз і те, що наслідки цих атак можуть бути серйозними. Однією з найбільш відомих атак на виробничі системи до початку повномаштабного вторгнення стала атака на енергомережу України в грудні 2015 року [39]. Комбінуючи низку тактик, включаючи використання шкідливих програм і відмову в обслуговуванні, зловмисникам вдалося привести інфраструктуру розподілу електроенергії в небажаний стан, спричинивши перебої в електропостачанні. Ці збої призвели до кількох відключень електроенергії, внаслідок чого сотні тисяч споживачів втратили електроенергію по всій Україні.

Іншим ключовим інцидентом у 2014 році став Havex/Dragonfly, у якому троян віддаленого доступу (RAT) використовувався для зламу промислових систем управління, включаючи SCADA, PLC і DCS, що використовуються в енергетичному секторі [40] по всьому світу. Метою RAT було промислове шпигунство. З початку 2013 року охоронні компанії спостерігали за

цілеспрямованими спробами шахрайства з вкладеннями у форматі PDF проти компаній США та Великобританії в енергетичному секторі [41]. Для встановлення RAT на машинах, що працюють з промисловими системами керування, була використана атака Watering-hole. Законні веб-сайти постачальників енергії були зламані та перенаправлені для завантаження зловмисного програмного забезпечення з серверів зловмисників.

Stuxnet, вперше зареєстрований у 2010 році, вважається першим хробаком, який був розроблений з єдиною метою завдати фізичної шкоди. Існує дуже мало неспростовної інформації про його дію, але вважається, що він був створений урядом або від імені уряду через технічний досвід і ресурси, необхідні для здійснення такої атаки. Аналіз, проведений Symantec [42], показав, що більшість заражених машин (приблизно 60%) були з Ірану. Це змусило експертів з безпеки запідозрити, що атака була спрямована саме на іранське підприємство зі збагачення урану на збагачувальному заводі в Натанзі. За оцінками дослідників, Stuxnet міг знищити близько 1000 (10%) центрифуг, встановлених під час атаки. Зловмисне програмне забезпечення було розроблено для атаки на дві моделі PLC Siemens (Siemens S7-125 і S7-417), які керувалися програмним забезпеченням Step 7 від Siemens. Він використовував чотири вразливості нульового дня, поширювався через знімні носії та USB-накопичувачі, які пізніше підключалися до систем контролю, і використовував передові методи, щоб маскуватися під легальними програмами, щоб уникнути виявлення.

Слід зазначити, що виявлення інцидентів безпеки супроводжується недостатнім звітуванням. Причиною може бути те, що інцидент не було визначено як результат порушення безпеки, або тому, що репутаційна шкода вважалася надто значною, щоб публічно повідомляти про збій безпеки. Інтернет-спільнота дещо просунулася вперед, і є щорічні огляди інцидентів кібербезпеки, які краще відображають досвід бізнесу. На жаль, про

інциденти, пов’язані з виробництвом, досі надходить досить мало повідомлень, і найяскравіші приклади – це ті, які спричинили значні збитки.

Поширеною помилкою у виробництві є те, що проблеми комп’ютерної безпеки однакові, незалежно від того, які комп’ютери захищені. Незважаючи на те, що досвід, отриманий у світі Інтернету, часто можна застосувати до інших мережевих систем, характеристики виробничих систем відрізняють вимоги безпеки до IT-систем, які використовуються на корпоративному рівні. Компоненти, що використовуються в області інтелектуальних виробничих систем, неоднорідні, з великою кількістю застарілих систем і пристроїв, термін служби яких може досягати 20 років. Завдання, якими керує невелика кількість користувачів (операторів та інженерів), мають обмеження в реальному часі, які необхідно накласти, щоб забезпечити безперервність процесу. Ці системи мають складну взаємодію з фізичними процесами, і збої можуть проявлятися у фізичних подіях.

Регулярні виправлення та оновлення є обов’язковою умовою безпеки IT-систем, і більшість компаній вносять виправлення принаймні щомісяця, а іноді й на разовій основі, коли стає очевидною важливість загрози. Виправлення та оновлення стають все більш поширеними в операціях промислового контролю; однак це потрібно ретельно спланувати, оскільки зупинка систем для виправлення чи оновлення може призвести до значного простою всієї виробничої лінії з відповідними витратами. Дійсно, багато власників виробничих систем можуть не встановлювати виправлення негайно, а можуть вирішити не встановлювати виправлення, щоб уникнути ризику, пов’язаного з деякими з цих проблем. Щоб мати можливість встановлювати виправлення, постачальникам потрібні випуски виправлень, а час між розкриттям уразливості та випуском виправлення може бути недостатньо коротким, щоб запобігти атакам.

2.5 Висновки до другого розділу

Існуючі рішення безпеки для виробничих систем можна класифікувати на два основні типи: статичний і активний захист. Статичний метод захисту зосереджується на дотриманні правил, які зазвичай випливають із промислових стандартів і вказівок. Методи динамічного захисту – це криптографічні протидії, системи виявлення та запобігання вторгненням, навчання та управління інцидентами.

Традиційна кібербезпека передбачає механізми безпеки, як автентичність, контроль доступу, конфіденційність, невідмовність, а також цілісність. Наявність цих механізмів буде критично важливою для запобігання атакам і вторгненням у певну мережу чи комп’ютер. Недостатня криптографічна стійкість даних, що зберігаються на пристроях промислового інтернету речей, створює умови для реалізації атак типу "людина посередині". Атаки, спрямовані на компрометацію даних та облікових записів користувачів, становлять особливу загрозу для систем з множинними точками доступу. Сучасні кіберзагрози характеризуються високою динамічністю, масштабністю, стійкістю, складністю та швидкістю поширення. Тому наявність таких атрибутів у кіберзагрозі збільшує складність необхідних запобіжних заходів.

3 ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ ЗАХОДІВ З ПРОТИДІЇ ВРАЗЛИВОСТЯМ

3.1 Принципи кібербезпеки платформ розумного виробництва

Аналіз наявних даних [43, 44] дозволяє виділити основні загрози, пов’язані з кібербезпекою в Індустрії 4.0:

1. Збільшена поверхня атаки: широкий спектр підключених пристроїв і датчиків розширює зону атаки для кіберзловмисників, надаючи більше точок входу для несанкціонованого доступу.
2. Цілісність даних: повнота, правильність і надійність згенерованих даних протягом усього життєвого циклу даних (DLC). DLC починається з початкової генерації та запису даних, шляхом їх обробки, використання, зберігання, архівування та знищення. Так звана цілісність даних також гарантує, що дані не будуть навмисно чи випадково змінені, фальсифіковані, спотворені, видалені чи змінені несанкціонованим чином. Це стосується як даних, що зберігаються в електронному форматі, так і даних у паперовій формі.
3. Ризики застарілої системи: об’єкти багатьох компаній досі працюють із застарілими системами, які можуть не мати сучасних функцій безпеки. Інтеграція цих систем в Індустрії 4.0 вимагає ретельного врахування кібербезпеки.
4. Постачання в комунікаційному ланцюжку: взаємопов’язані ланцюги поставок у розумному виробництві створюють нові вразливості. Кібербезпека має виходити за межі окремих фабрик і охоплювати всю мережу постачання.
5. Індустрія 4.0 пропонує величезні можливості для інновацій та ефективності у виробництві, але ці переваги супроводжуються відповідальністю за вирішення проблем кібербезпеки.

6. Впровадження надійних заходів кібербезпеки має важливе значення для захисту розумних виробничих систем від нових кіберзагроз.

Рисунок 3.1 – Принципи кібербезпеки в застосуванні до розумних виробництв [45]

IT-системи, як правило, побудовані для підтримки належного рівня обслуговування з огляду на неминучість затримок і простоїв, викликаних необхідністю управління підсистемами безпеки. Проектування виробничих систем (див. рис. 3.1) базується на пріоритеті операційної продуктивності, але ця оптимізація здійснюється без урахування необхідності підтримки безпеки системи як невід'ємної частини цього процесу. Передбачається, що він може бути доданий пізніше. Тому не дивно, що зараз галузь значною мірою покладається на велику кількість застарілих систем, які мають низький рівень безпеки (наприклад, паролі за замовчуванням, відсутність контролю доступу та незадокументовані бекдори), і покладається на постачальників для надання послуг безпеки. За визначенням, вони мають бути цілісними, але вони часто поширюються не далі, ніж базове шифрування.

Завдяки досвіду та необхідності IT-індустрія створила кращі знання безпеки, навички та людей, ніж промисловий і виробничий сектор. Крім того, безпекові пріоритети обох секторів принципово відрізняються. В IT-системах безпека часто визначається з огляду на ключові принципи конфіденційності,

цілісності та доступності (також відомих як тріада CIA). Конфіденційність зосереджена на тому, щоб активи не розголошувалися особами, які не мають права переглядати їх; цілісність стосується захисту активів від несанкціонованих модифікацій; а доступність визначається щодо забезпечення доступу до активів для уповноважених осіб у будь-який дозволений час. Тріада CIA допомагає визначити пріоритети управління ризиками безпеки. Найбільше занепокоєння для промислових і виробничих систем, як правило, викликає доступність і цілісність (який з них буде першим, залежить від системи), оскільки відсутність даних і неправдиві дані можуть пошкодити процес або виробництво. Мета конфіденційності не менш важлива; однак бюджетні обмеження можуть означати, що цілі доступності та цілісності матимуть вищий пріоритет.

Так само для корпоративних мереж важливість самих даних означає, що більше вкладається в конфіденційність і цілісність. Безпека та надійність є важливими параметрами проектування промислових і виробничих систем; однак це зосереджено на профілактичних і діагностичних можливостях для запобігання виникненню небезпек і збоїв, які можуть зашкодити людям і середовищу, порушення процесу, пошкодження обладнання або будь-яких інших активів. Із зростанням кіберзлочинності з’явилися інструменти та методології для проведення цифрової криміналістики та обробки цифрових доказів, які набули значення як галузь досліджень в IT-інфраструктурі; однак криміналістика інфраструктури виробничих систем все ще не є достатньо розвинутою [46].

Промислові та виробничі системи складаються із сотень або навіть тисяч пристроїв. Ці пристрої використовують програмне забезпечення та мережеві протоколи для зв’язку з іншими пристроями та операторами. Криптографічні заходи широко використовуються в корпоративних мережах для досягнення конфіденційності та цілісності даних. Використання симетричних алгоритмів шифрування, інфраструктури відкритих ключів,

гібридних схем шифрування, криптографічних хеш-функцій, цифрових підписів, узгодження ключів і протоколів розповсюдження широко використовуються для забезпечення лише авторизованих організацій. Використання шифрування, ідентифікації та контекстного контролю доступу не широко використовується в автоматизації та виробничій промисловості.

Потенційні наслідки атак безпеки на інтелектуальні виробничі системи неможливо переоцінити: травми, смерть і пошкодження фізичної інфраструктури, обладнання та навколишнього середовища, ймовірно, виникнуть просто тому, що виконавчі механізми виробничих систем тісно пов’язані з такими речами. Промислові та виробничі організації повинні враховувати ці проблеми та взяти на себе зобов’язання зробити безпеку основною діяльністю, пам’ятаючи про те, що безпека – це процес, а не продукт. У той час як IT-безпека рухається до моделей двофакторної автентифікації, запобігання, виявлення та реагування, виробничі системи покладаються на обмежені механізми безпеки, такі як спільні короткі паролі за замовчуванням, рідко зашифровані дані, брандмауери між різними рівнями мережевої інфраструктури та прийняття архітектури демілітаризованої зони. Мало того, що доступ відносно легко отримати, зловмисники практично не можуть зупинити зміну параметрів процесу, коли вони отримають доступ до критично важливих систем або даних.

Планування безпеки (див. рис. 3.2). передбачає розуміння природи загроз, виявлення вразливостей, кількісну оцінку вартості, яку буде втрачено в разі використання цих вразливостей, і належне інвестування в безпеку. Процес управління безпекою, як правило, визначається політикою, яка охоплює як цей стратегічний процес високого рівня, так і обмеження, які необхідно запровадити, щоб зменшити ймовірність порушень безпеки, пов’язаних із певними вразливими місцями, і реакції на фактичні порушення, як у в реальному часі та після події.

Рисунок 3.2 – Послідовність моделювання кіберзагроз IDT [47]

Захист даних, які зберігаються та обробляються цифровою платформою Індустрії 4.0 вимагає цілісного підходу [44], який враховує такі елементи:

1. Контроль доступу до даних та інфраструктури є ключовою складовою кібербезпеки. Це означає, що лише авторизовані особи або системи мають доступ до захищених ресурсів. Цього можна досягти за допомогою надійних паролів, двофакторної автентифікації, цифрових сертифікатів тощо.
7. Шифрування: шифрування даних є важливим під час зберігання, обробки та передачі даних. Шифрування передбачає перетворення даних у спосіб, який читають лише авторизовані користувачі. Приклади включають шифрування диска та шифрування зв’язку за допомогою протоколів HTTPS або VPN.
8. Моніторинг і виявлення загроз. Системи моніторингу та виявлення загроз (такі як антивірусні програми та системи виявлення вторгнень) необхідні для виявлення потенційних атак на дані та системи. Вони дозволяють реагувати на загрози в реальному часі.
9. Управління ризиками: управління ризиками передбачає ідентифікацію, оцінку та управління потенційними загрозами та діяльність для мінімізації ризику. Це процес, який є невід’ємною частиною стратегії кібербезпеки.

10. Фізична безпека: захист цифрових даних часто вимагає фізичних заходів безпеки, таких як контроль доступу до серверних кімнат, системи моніторингу відеоспостереження або захист від крадіжки апаратного забезпечення.
11. Навчання та обізнаність співробітників: часто найбільша загроза безпеці даних походить від людей. Тому важливо навчати працівників кібербезпеці та підвищувати їхню обізнаність щодо потенційних загроз, таких як соціальна інженерія чи фішинг.

Гарантування безпеки даних у трьох основних контекстах – зберігання, обробка та передача – має вирішальне значення для ефективної кібербезпеки. Оброблені дані забезпечуються елементами безпеки додатків і операційної безпеки. Передані дані обробляються системою безпеки мережі. Захист мережі спрямований на захист даних, що передаються між усіма пристроями в комп’ютерній мережі.

3.2 Виявлення вразливостей промислової інформаційної платформи

Моделювання загроз є універсальним методом, який може бути застосований до широкого спектра систем, від програмного забезпечення до промислових процесів. За допомогою цієї методології можна ідентифікувати як загальні, так і специфічні для конкретної системи загрози. Наприклад, методологія STRIDE [48] дозволяє виявити вразливості, пов'язані з обробкою корпоративних даних в системах IIoT.

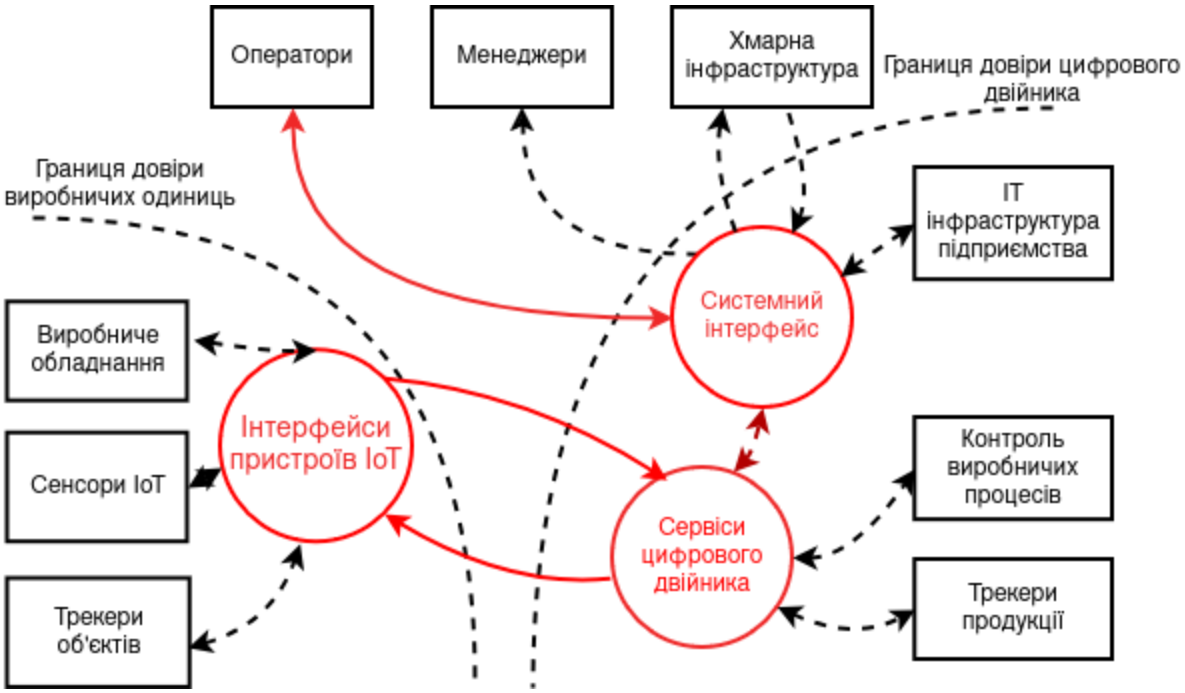

Рисунок 3.3 – Діаграма потоку даних для архітектури цифрового двійника металообробного виробництва

Для оцінки потенційних загроз промислової платформи даних, описаної в роботах [4,14], було розроблено детальну діаграму потоку даних та модель загроз (рис. 3.3) для IDT, модель якого подана на рис. 1.4. Зокрема, увагу було зосереджено на точках з'єднання між різними компонентами системи, механізмах автентифікації, каналах передачі даних. Визначені елементи були обрані через їхню потенційну вразливість до типів атак, розглянутих у попередньому розділі. За результатами аналізу було ідентифіковано вразливості, які можуть бути використані для компрометації IDT та пов’язаних систем.

Для більш детального аналізу та виявлення конкретних вразливостей було застосовано модель OWASP IoT Top Ten. Ця модель дозволила ідентифікувати 10 найбільш поширених загроз для пристроїв IoT. Для кожного елемента системи було визначено, яким чином ці загрози можуть бути реалізовані. Наприклад, для бездротових з'єднань були розглянуті такі загрози, як відсутність шифрування, використання слабких алгоритмів шифрування та вразливості протоколів. За результатами аналізу були

розроблені додаткові заходи захисту. Методологія STRIDE забезпечує високий рівень абстракції та дозволяє ідентифікувати широкий спектр загроз. OWASP IoT Top Ten, в свою чергу, дозволяє зосередитися на конкретних вразливостях, характерних для пристроїв IoT. Комбіноване використання цих двох методологій дозволяє провести більш повний і детальний аналіз безпеки системи та розробити ефективні заходи захисту.

3.3 Планування та проведення заходів з протидії вразливостям

Аналіз діаграми потоку даних архітектури Digital Twin (рис. 3.3) дозволив ідентифікувати ряд критичних точок, вразливих до кібератак. Для зниження ризиків було розроблено комплекс заходів безпеки, деталізованих у табл. 3.1. Запропоновані заходи забезпечують необхідну відстежуваність для перевірки відповідності системи вимогам таких нормативних документів, NIST Cybersecurity Framework. Завдяки регулярному аудиту та моніторингу можна продемонструвати, що система відповідає найвищим стандартам безпеки.

Таблиця 3.1 – Загрози безпеці та заходи протидії для розробленої промислової платформи даних

Тип загрози безпеки	Компонент, для якого загроза аналізується	Запропоновані контрзаходи
Спуфінг (фальшива ідентичність)	Інтерфейси пристроїв IoT, Сервіси цифрового двійника, Користувач	Використання шифрування, Надійні криптографічні протоколи: PGP, AES, SHA-2, TLS 1.2 / 1.3, Надійні механізми автентифікації: MFA, біометрична автентифікація, закріплення сертифіката, OAuth

Продовження таблиці 3.1

Тип загрози безпеки	Компонент, для якого загроза аналізується	Запропоновані контрзаходи
Тамперінг (зловмисні модифікації даних або процесу)	Команда пристрою IoT / Необроблені дані, Інтерфейси пристроїв IoT, Сервіси цифрового двійника	Маркування безпеки, Захищені протоколи зв'язку, Належні механізми авторизації, Хешування та підписування даних
Невизнання (відмова від вчинення дії або розпізнавання настання події)	Інтерфейси пристроїв IoT, Сервіси цифрового двійника, Користувач	Реєстрація та аудит
Розкриття інформації (витік конфіденційних даних)	Інтерфейси пристроїв IoT, Сервіси цифрового двійника, Команда пристрою IoT / Необроблені дані	Належні механізми авторизації, Використання шифрування, Надійні криптографічні протоколи: PGP, AES, SHA-2, TLS 1.2 / 1.3, Найкращі методи безпечного кодування
Відмова в обслуговуванні (недоступність активу, послуги чи мережевого ресурсу для цілеспрямованих користувачів)	Інтерфейси пристроїв IoT, Сервіси Digital Twin, Команда пристрою IoT / Необроблені дані	Програмне забезпечення для захисту від зловмисних програм, програми безпеки, надлишковість даних
Підвищення привілеїв (отримання неавторизованого доступу або привілеїв)	Інтерфейси пристроїв IoT, Сервіси Digital Twin	Належні механізми авторизації, Принципи найменших привілеїв, Реєстрація та відстежуваність, Сертифікація доступу

У таблиці 3.2 наведено описи вразливостей та відповідні засоби пом’якшення. Розуміючи ці вразливості та впроваджуючи ефективні стратегії

пом’якшення, інженери можуть створити надійну систему безпеки, яка захищає їхні екосистеми IoT.

Таблиця 3.2 – Вразливості та засоби пом’якшення для цифрового двійника виробничого процесу

Вразливість	Контрзахід для пом’якшення
Незахищені мережеві служби	Ізоляція мережі для пристроїв IoT. Періодична оцінка вразливості. Безпечні мережеві протоколи.
Незахищений інтерфейс екосистеми	Надійна автентифікація кінцевих точок IoT. Зашифровані канали зв’язку між пристроями / екосистемою IoT.
Відсутність безпечного механізму оновлення	Оновлення та виправлення всього програмного забезпечення та компонентів, що використовуються в пристроях IoT. Компоненти моніторингу вразливостей, що використовуються в екосистемі IoT. Відхід від застарілих технологій.
Використання небезпечних або застарілих компонентів	Оновлення та виправлення всього програмного забезпечення та компонентів, що використовуються в пристроях IoT. Компоненти моніторингу вразливостей, що використовуються в екосистемі IoT. Відхід від застарілих технологій.
Незахищена передача та зберігання даних	Використання шифрування для захисту конфіденційних даних під час передачі та зберігання. Використання захищених протоколів.
Недосконале конфігурування пристрою	Інтеграція пристроїв IoT із системами управління ресурсами, відстеженням помилок і виправленнями. Унікальні облікові дані пристрою та контроль доступу.
Небезпечні налаштування за замовчуванням	Зміна конфігурацій за замовчуванням під час початкового налаштування пристроїв IoT. Відключення непотрібних служб і портів.

Щоб уникнути ручного конфігурування, все частіше застосовується розвинутий інструментарій контролю за засобами IIoT, який надають корпорації:

Microsoft Azure IoT (https://azure.microsoft.com/es-es/overview/iot) – пропонує моніторинг пристроїв, систему правил, тіньове відстеження пристроїв і реєстр ідентифікаційних даних. До складу цих базових служб Azure IoT включає кілька існуючих продуктів, як-от Stream Analytics, Power BI, IoT Hub, центр сповіщень і деякі готові засоби машинного навчання. Крім того, Azure Digital Twins дозволяє створювати цифрові моделі будь-якого фізичного середовища; включаючи місця, речі та людей.

Хмарна служба Oracle Internet of Things (https://cloud.oracle.com/en_US/iot) – це хмарна пропозиція керованої платформи як послуги (PaaS), яка дозволяє підключати пристрої до хмари, збирати, обробляти та аналізувати дані з пристроїв IoT в реальному часі, а також інтегрувати їх з іншими системами Oracle.

Google Cloud IoT Core (https://cloud.google.com/iot-core) - це повністю керована платформа IoT. Ця платформа позначена як головний суперник на тлі інших подібних платформ, оскільки вона в основному зосереджена на інтелекті. Для досягнення цього інтелекту він використовує спеціальні запити за допомогою робочих процесів Google Big Query і Cloud Functions. Таким чином, пристрої можуть автоматизувати зміни на основі подій у реальному часі, візуалізація даних виконується за допомогою Google Data Studio, а машинне навчання здійснюється за допомогою Cloud Machine Learning Engine.

IBM Watson IoT (https://www.ibm.com/internet-of-things) - ця хмарна платформа IoT дозволяє користувачам підключати свої пристрої та дані пристроїв IoT до репозиторію, звідки ця хмара IoT допомагає їм отримати уявлення про мережу IoT, щоб не лише покращити свої операції, але й запустити різні нові бізнес-моделі. Користувачі цієї хмарної платформи

отримують обмін даними в режимі реального часу, зберігання даних, керування пристроями та безпечний зв'язок.

AWS IoT Core (https://aws.amazon.com/es/iot-core) - ця хмарна платформа IoT допомагає перетворювати автомобілі, сенсорні мережі та турбіни на «розумні» об'єкти, допомагаючи підключати та керувати датчиками на цих об'єктах. AWS IoT Core надає захищений шлюз пристрою, тіні пристрою, SDK пристрою, реєстр для розпізнавання різних пристроїв, брокер повідомлень і систему правил, яка б оцінювала вхідні повідомлення.

З огляду на доступність та функціональність, для дослідження було обрано хмарну платформу AWS IoT Core. Дана платформа дозволяє ефективно організувати взаємодію між пристроями Інтернету речей та іншими хмарними сервісами AWS. Сервіс забезпечує надійну обробку повідомлень, що передаються між пристроями та хмарою. Для забезпечення безпечного доступу пристроїв до платформи AWS IoT Core використовується механізм аутентифікації за допомогою сертифікатів X.509. Після успішної аутентифікації, пристрій отримує набір дозволів, визначених політиками доступу, що дозволяють виконувати певні дії, такі як підключення до брокера повідомлень та обмін даними.

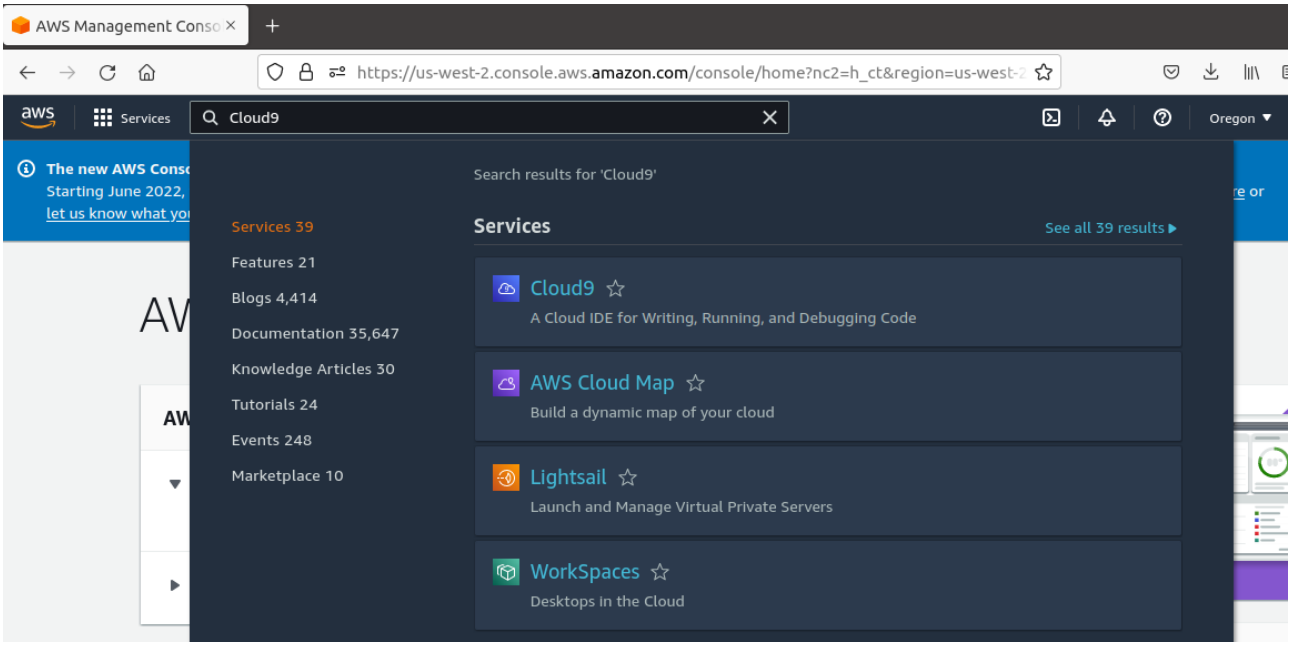

Рисунок 3.4 – Вибір інструментів платформи AWS IoT Core.

Для розробки та конфігурування пристроїв в рамках цього дослідження було використано інтегроване середовище розробки AWS Cloud9 (див. рис. 3.4). Дане середовище забезпечує необхідний набір інструментів для написання, відлагодження та тестування програмного забезпечення. Першим кроком у налаштуванні системи було створення нового середовища розробки з назвою "Sensor". Для забезпечення безпечного підключення пристрою до платформи AWS IoT Core необхідно мати кореневий сертифікат, який зазвичай надається виробником пристрою.

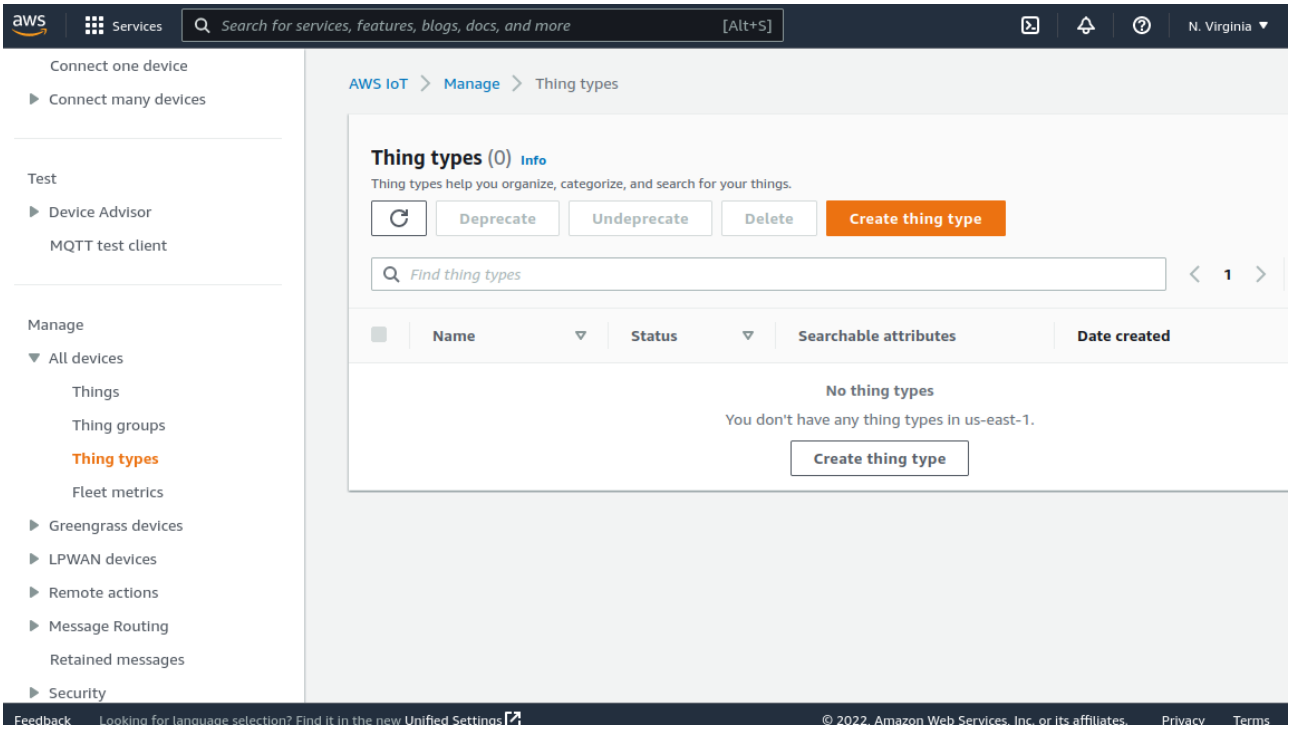

Рисунок 3.5 – Створення типу для пристрою в AWS IoT Core.

Перед тим, як налаштовувати конкретний пристрій Інтернету речей, необхідно створити в консолі AWS IoT Core базові структури даних, які будуть описувати типи та екземпляри цих пристроїв (див. рис. 3.5). Це робиться для того, щоб система розуміла, які дані очікувати від кожного пристрою та які дії з ними виконувати.

Крім стандартних атрибутів, можна додати довільні, які описують специфічні характеристики пристрою. За допомогою вбудованих функцій пошуку можна швидко знайти потрібні пристрої за їхніми атрибутами.

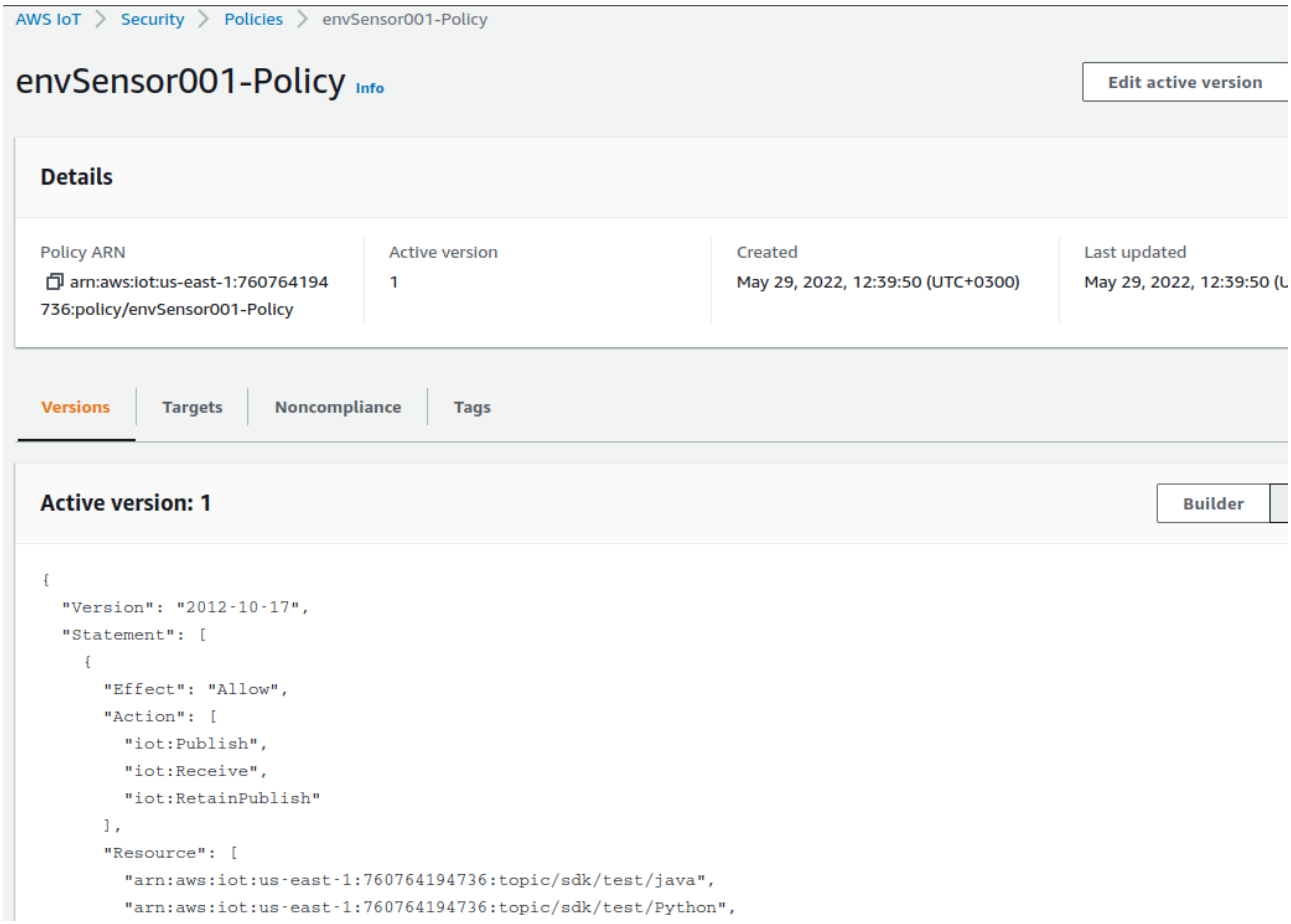

Рисунок 3.6 – Налаштування політики для датчика

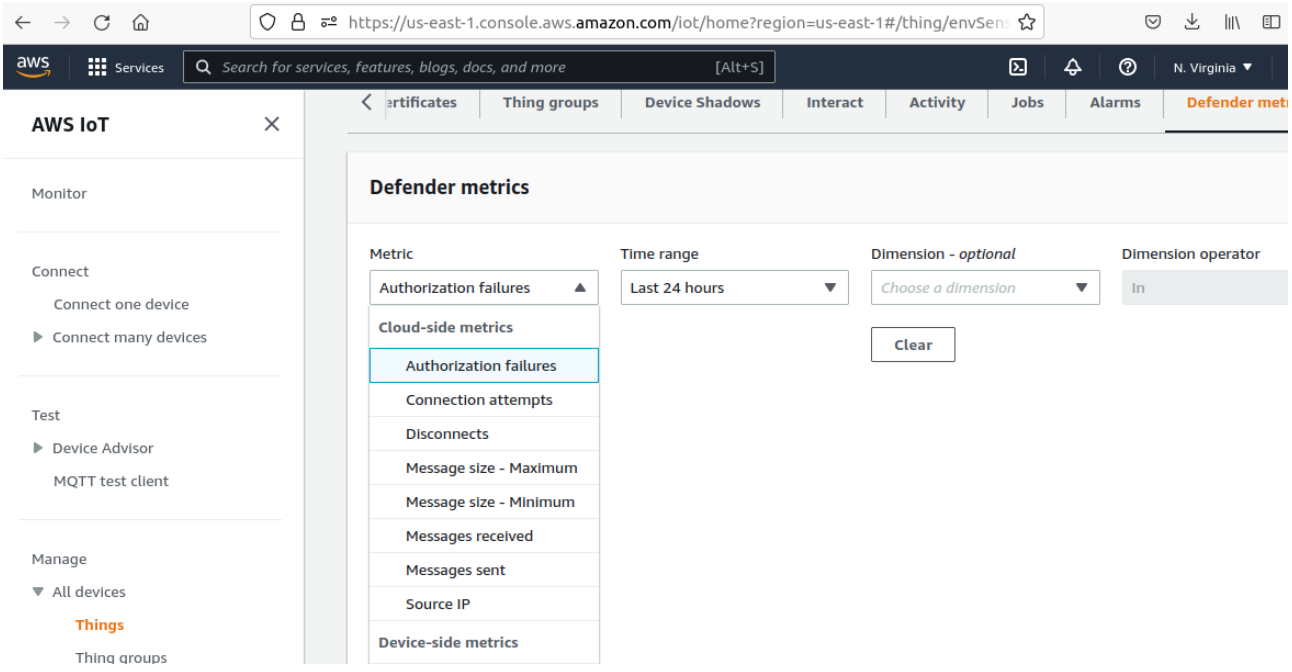

Рисунок 3.7 – Відлаштування подій, для яких відбудеться реагування і логування

Пакет підключення пристрою, як правило, містить набір криптографічних ключів (сертифікат пристрою, відкритий та закритий ключі), необхідних для встановлення безпечного з'єднання з AWS IoT Core. Крім того, пакет може включати початковий сценарій або конфігураційний файл, який містить базові налаштування (див. рис. 3.6) для підключення пристрою до сервісу та виконання тестових дій. Після того, як пристрій буде фізично підключено до мережі та завантажений необхідний програмний код, необхідно переконатися, що він успішно зареєстрований в AWS IoT Core. Для цього в консолі AWS IoT Core можна переглянути список речей (Things) та знайти в ньому запис, що відповідає вашому пристрою. Крім того, можна перевірити журнали подій, щоб переконатися, що пристрій успішно підключився та виконав необхідні дії. Кожній речі в AWS IoT Core можна привласнити політику безпеки, яка визначає, які дії може виконувати цей пристрій. Наприклад, можна обмежити права пристрою на публікацію повідомлень лише на певних темах, або заборонити йому підписуватися на певні теми. Це дозволяє забезпечити безпеку системи та запобігти несанкціонованому доступу. Базова політика для датчика (див. рис. 3.7) зазвичай надає пристрою права на публікацію повідомлень (наприклад, з даними вимірювань) та підписку на певні теми (наприклад, для отримання команд або оновлень конфігурації). Однак, для більш точного контролю над поведінкою пристрою, необхідно налаштувати політику індивідуально.

Наведений опис процесу конфігурації пристрою в AWS IoT Core підкреслює важливість використання детальних ідентифікаторів та їхнього зв'язку зі зібраними даними. Цей підхід має низку переваг для забезпечення безпеки та масштабованості IDT.

3.4 Висновки до третього розділу

Застосування методології STRIDE дозволило ідентифікувати такі основні загрози для системи IDT: несанкціонований доступ до даних, порушення цілісності даних, відмова в обслуговуванні, спотворення ідентичності, заперечення факту виконання дії та розкриття інформації а також вкритичні вразливості цифрового двійника. Для кожної загрози були визначені відповідні контрзаходи, такі як шифрування даних, автентифікація на основі сертифікатів, тощо. Для реалізації системи IDT була обрана платформа AWS IoT Core завдяки її гнучкості, масштабованості та широкому набору інтегрованих служб. AWS IoT Core дозволила легко підключити різноманітні пристрої до хмари та забезпечити безпечний обмін даними. Крім того, використання AWS Cloud9 спростило процес розробки та конфігурації системи. Для забезпечення безпеки системи мають були вжиті додаткові заходи: використання багатофакторної аутентифікації, регулярне оновлення програмного забезпечення, а також застосування систем виявлення вторгнень. Для захисту даних під час передачі використовується шифрування за протоколом TLS. Це дозволить забезпечити стійкість IDT до більшості типових кіберзагроз.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є дослідження вразливостей цифрових двійників виробничих ліній. Використання комп'ютерної техніки в будь-якій сфері діяльності вимагає неухильного дотримання норм охорони праці та техніки безпеки [49]. Зокрема, для працівників, що працюють з візуальними дисплейними терміналами, існують чіткі санітарні норми, визначені в ДСанПіН 3.3.2.007-98 "Державні санітарні норми і правила роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин". Цей нормативний документ регламентує умови праці, спрямовані на мінімізацію негативного впливу на здоров'я працівників, пов'язаного з тривалою експлуатацією електронно-обчислювальних машин (ЕОМ). Роботодавці зобов'язані забезпечити дотримання гігієнічних та ергономічних вимог до робочих місць з комп'ютерною технікою відповідно до чинного законодавства, зокрема НПАОП 0.00-7.15-18.

У контексті індустрії 4.0, де виробничі процеси все більше автоматизуються, питання безпеки набуває особливої актуальності. Інтеграція принципів безпеки має бути закладена в основу розробки та впровадження будь-якої нової технології. Це стосується як традиційних виробничих ліній, так і сучасних кіберфізичних систем, де ризики пов'язані не лише з фізичними, а й з кібернетичними загрозами. Недостатня регламентація в сфері безпеки нових технологій потребує розробки нових стандартів та норм. Інтеграція принципів безпеки в архітектуру кіберфізичних систем, систем машинного навчання та штучного інтелекту є необхідною умовою для забезпечення безпеки праці на сучасних виробництвах.

Перехід до концепції "розумного виробництва" ставить перед виробниками нові виклики, пов'язані з безпекою праці. Тісна взаємодія людини з інтелектуальними машинами та автономними системами підвищує ризики травматизму. Тому охорона праці має стати невід'ємною частиною проектування та експлуатації розумних підприємств.
Для забезпечення безпеки на розумних підприємствах необхідно:

1. Проводити комплексний аналіз потенційних загроз та оцінку ризиків.
2. Забезпечувати резервування компонентів та розробляти процедури виявлення дефектів.
3. Забезпечувати високий рівень кібербезпеки як промислового обладнання, так і інформаційних систем.
4. Розробляти методичні рекомендації щодо безпечної взаємодії людини і робота.
5. Забезпечувати персонал засобами індивідуального захисту.
6. Розвивати компетенції працівників з охорони праці.

На підприємствах металообробної галузі, які відповідають стандартам та принципам індустрії 4.0 безпека має бути інтегрована в роботизовані та автономні системи з самого початку за принципом “Security by Design”. Важливо забезпечувати надійне функціонування систем контролю та моніторингу стану обладнання, а також механізми аварійного вимкнення на випадок виходу з ладу.

Забезпечення безперебійної роботи промислових систем є критично важливим для підтримання безпечних умов праці. Надійність систем контролю та моніторингу обладнання, а також ефективність механізмів аварійного відключення є ключовими факторами у запобіганні нештатних ситуацій. Складність сучасних виробничих систем, інтегрованих з інформаційними технологіями, призводить до виникнення нових, кібернетичних загроз. Тому необхідний комплексний підхід до забезпечення

безпеки, який охоплює як фізичну, так і інформаційну інфраструктуру підприємства. Поширення концепції Індустрії 4.0 висуває нові вимоги до систем безпеки. Існуючі стандарти та норми часто не адекватно враховують специфіку нових технологій. Тому інтеграція принципів безпеки має бути закладена в основу розробки та впровадження будь-якої нової промислової системи. Комплексний підхід, що охоплює технології, процеси, нормативну базу - запорука уникнення ризиків для здоров'я та життя персоналу в високотехнологічних виробництвах майбутнього. Перехід промислових підприємств до концепції «розумного виробництва» на основі кіберфізичних систем, Інтернету Речей, хмарних обчислень та технологій штучного інтелекту ставить нові виклики в сфері охорони праці. Виробництва передбачають тісну взаємодію людини та інтелектуальних машин, автономних систем. Це підвищує ризики травматизму через можливі збої роботи обладнання, помилкові дії алгоритмів тощо. У зв’язку з цим, охорона праці має стати невід’ємною частиною проектування та функціонування розумних підприємств. Потрібний системний підхід з урахуванням специфіки нових технологій. Насамперед, необхідно проводити комплексний аналіз потенційних загроз, оцінку ризиків на етапах впровадження автоматизованих систем. Має бути передбачено резервування компонентів, процедури виявлення дефектів, системи попередження аварійних ситуацій.

Важливим є забезпечення належного рівня кібербезпеки як промислового устаткування, так і інформаційних систем управління виробництвом. Адже кібератаки здатні призвести до техногенних катастроф.

Доцільно розробити методичні рекомендації щодо безпечного застосування технологій автоматизації та роботизації у виробничих умовах, зокрема принципи безпечної взаємодії людини і робота. Не менш важливим є забезпечення персоналу засобами індивідуального захисту, що відповідають специфіці розумного виробництва. Крім того, потребують розвитку компетенції працівників з охорони праці щодо контролю безпечних

умов функціонування кіберфізичних систем та реагування на надзвичайні ситуації техногенного характеру.

Цифрові двійники відкривають нові можливості для підвищення рівня безпеки на виробництві. Вони дозволяють моделювати робочі процеси, аналізувати ризики та розробляти ефективні заходи безпеки. Застосування технологій доповненої та віртуальної реальності на основі цифрових двійників дозволяє створювати реалістичні моделі робочих зон та проводити навчання персоналу. Штучний інтелект може бути використаний для аналізу даних з датчиків та виявлення потенційно небезпечних ситуацій. Моделюючи різні сценарії функціонування обладнання, можна забезпечити тестування заходів безпеки до реального введення виробничих систем в експлуатацію. За допомогою цифрових двійників про параметри робочої зони можна в режимі реального часу здійснювати моніторинг дотримання норм охорони праці, створювати "розумне робоче місце".

4.2 Стійкість роботи платформ комп'ютерних систем виробництв в умовах надзвичайного стану

Цифрові платформи мають критичні вразливості, які можуть проявитися у воєнний час, внаслідок чого вони можуть бути пошкоджені, заблоковані, викрадені, змінені, видалені або використані проти інтересів держави, організацій або осіб. Стійкість роботи платформ IIoT є стратегічним пріоритетом для забезпечення національної безпеки. В умовах зростаючих кіберзагроз та гібридних воєн, здатність критичної інфраструктури, що базується на таких платформах, продовжувати функціонувати є гарантією стабільності економіки та суспільства. Для забезпечення стійкості платформ IIoT необхідно комплексне впровадження заходів [50], що включають:

Архітектурні рішення: розподілені системи, резервування даних, мікросегментація мережі.

Кіберзахист: використання сучасних засобів шифрування, систем виявлення вторгнень, а також навчання персоналу.

Фізичний захист: забезпечення безпеки фізичних компонентів платформи, включаючи центри обробки даних та мережеву інфраструктуру.

Планування відновлення: розробка планів відновлення після аварій та проведення регулярних тренувань.

Стійкість роботи платформ IIoT - це здатність платформ IIoT працювати надійно, безпечно, ефективно та гнучко в різних умовах, а також відновлювати свою функціональність після виникнення збоїв, помилок, атак або надзвичайних ситуацій. Стійкість роботи платформ IIoT залежить від багатьох факторів, таких як:

1. Якість та надійність пристроїв, машин, сенсорів, обладнання, систем та людей, які підключені до платформ IIoT. Ці компоненти повинні мати високу точність, швидкість, продуктивність, довговічність,

стабільність, сумісність, стандартизацію, захист, діагностику, обслуговування, оновлення, резервування тощо.

2. Якість та надійність мережевого зв'язку, який забезпечує передачу даних між компонентами платформ IIoT. Мережевий зв'язок повинен мати високу пропускну здатність, доступність, шифрування, аутентифікацію, авторизацію, контроль, моніторинг, фільтрацію, виявлення, блокування, видалення, відновлення тощо.
3. Якість та надійність хмарних сервісів, які забезпечують зберігання, обробку, аналіз, візуалізацію та використання даних з платформ IIoT. Хмарні сервіси повинні мати високу масштабованість, еластичність, гнучкість, доступність, шифрування, аутентифікацію, авторизацію, контроль, моніторинг, фільтрацію, виявлення, блокування, видалення, відновлення тощо.
4. Якість та надійність програмного забезпечення, яке забезпечує інтеграцію, координацію, автоматизацію та оптимізацію промислових процесів за допомогою платформ IIoT. Програмне забезпечення повинно мати високу функціональність, інтелектуальність, адаптивність, інтероперабельність, модульність, конфігурування, тестування, налагодження, оновлення, захист, діагностику, відновлення тощо.
5. Для підвищення стійкості роботи платформ IIoT необхідно використовувати різні методи та заходи, такі як:
6. Профілактика. Це комплекс дій, спрямованих на запобігання виникненню збоїв, помилок, атак або надзвичайних ситуацій, зниження їх імовірності та наслідків. Профілактика включає такі елементи, як: аналіз ризиків, планування, проектування, тестування, перевірка, сертифікація, стандартизація, навчання, інструктаж, контроль, моніторинг, діагностика, обслуговування, оновлення, резервування, захист, застрахування тощо.

7. Реагування. Це комплекс дій, спрямованих на ліквідацію збоїв, помилок, атак або надзвичайних ситуацій, забезпечення безпеки та відновлення роботи платформ IIoT. Реагування включає такі елементи, як: виявлення, ідентифікація, оцінка, інформування, сповіщення, мобілізація, евакуація, локалізація, ліквідація, відновлення, допомога, управління, взаємодія, забезпечення тощо.
8. Адаптація. Це комплекс дій, спрямованих на підлаштування платформ IIoT до змінних умов, використання нових можливостей, покращення якості та надійності роботи. Адаптація включає такі елементи, як: навчання, інновації, модернізація, розширення, розвиток, підтримка, зміцнення та вдосконалення.

Значну увагу слід приділяти навчанню персоналу діям у критичних ситуаціях [51] (вибухи, хімічні забруднення, вимкнення електроживлення): швидкому реагуванню на інциденти, відновленню працездатності систем після збоїв, організації роботи в умовах перебоїв з електропостачанням чи зв’язком.

Доцільно сформувати мобільні групи оперативного реагування з представників інженерних та IT-підрозділів для оперативної діагностики і усунення наслідків кібератак чи фізичних пошкоджень на об’єктах критичної інфраструктури.

Стійкість комп’ютерних систем виробництва є критично важливою для безперебійної роботи підприємства в умовах надзвичайних ситуацій. Такі події, як вибухи, хімічні забруднення або вимкнення електроживлення, можуть призвести до значних збитків та перерви у виробничому процесі. Тому, розробка та впровадження комплексу заходів для забезпечення стійкості IT-інфраструктури є необхідним кроком для будь-якого підприємства. Основні заходи заходи з забезпечення стійкості стійкості комп'ютерних систем виробництва в умовах надзвичайної ситуації (вибухи,

хімічні забруднення, вимкнення електроживлення) можна класифікувати наступним чином:

1. Резервне копіювання даних (регулярне створення повних та інкрементних резервних копій всіх критичних даних; зберігання резервних копій на віддалених серверах або зовнішніх носіях у безпечному місці; тестування процесу відновлення даних для перевірки його ефективності.
2. Забезпечення безперебійного живлення (використання джерел безперебійного живлення для захисту серверів та мережевого обладнання від перепадів напруги та короткочасних відключень електроенергії; встановлення генераторів для забезпечення тривалого електроживлення в разі тривалого відключення; розробка плану аварійного електропостачання).
3. Захист від фізичних пошкоджень (розміщення серверних кімнат у безпечних місцях, захищених від вогню, затоплення та інших фізичних впливів; використання спеціальних шаф та стійок для обладнання; встановлення систем пожежогасіння та сигналізації).
4. Захист від кіберзагроз (впровадження системи захисту інформації для запобігання кібератак та несанкціонованого доступу до даних; регулярне оновлення програмного забезпечення та операційних систем; проведення навчання персоналу з питань кібербезпеки).
5. Дублювання обладнання (створення резервних серверів та мережевого обладнання для забезпечення безперервності роботи в разі виходу з ладу основного обладнання; використання технології віртуалізації для швидкого відновлення роботи систем).
6. Відновлення після аварії (розробка детального плану відновлення після аварії - ДРПА; регулярні тренування персоналу з виконання ДРПА; створення команди швидкого реагування для ліквідації наслідків аварій).

7. Моніторинг та управління (використання систем моніторингу для контролю стану обладнання та виявлення потенційних проблем; централізоване управління IT-інфраструктурою для спрощення адміністрування та підтримки).
8. Отже, комплексний підхід до забезпечення стійкості платформ промислового IoT має охоплювати як технологічні рішення і резервування засобів, так і належну підготовку персоналу. Це дозволить мінімізувати ризики переривання важливих виробничих процесів в умовах воєнного стану.

4.3 Висновки до четвертого розділу

В даному розділі, у результаті аналізу вимог щодо охорони праці в умовах діяльності цифрових двійників промислових підприємств встановлено, що для забезпечення безпеки персоналу підприємств Індустрії 4.0, які використовують промислові цифрові двійники для розумного виробництва, необхідне ретельне дотримання вимог до охорони праці, а також необхідно проводити навчання персоналу та інформувати користувачів про потенційні наслідки для здоров’я та практику їх запобігання.

Також розглянуто питання стійкості платформ Індустрії 4.0 в умовах воєнного стану. Комплексний підхід до забезпечення стійкості цифрових двійників виробничих підприємств має охоплювати як технологічні рішення і резервування засобів, так і належну підготовку персоналу. Це дозволить мінімізувати ризики переривання важливих виробничих процесів в умовах воєнного стану.

ВИСНОВКИ

В ході виконанні кваліфікаційної робота освітнього рівня «Магістр» було проведено аналіз вразливостей промислових цифрових двійників, які можуть суттєво вплинути на безпеку цих інформаційних систем. Перевага використання цифрових двійників для малого та середнього бізнесу полягає в можливості оптимізувати виробничі процеси, забезпечити навчання персоналу та розширити можливості моделювання, виправдовуючи розробку ресурсомісткого, але важливого програмного забезпечення, призначеного для моделювання та навчання. Побудова повнофункціонального IDT дозволяє бізнесу забезпечити оптимізацію витрат та раціональне використання людського потенціалу шляхом цифровізації процесів. Розробка IDT повинна спиратися на аналіз всіх аспектів його діяльності, загроз, вразливостей та обов'язкове планування заходів кіберзахисту вже на етапі дизайну архітектури IDT. Необхідно враховувати можливості обробки даних, оптимізацію ресурсів і заходи безпеки, щоб забезпечити ефективність промислової екосистеми.

З метою оцінки ризиків для цифрових двійників в другому розділі роботи було проведено ретельний аналіз інформації щодо загроз для конкретних DT і притаманних їм вразливостей, базуючись на розумінні процесів конкретного виробництва. Для забезпечення прийняття обґрунтованих рішень і управління процесами вирішальним є збір даних за допомогою правильно вибраних, встановлених і підключених датчиків і виконавчих механізмів IoT. На сучасному етапі виникають атаки, які можна охарактеризувати як постійно змінювані, масштабні, постійні, високоскладні та надшвидкісні. Тому наявність таких атрибутів у кіберзагрозі збільшує складність необхідних запобіжних заходів.

Методологія моделювання загроз STRIDE була використана в третьому розділі роботи для ідентифікації та характеристики загроз і вразливостей,

притаманних IDT. Було визначено типи загроз безпеці для кожного елемента конкретної групи в діаграмі потоку даних архітектури IDT разом із контрзаходами, які слід застосувати для зменшення ризиків безпеки відповідно до методології STRIDE. Щоб уникнути ручного конфігурування, враховуючи доступність та функціональність, було обрано платформу AWS IoT Core, яка дозволяє налаштувати підключення пристроїв IoT до AWS Cloud та дозволяє іншим хмарним службам взаємодіяти з цим пристроєм. Для виконання операції на платформі AWS, реєстрації та конфігурування пристроїв в цьому дослідженні використано інтегроване середовище розробки AWS Cloud9.

Також в роботі були розглянуті питання з охорони праці і безпеки в надзвичайних ситуаціях.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Boyes H., Hallaq B., Cunningham J., Watson T. (2018) The industrial internet of things (IIoT): An analysis framework. Computers in Industry 101: 1-12. doi:10.1016/j.compind.2018.04.015

2. Zagorodna N., Kramar I. Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty&Co., AshokRajpath, 446 p., pp.25-39, 2020.

3. Yang Lu. (2017) Industry 4.0: A Survey on Technologies, Applications and Open Research Issues. Journal of Industrial Information Integration, 6: 1-10. doi:10.1016/j.jii.2017.04.005.

4. Skorenky Y., Voroshchuk V., Vitenko T., Kramar O. (2024) Development of digital twin interface for Industry 4.0 production line. CEUR Workshop Proceedings 3742, pp. 358–369

5. Wan J., Tang S., Shu Zh., Li D., Wang S., Imran M., Vasilakos A. (2016) Software-Defined Industrial Internet of Things in the Context of Industry 4.0. IEEE Sensors Journal. 16(20) 7373-7380. doi:10.1109/JSEN.2016.2565621

6. Skorenkyy Y., Zolotyy R., Fedak S., Kramar O., Kozak R. (2023) Digital Twin Implementation in Transition of Smart Manufacturing to Industry Practices. CEUR Workshop Proceedings 3468 :12–23.

7. Tuptuk N., Hailes S. (2018) Security of smart manufacturing systems. Journal of Manufacturing Systems 47 : 93–106.

8. Mittal S., Khan M.A., Romero D., Wuest T. (2017) Smart manufacturing: characteristics, technologies and enabling factors. Proc Inst Mech Eng Part B J Eng Manuf 10(2). http://dx.doi.org/10.1177/0954405417736547.

9. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

10. Kritzinger W., Karner M., Traar G., Henjes J. (2018) Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine, 51(11) : 1016-1022. doi:10.1016/j.ifacol.2018.08.474

11. Tao F., Zhang H., Liu A., Nee A. (2019) Digital twin in Industry: State-of-the-art. IEEE Transactions on Industrial Informatics, 15(4) : 2405-2415. doi:10.1109/TII.2018.2873186

12. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

13. Mazurkiewicz D., Smart maintenance with time series modelling and digital twin, Wydawnictwo Politechniki Lubelskiej, Lublin, 2021.

14. Fedak S., Skorenkyy Y., Dautaj M., Zolotyy R., Kramar O. (2023) Digital Twins for Optimisation of Industry 5.0 Smart Manufacturing Facilities. CEUR Workshop Proceedings 3628 : 344–349.

15. Qi Q., Tao F. (2018) Digital twin and big data towards smart manufacturing and Індустрії 4.0: 360 degree comparison. IEEE Access 6 : 3585-3593. doi:10.1109/ACCESS.2018.2793265

16. Singh M., Fuenmayor E., Hinchy E.P., Qiao Y., Murray N., Devine D. (2021) Digital Twin: origin to future. Appl. Syst. Innov. 4 : 36. doi:10.3390/asi4020036

17. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

18. Digital twins [Електронний ресурс]. URL: https://www.ibm.com/topics/what-is-a-digital-twin

19. Mazurkiewicz D., Yi Ren, Cheng Qian. (2023) Novel Approach to Prognostics and Health Management to Combine Reliability and Process Optimisation. Springer Series in Reliability Engineering, in: Yu Liu & Dong Wang

& Jinhua Mi & He Li (ed.), Advances in Reliability and Maintainability Methods and Engineering Applications, Springer, 559-580.

20. Lee J., Kao H.-A., Yang S. (2014) Service innovation and smart analytics for Industry 4.0 and big data environment. Procedia CIRP 16 : 3-8. doi:10.1016/j.procir.2014.02.001

21. Digital Twins for Industrial Applications. An Industrial Internet Consortium White Paper Version 1.0. 2020-02-18, [Електронний ресурс]. URL: https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf

22. Korves B. (2015) The Future of Manufacturing – On the way to Industry 4.0. Siemens AG [Електронний ресурс]. URL: https://assets.new.siemens.com/siemens/assets/api/uuid:558e2625-d63c-4567-9bb0-1553ae567ff2/presentation-e.pdf

23. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

24. EFFRA, The European Factories of the Future Research Association. Digital Manufacturing Platforms. [Електронний ресурс]. URL: https://www.effra.eu/digital-manufacturing-platforms

25. BMWi, Federal Ministry for Economic Affairs and Energy. Benefits of Application Scenario Value-Based Service. [Електронний ресурс]. URL: https://www.plattformi40.de/PI40/Redaktion/DE/Downloads/Publikation/benefits-application

26. Flechais I., Sasse M.A., Hailes S.M.V. (2003) Bringing Security Home: a process for developing secure and usable systems. Proceedings of the 2003 workshop on New Security Paradigms, NSPW ‘03. 49–57. ISBN 1-58113-880-6.

27. Clim A. (2019) Cyber security beyond the Industry 4.0 era. A short review on a few technological promises, Informatica Economică 23: 2.

28. Urciuoli L., Mannisto T., Hintsa J., Khan T. (2013) Supply Chain Cyber Security - Potential Threats. Information & Security: An International Journal, 29 : 51-68.

29. Viega J, McGraw G. (2006) Building secure software: how to avoid security problems the right way. Addison Wesley. ISBN 978-0321425232.

30. Fovino I., Carcano A., De Lacheze Murel T., Trombetta A., Masera M. (2010) Modbus/DNP3 state-based intrusion detection system. 2010 24th IEEE international conference on advanced information networking and applications (AINA) 2010:729–36.

31. Burton G. (2017) BrickerBot: Mirai-like Malware threatens to brick insecure IoT devices. [Електронний ресурс]. URL: https://www:theinquirer:net/inquirer/news/3008037/brickerbot-mirai-like-malware-threatens-to-brick-insecure-iot-devices.

32. Page C. (2017) A new IoT Botnet storm is coming. [Електронний ресурс]. URL: https://research.checkpoint.com/new-iot-botnet-storm-coming/.

33. Wang J.K., Peng C. (2017) Analysis of time delay attacks against power grid stability. Proceedings of the 2nd workshop on cyber-physical security and resilience in smart grids, CPSR-SG‘17. New York, NY, USA: ACM.; 67–72. http://dx.doi.org/10.1145/3055386.3055392. ISBN 978-1-4503-4978-9.

34. Tuptuk N., Hailes S. (2015) Covert channel attacks in pervasive computing. 2015 IEEE international conference on pervasive computing and communications (PerCom) 2015:236–42. http://dx.doi.org/10.1109/PERCOM.2015.7146534.

35. Arreno M., Nelson B., Joseph A.D., Tygar J.D. (2010) The security of machine learning. Mach Learn 81(2):121–48. http://dx.doi.org/10.1007/s10994-010-5188-5.

36. Biggio B., Fumera G., Russu P., Didaci L., Roli F. (2015) Adversarial biometric recognition: a review on biometric system security from the adversarial

machine-learning perspective. IEEE Signal Process Mag 32(5):31–41. http://dx.doi.org/10.1109/MSP.2015.2426728. ISSN 1053-5888.

37. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

38. Breaking Down Mirai: an IoT DDoS Botnet analysis 2016 [Електронний ресурс]. URL: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

39. Tuptuk N., Hailes S. (2016) The cyberattack on Ukraine's power grid is a warning of what's to come. [Електронний ресурс]. URL: https://theconversation.com/the-cyberattack-on-ukraines-power-grid-is-a-warning-of-whats-to-come-52832.

40. Havex Hunts for ICS/SCADA systems. 2014[Електронний ресурс]. URL: https://www.f-secure.com/weblog/archives/00002718.html.

41. Dragonfly: cyber espinoage attacks against energy suppliers. 2014. [Електронний ресурс]. URL: https://docs.broadcom.com/docs/dragonfly_threat_against_western_energy_suppliers

42. W32.Stuxnet Dossier (Version 1.4), Tech. Rep. 2011. [Електронний ресурс]. URL: http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32_stuxnet_dossier.pdf

43. ENISA: Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2019 [Електронний ресурс]. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

44. Pochmara J., Świetlicka A. (2024) Cybersecurity of Industrial Systems—A 2023 Report. Electronics 13 : 1191.

45. Understanding IoT Security – Part 2 of 3: IoT Cyber Security for Cloud and Lifecycle Management [Електронний ресурс]. URL: https://iot-analytics.com/understanding-iot-cyber-security-part-2/

46. Industrial Control Systems [Електронний ресурс]. URL: https://www.cisa.gov/topics/industrial-control-systems

47. Lotfi ben Othmane. On Continuous Threat Modeling of Cyber-physical Systems. [Електронний ресурс]. URL:https://works.bepress.com/lotfi-benothmane/

48. Khan R., McLaughlin K., Laverty D., Sezer S. (2018) STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc. 1-6. DOI: 10.1109/ISGTEurope.2017.8260283.

49. Бедрій Я.І. Безпека життєдіяльності: Навч.посібн. – К.: Вид-во Кондор, 2009.

50. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ» / В.С. Стручок – Тернопіль: ФОП Паляниця В. А., –156 с. Отримано з https://elartu.tntu.edu.ua/handle/lib/39196.

51. Навчальний посібник «ТЕХНОЕКОЛОГІЯ ТА ЦИВІЛЬНА БЕЗПЕКА. ЧАСТИНА «ЦИВІЛЬНА БЕЗПЕКА»» / автор-укладач В.С. Стручок– Тернопіль: ФОП Паляниця В. А., – 156 с. Отримано з https://elartu.tntu.edu.ua/handle/lib/39424.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 004.056
М. Копач; Ю. Скоренький, к.ф.-м.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ЦИФРОВИХ ДВІЙНИКІВ ВИРОБНИЧИХ ЛІНІЙ МЕТАЛООБРОБНИХ ПІДПРИЄМСТВ

UDC 004.056
M. Kopach; Yu. Skorenkyy, Ph.D., Assoc. Prof.

STUDY OF VULNERABILITIES OF DIGITAL TWINS OF THE METAL PROCESSING ENTERPRIZES

Ключові слова: інформаційна безпека, промисловий інтернет речей, вразливості.
Key words: information security, industrial internet of things, vulnerability.

Поява Інтернету речей (Internet of Things, IoT) проклала шлях до нових можливостей для вдосконалення промислових процесів за допомогою інтеграції та складного керування машинами та приводами, обладнаними датчиками. У технологічних процесах промисловий Інтернет речей дає виробникам можливість отримати всебічне уявлення про кожен етап виробничого процесу, сприяючи коригуванням у реальному часі для забезпечення безперебійного виробництва та зниження ймовірності дефектів і збоїв, спричинених людськими помилками, відповідно до принципів Індустрії 4.0. Позитивні наслідки інтелектуального виробництва виходять за рамки виробничих операцій, обладнання та оптимізації запасів. Цифрові близнюки (Digital Twin, DT), які широко використовуються в Індустрії 4.0 для моделювання та керування виробничими процесами [1], є віртуальними копіями фізичних об'єктів або систем. Перевага використання цифрових двійників для малого та середнього бізнесу полягає в можливості оптимізувати виробничі процеси, забезпечити навчання персоналу та розширити можливості моделювання, виправдовуючи розробку ресурсомісткого, але важливого програмного забезпечення, призначеного для моделювання та навчання.

Для металообробного виробництва з високим рівнем цифровізації промислове моделювання на основі даних дозволяє розробити відповідну архітектуру цифрового двійника. Зібрані дані та оброблена інформація є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

В даній роботі представлено аналіз вразливостей [2] промислових цифрових двійників, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Література

1. Skorenky Yu. et al. Development of digital twin interface for Industry 4.0 production line. CEUR Workshop Proceedings, 2024, 3742, pp. 358–369
2. R. Khan, K. McLaughlin, D. Laverty, S. Sezer. STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc. (2018) 1-6. URL: https://doi.org/10.1109/ISGTEurope.2017.8260283