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 платформ промислового інтернету речей

Виконав: студент VI курсу, групи СБмз-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Карпець М.Р. (прізвище та ініціали)

Керівник (підпис) Александер М.А. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

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

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

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)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Карпцю Миколі Романововичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження вразливостей платформ промислового інтернету речей

Керівник роботи Александер Марек-Богуслав Антонович, д.т.н., професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_16_» _листопада_ 2023 року № _4/7-1060_

2. Термін подання студентом завершеної роботи 14 грудня 2023р.

3. Вихідні дані до роботи Наукові публікації про особливості функціонування платформ промислового інтернету речей

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Область застосування та основні принципи роботи промислового інтернету речей, 1.1 Індустрія 5.0 як новий етап промислового розвитку, 1.2 Технологічні можливості промислового інтернету речей, 1.3 Комунікаційні системи промислового інтернету речей, 1.4 Концепція цифрових двійників, 1.5 Висновки до першого розділу, 2 Проблеми безпеки систем промислового інтернету речей, 2.1 Основні проблеми безпеки вбудованих систем, 2.2 Аспекти кібербезпеки промислового інтернету речей, 2.3 Вразливості, характерні для цифрових двійників, 2.4 Висновки до другого розділу, 3 Практичне дослідження вразливостей промислового інтернету речей, 3.1 Моделі систем промислового інтернету речей, 3.3 Планування заходів з протидії вразливостям, 3.3 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. Цифрові двійники в Індустрії 5.0, 4. Найважливіші вразливості систем ітернету речей, 5. Класифікація вразливостей OWASP, 6. Набір протоколів IoT Protocol Suite, 7. Структура кібербезпеки NIST, 8. Рівні критичності вразливостей, 9. Реалізація та наслідки атаки, 10. Екосистема AWS IoT Core як спосіб автоматизувати захист платформи IioT, 11. Вразливості безпеки та засоби протидії для промислового інтернету речей, 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 17 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	17.11.2023-19.11.2023	*Виконано*
2.	Підбір наукових джерел про пристрої IIoT	20.11.2023-23.11.2023	*Виконано*
3.	Переклад та опрацювання наукових джерел		
	про платформи промислового інтернету речей	24.11.2023-26.11.2023	*Виконано*
4.	Виконання дослідження щодо аналізу вразливостей цифрових двійників	27.11.2023-27.11.2023	*Виконано*
5.	Оформлення розділу «Область застосування та		
	основи роботи промислового інтернету речей»	28.11.2023-30.11.2023	*Виконано*
6.	Оформлення розділу «Проблеми безпеки систем		
	промислового інтернету речей»	01.12.2023-04.12.2023	*Виконано*
7.	Оформлення розділу «Практичне дослідження		
	вразливостей систем промислового інтернету речей»	05.12.2023-07.12.2023	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2023-09.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2023-11.12.2023	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2023-13.12.2023	*Виконано*
11.	Нормоконтроль	15.12.2023-16.12.2023	*Виконано*
12.	Перевірка на плагіат	14.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	28.12.2023	

Студент _____ Карпець М.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер М.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження вразливостей платформ промислового інтернету речей // Кваліфікаційна робота освітнього рівня «Магістр» // Карпець Микола Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2023 // С. 45, рис. – 10, табл. – 1, додат. – 1, бібліогр. – 19.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНТЕРНЕТ РЕЧЕЙ, ЦИФРОВИЙ ДВІЙНИК, ВРАЗЛИВОСТІ.

Кваліфікаційна робота присвячена аналізу ризиків при використанні цифрових двійників, які є важливими компонентами розумного виробництва.

У першому розділі зроблено аналіз особливостей роботи пристроїв промислового інтернету речей. Розглянуто типи цифрових двійників та їх застосування в розумному виробництві (Індустрії 5.0).

В другому розділі розглядаються проблеми безпеки цифрових двійників виробничих ліній та атаки на них.

У третьому розділі проведено дослідження вразливостей платформ промислового інтернету речей та розроблено рекомендації щодо протидії вразливостям.

Четвертий розділ присвячено проблемам охорони праці та безпеки в надзвичайних ситуаціях.

ANNOTATION

Research on Vulnerabilities in Industrial Internet of Things Platforms // Qualification work of the educational level “Master” // Mykola Karpets // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, СБмз-61 group // Ternopil, 2023 // P. 45, fig. - 10, tables - 1, annexes -1, references - 19.

Key words: INFORMATION SECURITY, INTERNET OF THINGS, DIGITAL TWIN, VULNERABILITIES

Qualification work devoted to the analysis of risks in the use of digital twins, which are essential components of smart manufacturing.

In the first chapter, an analysis of the features of the industrial Internet of Things devices is made. The types of digital twins and their application in smart manufacturing (Industry 5.0) are considered.

The second chapter deals with security issues of digital twins of production lines and attacks on them.

In the third chapter, a study of the vulnerabilities of the Industrial Internet of Things platform was conducted and recommendations were developed to counter vulnerabilities.

The fourth chapter is devoted to the problems of labor protection and safety in emergency situations.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CAD – Computer-Aided Design (автоматизоване проектування).

CAE – Computer-Aided Engineering (автоматизована розробка).

CAM – Computer-Aided Manufacturing (автоматизоване виробництво).

DT – Digital Twin (цифровий двійник)

IDT – industria digital twin (платформа промислового ціфрового двійника)

IoT – Internet of Things (інтернет речей).

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

IT – Information Technology (інформаційні технології).

LPWAN - Low-power Wide Access Network

ПЗ – програмне забезпечення.

НС – надзвичайна ситуація.

ШІ – штучний інтелект.

ЗМІСТ

ВСТУП

Актуальність теми. Розумна промисловість, яка є мережею інтелектуальних виробничих підприємств, пов’язаних за допомогою інформаційно-комунікаційних технологій з дослідниками та розробниками, постачальниками, дистриб’юторами та споживачами, є системою зі складною мережевою взаємодією. Саме завдяки цим взаємодіям обробка детальних даних, отриманих за допомогою інформаційно-комунікаційних технологій у режимі реального часу про фактичний стан будь-якого даного процесу, від замовлення до постачання продукції, дозволяє забезпечити гнучкість виробництва відповідно до вимог. Найбільше страждають сфери господарської діяльності, які за своїми техніко-технологічними характеристиками краще адаптовані до цифрового етапу вдосконалення виробництва та організації управління. Це, перш за все, ті галузі, де широко застосовуються спеціалізовані стандартизовані виробничі процеси та продукція (машинобудування, харчова промисловість, хімія, металургія тощо). Галузі, виробниче середовище яких характеризується високою складністю та варіативністю технологічних процесів (фармацевтика, хімія, гірничодобувна промисловість), також мають хороший потенціал, а отже, мають хороші можливості для ефективного використання великих даних для їх вдосконалення.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є дослідження ризиків пов’язаних із застосуванням платформ промислового інтернету речей в Індустрії 5.0.

Для досягнення поставленої мети було потрібно виконати такі завдання:

- проаналізувати завдання та предметну область;
- з’ясувати характерні особливості платформ промислового інтернету речей;

- проаналізувати способи запобігання загрозам, специфічним для цифрових двійників промислового обладнання;
- дослідити роботу та спланувати захисту для цифрових двійників;
- розробити висновки стосовно можливих шляхів забезпечення конфіденційності, незмінності та доступності даних, які передаються через платформи даних розумного виробництва.

Об'єкт дослідження. Процеси захисту інформації у платформах промислового інтернету речей.

Предмет дослідження. Вразливості цифрових двійників промислового обладнання.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що проведено аналіз вразливостей платформ промислового інтернету речей.

Практичне значення одержаних результатів. Розроблено рекомендації щодо захисту цифрових двійників промислового обладнання.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на X науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 13 – 14 грудня 2023 р.

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

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури із 31 найменувань та 1 додатка. Загальний обсяг кваліфікаційної роботи складає 60 сторіноку, з них 58 сторінок основного тексту, який містить 14 рисунки та 3 таблиці.

1 ОБЛАСТЬ ЗАСТОСУВАННЯ ТА ОСНОВИ РОБОТИ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

У технологічних операціях компоненти та платформи промислового інтернету речей (IIoT) дозволяють виробникам отримати повну інформацію про те, що відбувається на кожному етапі виробництва, щоб забезпечити плавний потік та уникнути дефектів [1-7]. Проблеми можна вирішувати в реальному часі та запобігати збоям, зменшуючи ймовірність людської помилки. Розумне виробництво також може продемонструвати високі результати, необхідні для погашення високих витрат на створення, експлуатацію та кібербезпеку, завдяки кращому врахуванню вимог споживачів, які висувають все більш високі вимоги до якості продукції, їх активної участі в проектуванні та інжиніринг продукції, перехід у цій комунікації від масового сучасного продукування до кастомного (за індивідуальними замовленнями) із використання розумних систем управління взаємовідносинами з клієнтами, а також гнучкість вузькоспеціалізованого автоматизованого (з мінімальним втручанням людини) виробництва, побудованого відповідно до децентралізований модульний принцип і пристосований до швидкої переналаштування для виробництва саме того продукту, який в даний момент потрібен споживачеві. Особливо важливо використовувати високий потенціал і креативність персоналу, який здатний творчо виконувати функції обслуговування, контролю та подальшого вдосконалення виробничих кіберфізичних систем, що є вирішальним чинником переходу виробництва до Індустрії 5.0.

1.1 Індустрія 5.0 як новий етап промислового розвитку

Цифрова трансформація відкриває нові можливості для сучасного промислового виробництва, яке знаходиться на етапі розвитку, відомому як Індустрія 4.0. Для цього етапу характерне широке впровадження автоматизації та комп'ютеризації. Наступний етап, елементи якого зараз розробляються і частково впроваджуються, називають Індустрією 5.0 [5-7].

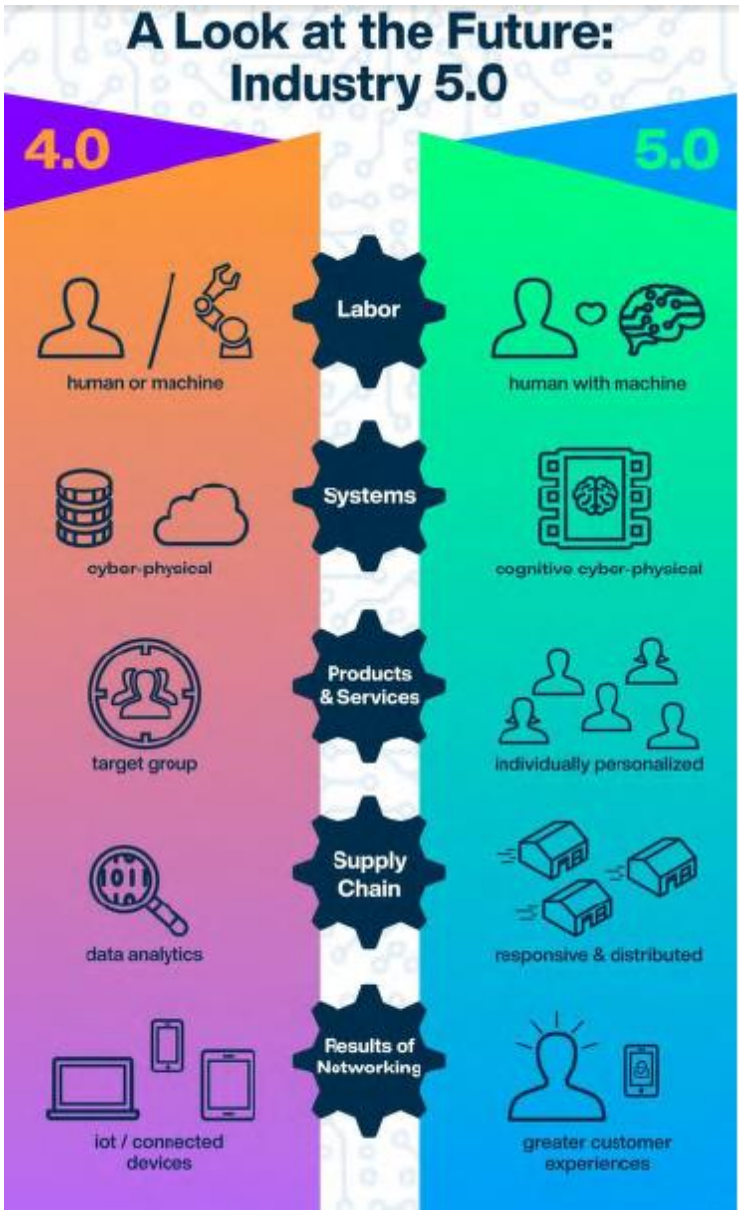

Рисунок 1.1 – Відмінності Індустрії 5.0 в порівнянні з Індустрією 4.0 [8] .

Цей етап вимагає запровадження людиноцентричних підходів, збалансованого стійкого господарювання та більш глибокої цифровізації, яка передбачає насамперед комплексний аналіз та інтеграцію цифрових технологій у всі процеси підприємства. Індустрію 5.0 слід розглядати не як альтернативу існуючій парадигмі індустрії 4.0, а як доповнення (див. рис. 1.1). Фактично, мета залишається незмінною – допомогти галузям оцифруватися та прийняти нові передові технології, але додає три ключові компоненти:

- Людиноцентричний підхід. Індустрія 5.0 визнає важливість не лише досягнення високої продуктивності, але й створення безпечного та інклюзивного робочого середовища, де здоров'я та благополуччя людини є пріоритетом;
- Стійкість. Можливість швидкої адаптації до змін має вирішальне значення для компаній Індустрії 5.0, які хочуть залишатися конкурентоспроможними в мінливому світі невизначеності (нові технології, зміна потреб ринку);
- Екологічний розвиток полягає у впровадженні циркулярних процесів, які дозволяють повторне використання, перепрофілювання та переробку природних ресурсів, зменшення відходів і шкоди навколишньому середовищу, а також підвищення ефективності наших виробничих процесів.

Застосовуючи діджитал-технології, компанії Індустрії 5.0 зможуть покращити продуктивність і ефективність. Автоматизація, аналітика даних і штучний інтелект – це лише деякі приклади технологій, які можуть оптимізувати роботу, підвищити продуктивність і зменшити витрати. Цифрова трансформація також допомагає організаціям адаптуватися до мінливої ринкової динаміки, зміни очікувань клієнтів та швидкого технологічного прогресу.

Поширеною проблемою є інтеграція нових технологій із існуючими застарілими системами, що ставить під загрозу цілісність та безпеку даних.

Управління даними та кібербезпека є критично важливими аспектами цифрової трансформації. Зі збільшенням залежності від прийняття рішень на основі даних і впровадження таких технологій, як штучний інтелект і машинне навчання, організації повинні вирішувати питання конфіденційності даних, безпеки та відповідності стандартам.

1.2 Технологічні можливості пристроїв інтернету речей

Інтернет речей (IoT) - це мережа фізичних пристроїв, які можуть обмінюватися даними між собою та з іншими системами через інтернет [1]. IoT має великий потенціал для покращення різних сфер життя, таких як промисловість, медицина, освіта, розваги, безпека, екологія та інші. Для реалізації цього потенціалу, пристрої IoT повинні мати такі технологічні можливості:

- Збір даних. Це можливість отримувати дані з різних пристроїв, таких як датчики, камери, мікрофони, GPS, RFID, NFC тощо. Збір даних дозволяє вимірювати різні параметри, такі як температура, вологість, тиск, рух, світло, звук, положення, швидкість, напрямок, ідентифікація тощо.
- Передача даних. Це можливість відправляти дані з пристроїв IoT до інших пристроїв, систем або хмарних сервісів через інтернет або локальні мережі. Передача даних дозволяє зв'язувати різні компоненти IoT між собою та з іншими системами, такими як смартфони, комп'ютери, сервери, бази даних, веб-сайти, додатки тощо.
- Обробка даних. Це можливість аналізувати, фільтрувати, класифікувати, агрегувати, візуалізувати, інтерпретувати та використовувати дані, отримані з пристроїв IP. Обробка даних дозволяє отримувати корисну інформацію, знання, ухвалювати рішення, виробляти стратегії, виявляти закономірності, прогнозувати події, вирішувати проблеми тощо.
- Виконання дій. Це можливість впливати на реальний світ за допомогою пристроїв IP, які мають виконавчі механізми, такі як реле, мотори,

світлодіоди, динаміки, екрани, клапани, насоси тощо. Виконання дій дозволяє контролювати різні процеси, такі як включення, вимикання, регулювання, перемикання, переміщення, зміна, відтворення, відображення тощо.

1.3 Комунікаційні системи промислового інтернету речей

Комунікаційні системи IIoT - це технології [8,9], які забезпечують зв'язок між різними компонентами IIoT, а також між IIoT та іншими системами, такими як хмарні сервіси, мобільні пристрої, веб-сайти, додатки тощо.

Комунікаційні системи IIoT мають такі особливості:

- Різноманітність та гетерогенність. Комунікаційні системи IIoT повинні підтримувати різні типи, формати, протоколи, стандарти та інтерфейси даних, які використовуються на різних пристроях, машинах, сенсорах, обладнанні, системах та людях, які підключені до IIoT (рисунок 1.2). Комунікаційні системи IIoT повинні забезпечувати сумісність, інтероперабельність, адаптацію, конвертацію, трансляцію, агрегацію, синхронізацію та координацію різних даних.
- Висока пропускна здатність та низька затримка. Комунікаційні системи IIoT повинні забезпечувати швидку та надійну передачу великих обсягів даних між різними компонентами IIoT, а також між IIoT та іншими системами. Комунікаційні системи IIoT повинні мінімізувати час, який потрібен для передачі даних від джерела до призначення, який залежить від відстані, пропускної здатності, навантаження, протоколів, шифрування, фільтрації, буферизації тощо. Висока пропускна здатність та низька затримка даних впливають на якість та ефективність взаємодії між людьми та машинами, а також на можливість виявлення, реагування та адаптації до змін у середовищі.

• Висока стійкість та безпека. Комунікаційні системи IIoT повинні бути стійкими до різних загроз, таких як помилки, збої, атаки, надзвичайні ситуації, які можуть призвести до порушення, пошкодження, втрати, зміни, викрадення, розголошення або зловживання даними. Комунікаційні системи IIoT повинні забезпечувати захист даних від несанкціонованого доступу, втручання, модифікації, видалення або використання. Комунікаційні системи IIoT повинні також відновлювати свою функціональність після виникнення збоїв, помилок, атак або надзвичайних ситуацій.

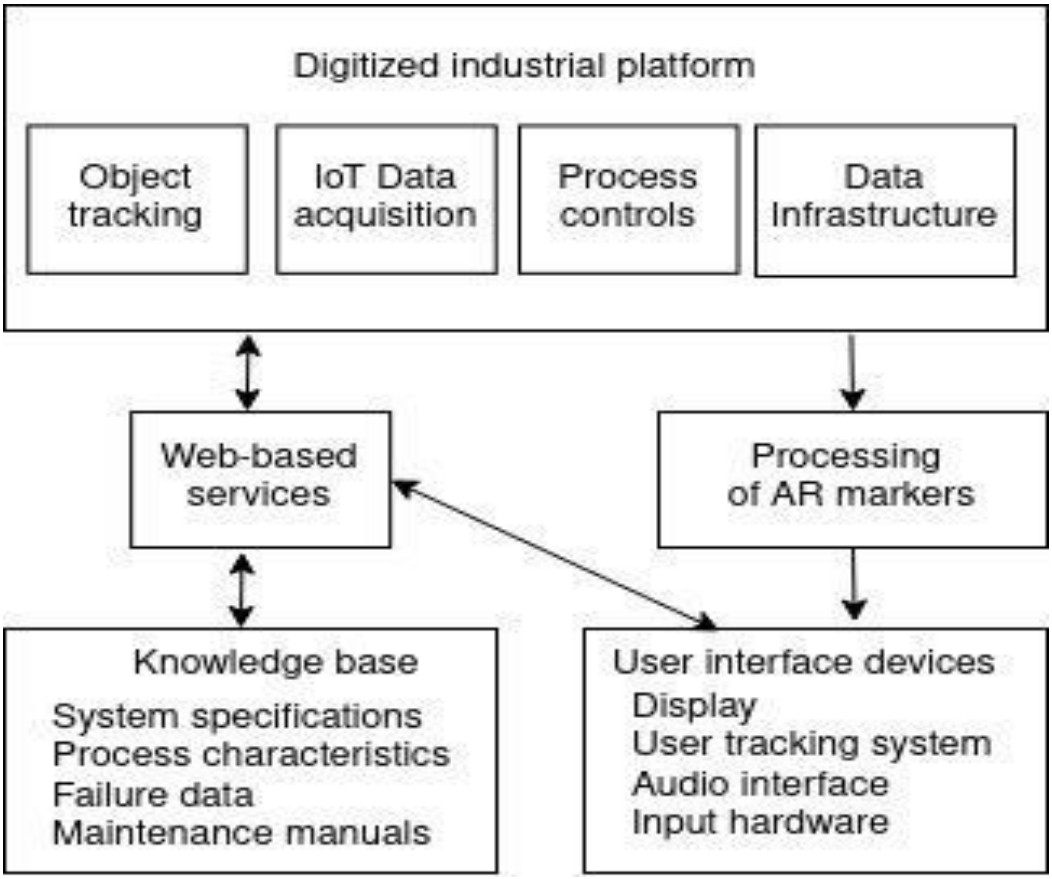

Рисунок 1.2 – Взаємозв’язки в рамках цифрової платформи розумного виробництва [2].

В комунікаційній підсистемі промислового інтернету речей можна виділити кілька рівнів (рисунок 1.3):

Рівень кінцевих вузлів:

Цей рівень складається з датчиків, приводів, тегів RFID, машин тощо, які складають «речі» в системі IIoT. Ці кінцеві вузли сприймають дані або виконують дії.

Рівень підключення:

Рівень підключення забезпечує підключення між кінцевими вузлами та крайовими пристроями/шлюзами. Він включає такі технології, як WiFi, Bluetooth, радіо LPWAN, 5G тощо.

Крайовий шар:

Це включає периферійні пристрої та крайові шлюзи. Вони агрегують дані з кінцевих вузлів, виконують локальний аналіз і обробку, а також передають дані на рівень платформи. Граничні обчислення зменшують використання пропускної здатності.

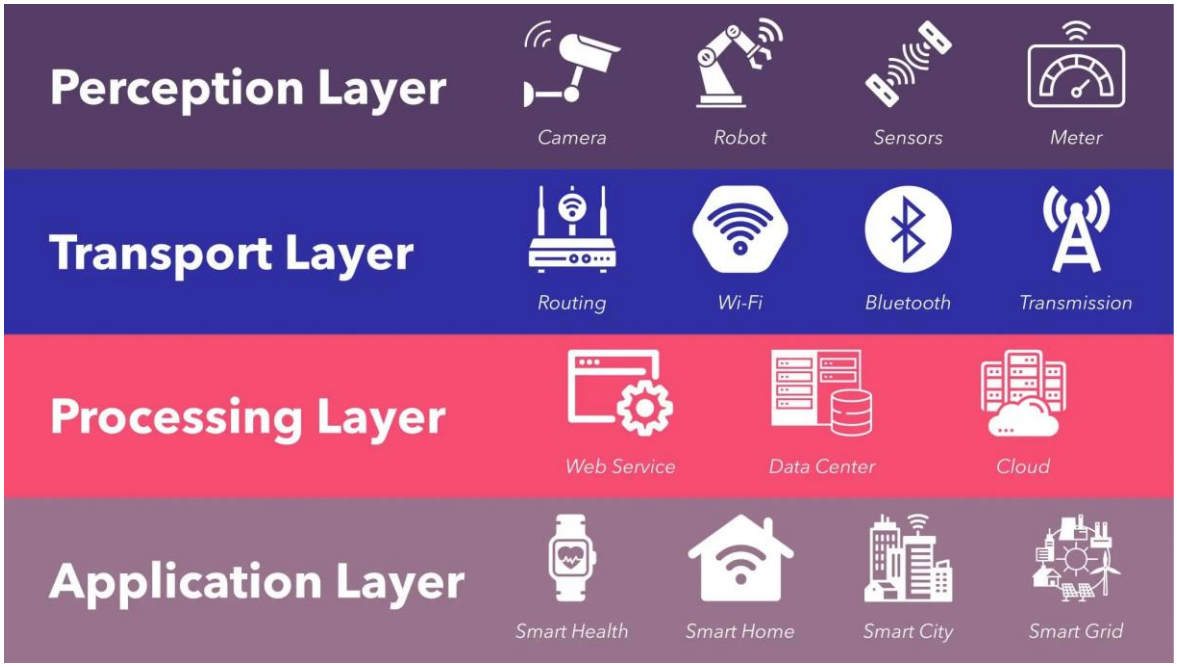

Рисунок 1.3 – Рівні комунікаційної системи промислового інтернету речей [10].

Рівень платформи:

Рівень платформи отримує проаналізовані/оброблені дані з периферійного рівня та зберігає їх. Він включає рішення для керування

пристроями, активації додатків, керування даними, аналітики тощо. Хмарні платформи є частиною цього рівня.

Рівень програми:

Цей найвищий рівень включає додатки IIoT, які використовують дані для надання бізнес-аналізу, аналітики, моніторингу, контролю тощо.

Кібербезпека систем IIoT - це комплекс заходів, які спрямовані на захист даних, пристроїв, систем та людей від різних кіберзагроз, таких як помилки, збої, атаки, надзвичайні ситуації, які можуть призвести до порушення, пошкодження, втрати, зміни, викрадення, розголошення або зловживання інформацією, ресурсами, функціями або безпекою систем IIoT.

Аспекти кібербезпеки систем IIoT можна розглядати з різних точок зору, таких як:

- Технічний аспект. Це аспект, який стосується технологій, які використовуються для забезпечення кібербезпеки систем IIoT, таких як шифрування, аутентифікація, авторизація, контроль, моніторинг, діагностика, виявлення, блокування, видалення, відновлення, оновлення, резервування тощо. Технічний аспект включає також вибір, проектування, розробку, тестування, впровадження, експлуатацію, підтримку, вдосконалення та інновацію технологій кібербезпеки систем IIoT.
- Організаційний аспект. Це аспект, який стосується організацій, які володіють, управляють, експлуатують, підтримують, вдосконалюють та інновують системи IIoT, а також організацій, які взаємодіють з ними, таких як клієнти, партнери, постачальники, регулятори, конкуренти, зловмисники тощо. Організаційний аспект включає також планування, управління, координацію, комунікацію, документацію, аналіз, оцінку, контроль, аудит, реагування, відновлення, навчання, адаптацію та інші процеси, які пов'язані з кібербезпекою систем IIoT.
- Правовий аспект. Це аспект, який стосується правових норм, які регулюють діяльність, пов'язану з системами IIoT, таких як закони,

нормативні акти, стандарти, політики, правила, договори, ліцензії, сертифікати, патенти, авторські права, торгові марки тощо. Правовий аспект включає також захист прав та інтересів організацій та осіб, які беруть участь у використанні, розробці, впровадженні, підтримці, вдосконаленні та інновації систем IIoT, а також вирішення спорів, конфліктів, порушень, санкцій, відшкодувань тощо, які пов'язані з кібербезпекою систем IIoT.

1.4 Концепція цифрових двійників

Цифровий двійник (DT) може представляти об’єкти різних типів за допомогою комп’ютерного моделювання в різних режимах моделювання. По суті, цифровий двійник імітує об’єкти (див. рис. 1.4) та їхні структурні/функціональні зв’язки, у цифровому вигляді представляючи його функціонування.

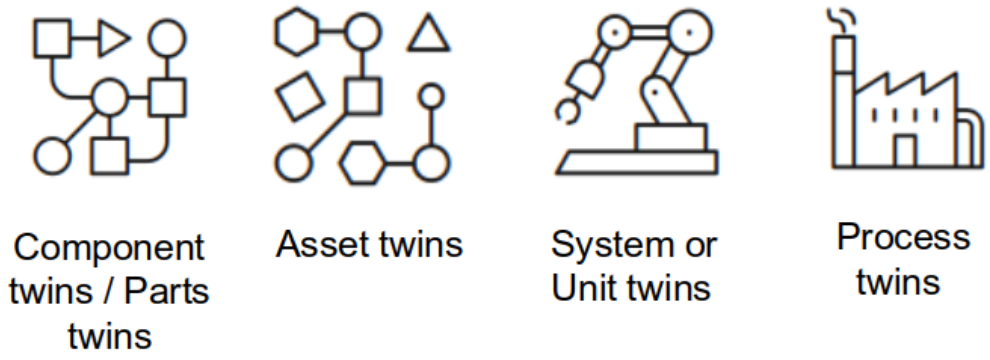

Рисунок 1.4 – Типи цифрових двійників [11].

У виробничому секторі DT зазвичай асоціюється з віртуальним введенням в експлуатацію - найбільш актуальною технологічною тенденцією - розробкою складних продуктів, які також вимагають гнучких виробничих процесів або додаткових компонентів і послуг для таких продуктів. Застосування DT веде до кращого контролю над різними етапами проектування та, як наслідок, до можливості обговорення продукту, коли він ще не реалізований, зменшуючи ризик відсутності вимог, які запитують клієнти. Крім того, наявність доступу до цифрового двійника зменшує

бар’єри входу на ринок компонентів і підвищує точність і надійність моделювання та тестування результатів у ланцюжку створення вартості.

Сучасне промислове виробництво має чітку тенденцію до широкого залучення цифрових інструментів, які використовують Інтернет речей для реалізації таких концепцій інтелектуального виробництва, як дистанційне технічне обслуговування, розширений зв’язок між машинами, формування гнучкої, адаптивної та автономної кіберфізичної системи промислового типу. системи. Важливим аспектом Інтернету речей є можливість розробки гібридних рішень, які здатні поєднувати фізичні продукти з цифровими послугами, зокрема через мобільні пристрої.

Загальноприйняте визначення Національного інституту стандартів і технологій передбачає, що для того, щоб система вважалася «розумною», вона має бути спільним виробничим об’єктом, здатним миттєво реагувати на зміни умов і попиту. Відмінною рисою цифрових двійників, які визначаються як віртуальні моделі систем реального світу, є зв’язок між одиницями продуктивної системи. Цифрові двійники використовують дані датчиків для керування виробничими процесами, керування інструментами та обладнанням, а також забезпечують підтримку прийняття рішень людьми-операторами [13] на різних етапах життєвого циклу продукту [14]. Моделі та програмне забезпечення створені для роботи з даними, зібраними з фізичних речей, для проектування цифрового двійника.

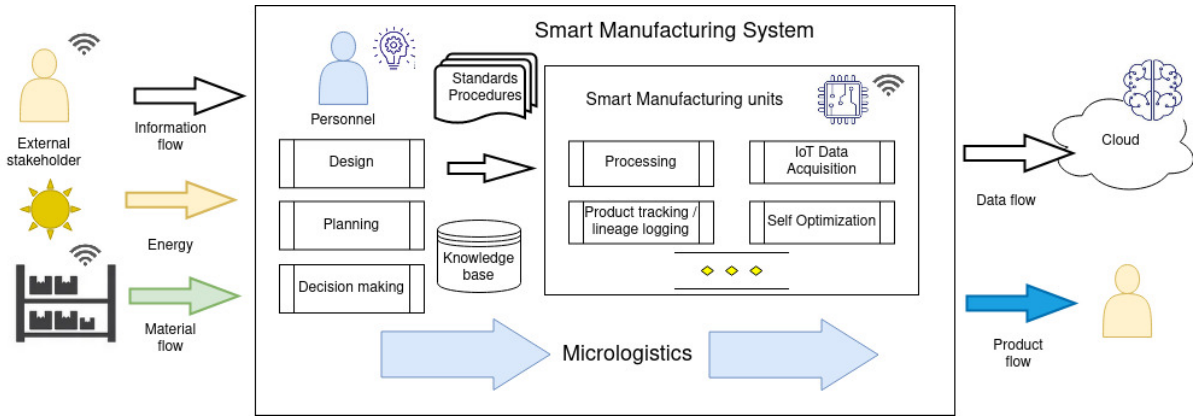

Рисунок 1.5 – Відображення матеріальних потоків, потоків даних і конкретних операцій в моделі цифрового двійника [11].

Розумне виробництво можна розглядати як продукт взаємодії обладнання, зібраних і оброблених даних, алгоритмів, штучного інтелекту та людської творчості. Дані, отримані від датчиків, внутрішніх і зовнішніх джерел, збираються, обробляються, візуалізуються та використовуються для моделювання промислових продуктів і виробничих процесів.

Розробка та розгортання аналітичної платформи має важливе значення для збору відповідних даних і належного їх аналізу з метою розумної оптимізації виробничих процесів, для чого матеріальні потоки, потоки даних і конкретні операції представлені на рисунку 1.5. Система управління даними повинна бути запровадити для керування виробничими процесами, виробничими сценаріями, моделями споживання та виробничими параметрами. Збір даних дозволить точно визначити конкретні процеси, які споживають найбільше енергії та створюють найбільше відходів, щоб оптимізувати ці процеси шляхом впровадження нових підходів, що керуються даними, завдяки оцифровці. Через низку унікальних елементів, таких як тип обладнання, робоче середовище та графік виробництва, енергоспоживання обладнання та процесів може значно відрізнятися. Збір даних про енергоспоживання, контроль виробництва за допомогою ретельно підібраних датчиків Інтернету речей, вбудованих у виробниче обладнання, життєво важливі для оптимізації енергоспоживання виробничими лініями.

Компоненти інтелектуальної виробничої лінії можуть надавати різноманітні дані різних типів. Варто зазначити, що вони виробляються з істотно різною швидкістю та обсягом, тому вимагають різних процедур для збору, передачі, попередньої обробки та зберігання. Наприклад, щоб безпечно керувати даними з кіберфізичної системи пристроїв IoT з низьким ресурсом, необхідно ретельно спроектувати потокову великомасштабну багатосторонню платформу обміну даними [15]. Для забезпечення прийняття обґрунтованих рішень і управління процесами вирішальним є збір даних за допомогою правильно вибраних, встановлених і підключених датчиків і виконавчих механізмів IoT.

1.5 Висновки до першого розділу

Програмні та апаратні компоненти IIoT можуть мати вразливості та зазнавати атак зловмисників, тому для забезпечення стійкого розвитку вітчизняних підприємств Індустрії 5.0 необхідним є детальний аналіз цих вразливостей та розробка заходів захисту. Модель цифрового двійника може допомогти не лише цифровізації виробництва, але також в в аналізі вразливостей, розробці та реалізації засобів захисту.

2 ПРОБЛЕМИ БЕЗПЕКИ СИСТЕМ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

2.1 Основні проблеми безпеки вбудованих систем

Вбудовані системи стали невід'ємною частиною багатьох сучасних пристроїв та інфраструктури. Проте їх широке розповсюдження призвело до появи значних проблем безпеки [9].

Одна з основних викликів полягає у недостатній увазі до безпеки на етапах проектування та розробки. Часто більше уваги приділяють функціональності та вартості, ніж захисту. Це призводить до уразливостей на апаратному та програмному рівнях. Ще одна ключова проблема - відсутність своєчасного оновлення вбудованого ПЗ через складність процесу. Тому виявлені вразливості залишаються невиправленими протягом тривалого часу. Багато вбудованих пристроїв мають обмеження за потужністю обчислень, пам'яттю, енергоспоживанням. Це ускладнює використання складних механізмів безпеки як-от криптографії, аутентифікації, контролю доступу. Проте компроміси в безпеці збільшують ризики.

Розвиток Інтернету Речей призвів до збільшення кількості підключених вбудованих пристроїв. Зростає ймовірність атак через мережеві інтерфейси, особливо на дешеві IoT пристрої з простими протоколами. Багато уразливостей виникає через складність розробки для вбудованих систем. Програмісти можуть припускатись типових помилок у пам'яті, логіці, використанні інтерфейсів. Їх важко виявити на етапі тестування через обмежені можливості. Процеси ланцюжка постачання також є проблемним місцем. Компоненти постачаються різними вендорами, існують ризики наявності зловмисного коду. Крім того, розробкою ПЗ та його оновленням часто займаються різні компанії. Ще одна загроза - порушення фізичної безпеки і можливість несанкціонованого доступу. Зловмисники можуть

перепрограмувати вбудовану систему або викрасти дані. Отже, забезпечення безпеки вбудованих систем потребує заходів на всіх етапах життєвого циклу - від проектування до експлуатації. Потрібен комплексний підхід з урахуванням специфіки таких систем - обмеженості ресурсів, вимог надійності, можливостей оновлення та підтримки. Важливу роль відіграє створення архітектури безпеки, використання спеціалізованих протоколів і технологій захисту даних та програм.

2.2 Аспекти кібербезпеки промислового інтернету речей

Вимоги до забезпечення конфіденційності, цілісності та доступності даних залишаються ключовими (див. рис. 2.1) також і у випадку промислової системи, особливо враховуючи той факт, що для розумного виробництва інформація є цінним ресурсом, який забезпечує перевагу на ринку.

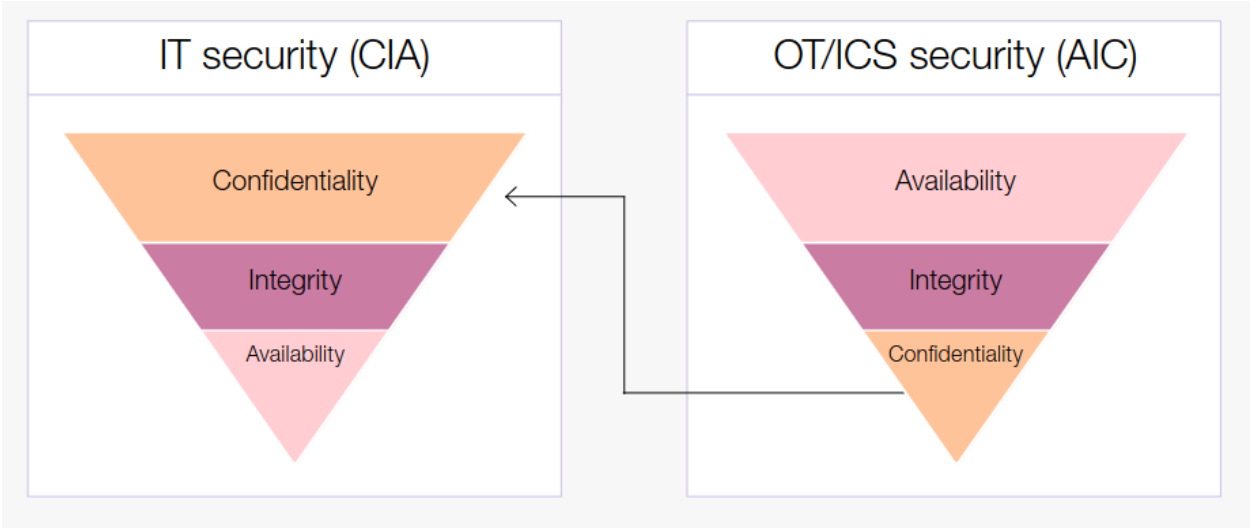

Рисунок 2.1 – Пріоритети IT-безпеки інвертуються в середовищі промислового інтернету речей [16].

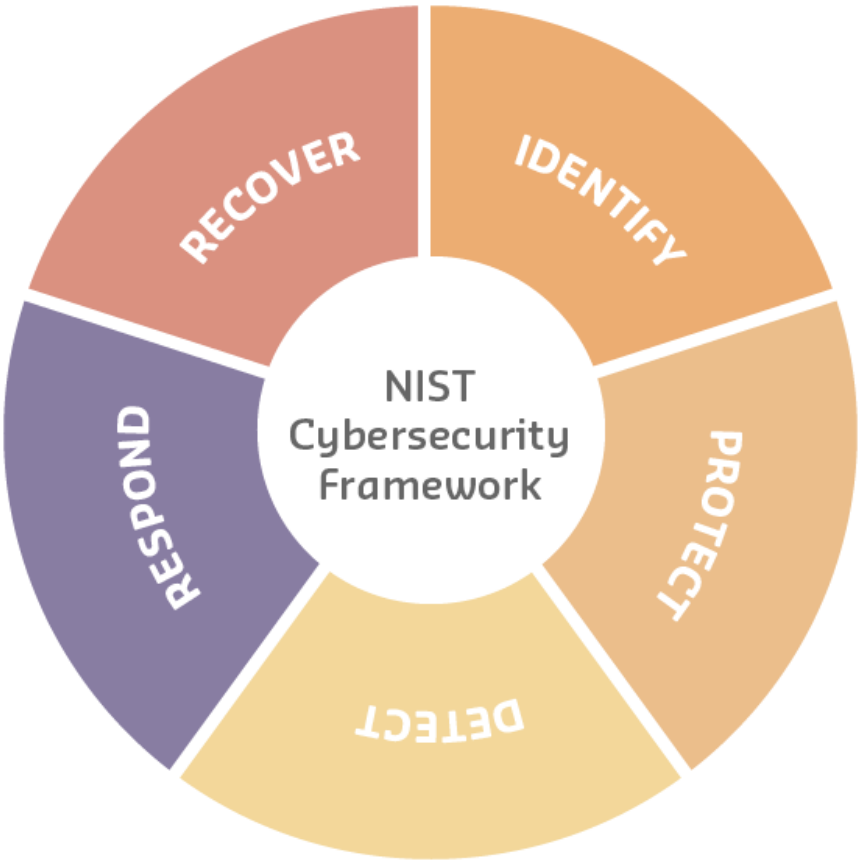

Рисунок 2.2 - Структура кібербезпеки, розроблена Національним інститутом стандартів і технологій .

Національний інститут стандартів і технологій США (NIST) розробив всеохоплюючу Структуру кібербезпеки для організацій (рисунок 2.2). Вона базується на підході управління ризиками. Структура визначає 5 основних функцій: ідентифікація, захист, виявлення, реагування, відновлення. Ідентифікація охоплює розуміння бізнес-контексту, управління активами, навколишнім середовищем та ризиками. Функція Захист включає розвиток безпечної інфраструктури, контроль доступу, навчання кадрів тощо. Виявлення передбачає моніторинг систем, дані про загрози, виявлення інцидентів. Реагування визначає плани і процедури реакції, аналіз інцидентів, управління змінами. Відновлення стосується планів безперервності бізнесу і відновлення систем після інцидентів чи аварій. Ці функції реалізуються через технічні, управлінські та операційні механізми. Структура NIST є ефективною основою для розбудови комплексних програм кібербезпеки, що

охоплюють людей, процеси і технології. Вона адаптується під потреби конкретних організацій для мінімізації ризиків кіберінцидентів.

2.3 Вразливості, характерні для цифрових двійників

Цифрові двійники швидко набувають популярності в різних галузях завдяки здатності моделювати складні фізичні об'єкти та процеси. Проте вони мають низку вразливостей, що можуть бути використані зловмисниками.

Одна з ключових проблем полягає у компрометації даних, що надходять від фізичних датчиків та систем. Зловмисники можуть спотворювати дані або впроваджувати шкідливий код на рівні пристроїв Інтернету Речей. Це призводить до похибок у моделях двійників.

Ще один вектор атак – вразливості хмарних та розподілених обчислень, де розгортаються цифрові двійники. Мова може йти про витік даних, порушення доступності сервісів, зараження шкідливим кодом. Окрема група ризиків пов’язана з недоліками технологій машинного навчання та штучного інтелекту, що часто застосовуються у двійниках. Вони можуть бути нестійкими до адверсаріальних прикладів та атак, спрямованих на маніпулювання даними і моделями. Багато двійників інтегруються з корпоративними системами для забезпечення бізнес-функцій. Це розширює поверхню кібератак як на OT, так і на IT інфраструктуру організацій.

На етапах проектування та розробки можуть виникати уразливості через помилки архітекторів та програмістів: незахищені інтерфейси, відсутність контролю доступу, складність в оновленні компонентів. Вразливості присутні і в процедурах збору та обробки даних. Наприклад, недостатня частота оновлення параметрів або затримки у передачі телеметрії з фізичних активів можуть знижувати адекватність цифрових двійників. Отже, комплексний підхід до кібербезпеки має важливе значення на всіх

рівнях побудови та функціонування технологій цифрових двійників - від датчиків і виконавчих пристроїв до хмарних платформ обробки даних. Системне врахування загроз і реалізація відповідних заходів захисту дозволять мінімізувати ризики для бізнесу.

2.4 Висновки до другого розділу

На етапах проектування та розробки можуть виникати уразливості через помилки архітекторів та програмістів: незахищені інтерфейси, відсутність контролю доступу, складність в оновленні компонентів. Вразливості потребують подальшого дослідження в рамках апробованих методологій.

3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

3.1 Моделі систем промислового інтернету речей

Рівень безпеки для промислового цифрового двійника середовищах має бути ретельно розроблений і належним чином розроблений. Захист IDT в цілому та кожного пристрою IoT зокрема потребує вирішення багатьох загроз інформаційній безпеці та кібербезпеці. Зібрані дані та оброблена інформація в платформі промислового цифрового двійника (IDT) є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

Оскільки цифровий двійник працює з конфіденційними даними та конфіденційними даними як частина кіберфізичних систем, за замовчуванням слід застосовувати найкращі методи безпеки, які відповідають галузевим стандартам і законам. Один із найважливіших етапів життєвого циклу розробки системи, безпека за проектом, означає, що вимоги безпеки повинні бути визначені для того, щоб інженери могли створити високоякісну, економічно життєздатну та безпечну систему.

Віртуалізація набуває все більшого поширення в архітектурах промислового інтернету речей завдяки своїй гнучкості та економічній ефективності. Замість використання фізичних серверів та мережевого обладнання для кожного додатку, віртуалізація дозволяє запускати віртуальні машини, контейнери та мережі на єдиній уніфікованій платформі. Це спрощує масштабування інфраструктури під зростаюче навантаження даних від IIoT пристроїв. Віртуальні середовища можна швидко розгортати чи згортати в хмарі. Також віртуалізація полегшує управління - оновлення, конфігурування, моніторинг можна здійснювати централізовано. З точки зору безпеки, віртуалізація дозволяє сегментувати трафік і дані, створювати

ізольовані середовища для критичних додатків. Це зменшує "поверхню атаки" окремих компонентів IIoT екосистем. Отже, технології віртуалізації значно спрощують побудову масштабованих, гнучких та захищених IoT інфраструктур для потреб промисловості. Вони дозволяють оптимізувати витрати і пришвидшити впровадження IIoT рішень.

Рисунок 3.1 – Приклади фізичної реалізації платформ Індустрії 5.0 в центрі MADE Міланської політехніки (фотографії надані лабораторією кіберфізичних систем ТНТУ).

Досліджувалися платформи промислового прототипування та розумного виробництва, надані центром MADE Міланської політехніки та лабораторією кіберфізичних систем ТНТУ (рисунки 3.1, 3.2).

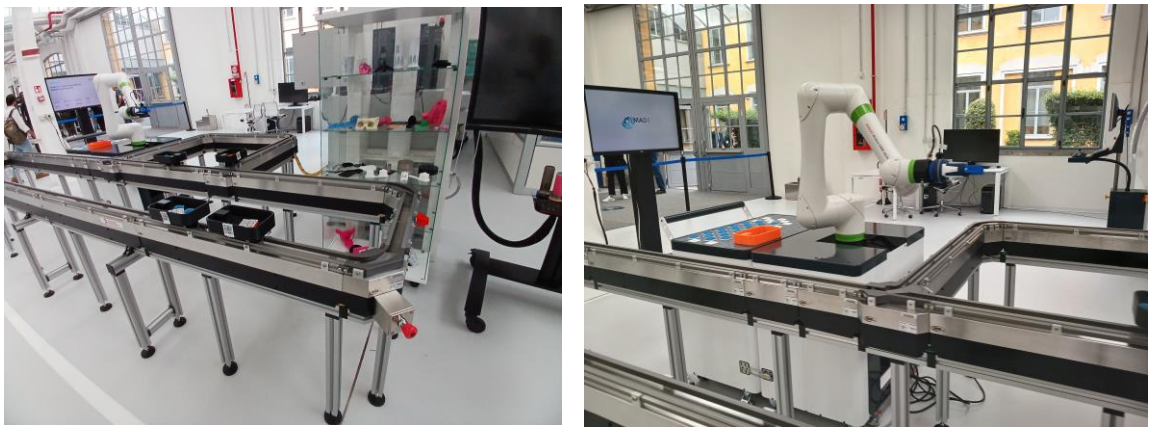

Рисунок 3.2 – Роботизована лінія розумного виробництва в центрі MADE Міланської політехніки (фотографії надані лабораторією кіберфізичних систем ТНТУ).

З точки зору кібербезпеки всі досліджені платформи базуються на процесах, відображених на рисунку 1.5. У сферах інформаційної безпеки та кібербезпеки моделювання загроз є методом визначення потреб безпеки. Це дозволяє ідентифікувати вимоги безпеки, знаходити загрози та вразливі місця, оцінювати їхній вплив і серйозність, таким чином роблячи можливим визначення пріоритетів життєздатних рішень і заходів. Ряд застосувань цього методу включає програмне забезпечення та мережі, компоненти IoT та промислові процеси. Методологія моделювання загроз STRIDE [20] була використана для ідентифікації та характеристики загроз і вразливостей, притаманних IDT і особистим даним користувачів. Було проаналізовано діаграму потоку даних і модель загроз (рисунок 3.3) для архітектури промислової платформи даних, зображеної на рисунку 1.5 для якої програми та технології розглядаються в статті [2]. Для цілей цього дослідження було визначено конкретну групу елементів (позначених червоним), які потрібно проаналізувати для вирішення розширених поверхонь атак, з якими можуть зіткнутися пристрої IDT та IoT . Було вивчено, чи існують загрози та ризики для платформи промислових даних і даних, що обробляються в системі.

3.2 Планування заходів з протидії вразливостей

Розглядаючи діаграму потоку даних архітектури DT, зображену на рисунку 3.3, було адаптовано десятку найкращих IoT OWASP і визначили групи методів безпеки та засобів контролю, покликаних зменшити загрози безпеці та ризики, з якими можуть зіткнутися пристрої IoT. 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. У той час як методологія STRIDE використовувалася як високорівневий підхід для виявлення загроз і визначення відповідних заходів протидії, OWASP IoT Top Ten може використовуватися з точки зору низького рівня для моделювання конкретних загроз безпеці та ризиків, а також для керівництва вибором тести, що використовуються для оцінки поверхонь атак IoT і пов’язаних із ними вразливостей [12].

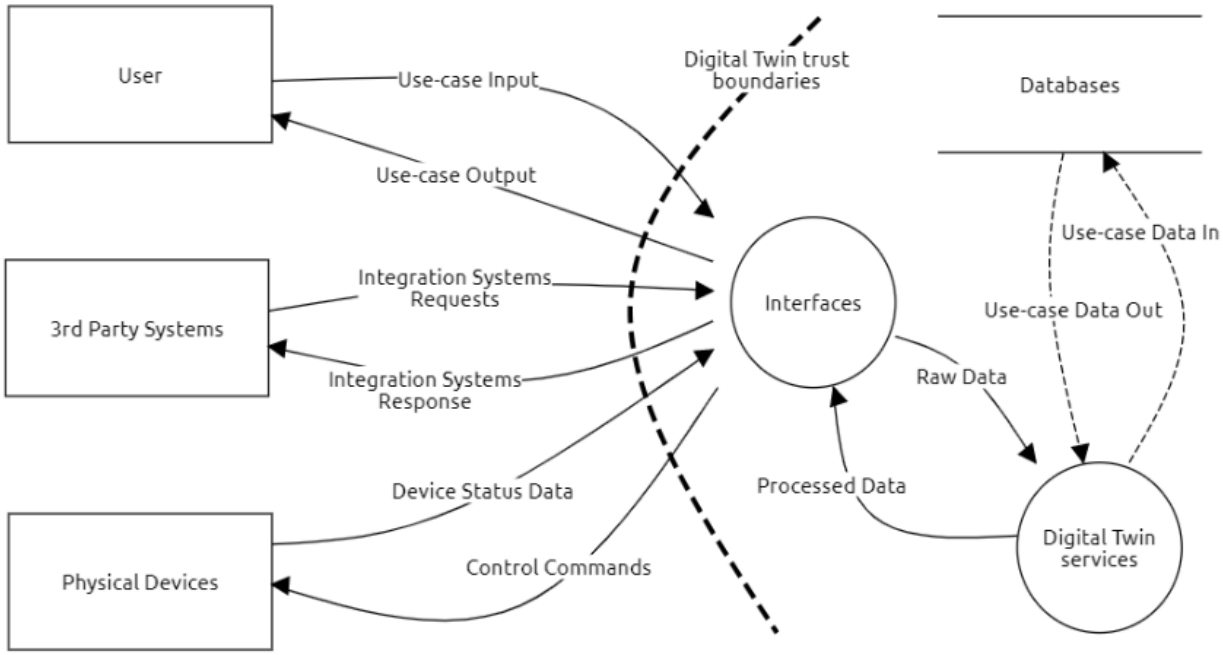

Рисунок 3.3 – Діаграма потоків даних архітектури DT [2], яка відповідає досліджуваним платформам промислового інтернету речей.

Першим ключовим заходом є забезпечення високого рівня безпеки всіх потоків даних, які надходять у модель цифрового двійника. Шифрування з'єднань від датчиків до хмарних або локальних систем допомагає захистити цілісність даних, що використовуються в межах двійника. Протоколи автентифікації також мають бути надійними, гарантуючи доступ лише авторизованим джерелам. Без гарантії даних аналізи чи оптимізація, отримані від двійника, можуть бути неточними або маніпуляційними.

Таблиця 3.1 – Вразливості та засоби протидії

Вразливість	**Можливі протидії**
Незахищені мережеві служби	Ізоляція мережі для пристроїв AR/VR Періодична оцінка вразливостей. Безпечні мережеві протоколи.
Незахищений інтерфейс екосистеми	Надійна автентифікація кінцевих точок IoT. Контроль доступу до чутливих API та інтерфейсів. Зашифровані канали зв'язку між пристроями / екосистемою IoT.

Використання застарілих компонентів	Оновлення та виправлення всього програмного забезпечення та компонентів, що використовуються в пристроях IoT.
Небезпечна передача та зберігання даних	Використання шифрування для захисту конфіденційних даних під час передачі та зберігання. Використання захищених протоколів.
Погане управління пристроєм	Інтеграція пристроїв IoT із системами управління ресурсами, відстеженням помилок і виправленнями. Контроль доступу.

Розробка планування на випадок непередбачених ситуацій за допомогою систем резервування або резервного копіювання забезпечує безперервність у разі проблем з мережею, обладнанням або програмним забезпеченням, які можуть порушити роботу цифрового двійника. Для подвійників критичної інфраструктури підтримання доступності та доступності має першочергове значення, якщо особам, які приймають рішення, необхідно використовувати аналітичні можливості двійника під час реагування на реальні ситуації. Часте резервне копіювання даних і віддзеркалені хмарні екземпляри можуть зменшити ризик простою.

Протоколи налаштування та повторного калібрування для цифрових двійників зберігають точність, оскільки їхні фізичні аналоги з часом розвиваються через ремонт, модернізацію, погіршення тощо. Якщо зміни у фізичній системі не відображаються в її цифровому двійнику через налаштовані параметри та логіку, близнюк може втратити моделювання та прогностична ефективність. Автоматизоване або ручне тестування якості визначає, коли двійники відрізняються від реальних вхідних даних.

Надійний контроль доступу та процедури керування змінами, які керують цифровими двійниками, обмежують ризики як внутрішніх, так і зовнішніх загроз. Детальне призначення ролей, багатофакторна автентифікація, можливість аудиту та суворий аналіз модифікацій допомагають командам інформаційної безпеки керувати цифровими

двійниками в масштабі для різних користувачів і точок дотику інтеграції з іншими системами.

3.3 Висновки до 3 розділу

Завчасно враховуючи безпеку за допомогою суворих заходів безпеки, доступності, точності та управління, організації можуть впевнено розгортати можливості цифрового двійника, не підвищуючи ризику. Підтримка цих операційних дисциплін дозволяє цифровим двійникам безпечно підвищувати надійність і продуктивність у більш віддалені горизонти. Запропоновані контрзаходи допоможуть розробникам програмного забезпечення та експертам із безпеки в процесах проектування та вдосконалення промислових платформ даних.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Перехід до концепції Індустрії 5.0, що передбачає широку автоматизацію та роботизацію виробництв, ставить нові виклики в сфері охорони праці [17]. Адже поряд з людьми будуть задіяні інтелектуальні системи, роботи, обладнання з технологіями штучного інтелекту. Питання безпеки персоналу постає особливо гостро через можливу взаємодію людини та машини в одному виробничому середовищі. Саме усунення небезпек цієї колаборації і є ключовим завданням у контексті охорони праці для Індустрії 5.0. Насамперед, унеможливлення травм вимагає уважного аналізу ризиків на етапах проектування та розробки технологій. Безпека має бути інтегрована в роботизовані та автономні системи з самого початку за принципом Security by Design. Не менш важливо забезпечувати надійне функціонування систем контролю та моніторингу стану обладнання, а також механізми аварійного вимкнення на випадок виходу з ладу.

Додаткові ризики виникають через мережеву взаємодію виробничих компонентів у кіберфізичних системах. Тому вимагається wholistичний підхід до кібербезпеки як IT, так і OT інфраструктури підприємств. Важливу роль відіграватимуть технологічні рішення щодо безпечної співпраці людини і робота: сенсорні системи моніторингу робочих зон, засоби контролю та обмеження руху, зворотний зв'язок. З іншого боку, роботи з AI будуть здатні автономно приймати рішення щодо попередження нещасних випадків, наприклад, шляхом комунікації з працівниками чи аварійної зупинки процесів. Впровадження принципів «антропоцентричної робототехніки» на основі біомеханіки та ергономіки допоможе зробити автоматизовані системи безпечними та зручними для людей.

Потребуватиме розвитку і нормативно-правова база у сфері охорони праці. Концепція Індустрії 5.0 наразі недостатньо відображена в діючих стандартах та вимогах. Необхідно враховувати специфіку нових технологій та процедур їх безпечного застосування на виробництвах. Таким чином, інтеграція принципів безпеки людини в архітектуру кіберфізичних систем, систем машинного навчання і штучного інтелекту має стати обов'язковою умовою при переході до моделі Індустрії 5.0. Комплексний підхід, що охоплює технології, процеси, нормативну базу - запорука уникнення ризиків для здоров'я та життя персоналу в high-tech 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.

Отже, впровадження інноваційних технологій вимагає перегляду всієї системи охорони праці на виробництві з позицій кібербезпеки, безпеки машин та автономних систем, готовності персоналу. Це сприятиме мінімізації ризиків травматизму персоналу розумних фабрик. Цифрові двійники відкривають нові можливості для вдосконалення системи охорони праці на виробництві. Вони дозволяють моделювати робочі процеси, аналізувати потенційні загрози і прогнозувати виробничі ризики на основі даних датчиків та інших пристроїв Інтернету Речей. За допомогою технологій доповненої/віртуальної реальності на базі цифрових двійників можна створити реалістичне тривимірне зображення робочих зон, відтворити діяльність персоналу, обладнання, інструментів. Це дає змогу дослідити ергономічні аспекти задля попередження виробничого травматизму. Застосування ШІ для аналізу даних дає змогу розпізнавати потенційно небезпечні ситуації, ідентифікувати фактори ризику (підвищена температура, тиск тощо). На основі цього формуються тривожні сповіщення для персоналу або керуючих сигналів на устаткування чи виконавчі механізми.

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".

Ефективним є використання цифрових двійників робітників для відстеження їх стану, навантажень, стомлюваності, стресів задля попередження перевтоми та помилок. Цифровізація процесів охорони праці значно підвищує прозорість і дає цілісну картину щодо безпеки робочих

місць. У разі нещасних випадків забезпечується швидке реагування, розслідування причин подій. Отже, впровадження цифрових двійників відкриває широкі перспективи для проактивного управління системою безпеки та гігієни праці на основі аналізу реальних даних, симуляцій, моделей штучного інтелекту.

4.2 Підвищення стійкості роботи платформ промислового інернету речей у воєнний час

Військові дії та кібератаки створюють значні загрози для безперервного функціонування автоматизованих систем управління виробництвом в промисловості [18,19]. Тому питання підвищення стійкості платформ промислового інтернету речей набуває особливого значення у воєнний час. Першочерговим заходом є розгортання комплексних систем інформаційної безпеки на всіх рівнях: від виробничого устаткування до корпоративної мережі і дата-центрів. Моніторинг кіберзагроз, шифрування трафіку, резервне копіювання, антивірусний захист мають стати обов’язковими складовими архітектури IoT.

Не менш важливою є фізична безпека обладнання і каналів зв’язку на випадок руйнувань чи пошкоджень інфраструктури внаслідок бойових дій. Для цього використовують розподілені mesh-мережі з надлишковістю вузлів, міцні захищені сервери, резервне живлення.

Платформи IIoT - це комплексні рішення, які забезпечують збір, передачу, зберігання, обробку, аналіз, візуалізацію та використання даних з різних джерел, а також інтеграцію, координацію, автоматизацію та оптимізацію промислових процесів.

Всі цифрові платформи, в тому числі платформи промислового інтернету речей мають велике значення для розвитку економіки, суспільства, науки, освіти, культури, безпеки та інших сфер життя. Однак, цифрові

4.3 Висновки до 4 розділу

Платформи також є вразливими до різних загроз, особливо у воєнний час, коли вони можуть бути атаковані, пошкоджені, заблоковані, викрадені, змінені, видалені або використані проти інтересів держави, організацій або осіб [https://kpmg.com/ua/uk/blogs/home/posts/2022/4/pytannya-kiberbezpeky-v-umovakh-voyennoho-chasu.html]

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:

- 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.
- 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.
- 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.

• 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.

Для підвищення стійкості роботи платформ IIoT необхідно використовувати різні методи та заходи, такі як:

• 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.

• 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.

• 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: 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.

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 4 розділу

У результаті аналізу вимог щодо охорони праці користувачів інтерфейсів людино-машинної взаємодії встановлено, що для забезпечення добробуту персоналу підприємств Індустрії 5.0, які 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.

Стосовно безпеки життєдіяльності на підприємствах Індустрії 5.0, то впровадження результатів цієї роботи сприятиме її покращенню, за умови, що належна увага приділятиметься важливим аспектам впровадження, а саме профілактиці та реагуванню на надзвичайні ситуації, як природнього походження, так і техногенного характеру.

ВИСНОВКИ

Програмні та апаратні компоненти IIoT можуть мати вразливості та зазнавати атак зловмисників, тому для забезпечення стійкого розвитку вітчизняних підприємств Індустрії 5.0 необхідним є детальний аналіз цих вразливостей та розробка заходів захисту. Модель цифрового двійника може допомогти не лише цифровізації виробництва, але також в в аналізі вразливостей, розробці та реалізації засобів захисту.

На етапах проектування та розробки можуть виникати уразливості через помилки архітекторів та програмістів: незахищені інтерфейси, відсутність контролю доступу, складність в оновленні компонентів. Вразливості потребують подальшого дослідження в рамках апробованих методологій.

Завчасно враховуючи безпеку за допомогою суворих заходів безпеки, доступності, точності та управління, організації можуть впевнено розгортати можливості цифрового двійника, не підвищуючи ризику. Підтримка цих операційних дисциплін дозволяє цифровим двійникам безпечно підвищувати надійність і продуктивність у більш віддалені горизонти.

Запропоновані контрзаходи допоможуть розробникам програмного забезпечення та експертам із безпеки в процесах проектування та вдосконалення промислових платформ даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. C. Baudoin, E. Bournival, E. Clauer. Global Industry Standards for Industrial IoT An Industrial Internet Consortium White Paper. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf
2. Skorenkyy, Y., Zolotyy, R., Fedak, S., Kramar, O., Kozak, R. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. *CEUR Workshop Proceedings*, 2023, 3468, pp. 12–23.
3. M. Dautaj, M. Rossi, Towards a New Society: Solving the Dilemma Between Society 5.0 and Industry 5.0. In: Canciglieri Junior, O., Noël, F., Rivest, L., Bouras, A. (eds) Product Lifecycle Management. Green and Blue Technologies to Support Smart and Sustainable Organizations. PLM 2021. IFIP Advances in Information and Communication Technology, 639 (2022). Springer, Cham. Doi:10.1007/978-3-030-94335-6_37.
4. N. Zagorodna, I. Kramar. 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.
5. Індустрія 5.0: напрями дій та шляхи розвитку. [Електронний ресурс]. URL: https://www.clusters.org.ua/blog-single/industry-5-0-napriamy-diy/
6. Про Індустрію 5.0 – чому це стає актуальним для України. [Електронний ресурс]. URL: https://www.industry4ukraine.net/publications/pro-industriyu-5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/
7. Індустрія 5.0: бачення трансформацій від Європейської комісії. [Електронний ресурс]. URL: https://www.clusters.org.ua/blog-single/industry-5-0/

8. Miraz, Mahadi & Hasan, Mohammad Tariq & Sumi, Farhana & Sarkar, Shumi & Hossain, Mohammad. (2022). Industry 5.0: The Integration of Modern Technologies. 10.1201/9781003122401-14.
9. Clim, Antonio. Cyber security beyond the Industry 4.0 era. A short review on a few technological promises. 2019. DOI:10.13140/RG.2.2.25394.56002.
10. Internet of Things (IoT) Architecture [Електронний ресурс]. URL: https://dgtlinfra.com/internet-of-things-iot-architecture/
11. Digital twins [Електронний ресурс]. URL: https://www.ibm.com/topics/what-is-a-digital-twin
12. 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. DOI: 10.1109/ISGTEurope.2017.8260283.
13. V. Vijayakumar, F. Sgarbossa, W.P. Neumann, A. Sobhani, Framework for incorporating human factors into production and logistics systems. International Journal of Production Research, 60 (2022) 402-419.
14. F. Sgarbossa, E.H. Grosse, W.P. Neumann, D. Battini, C.H. Glock, Human factors in production and logistics systems of the future. Annual Reviews in Control, 49 (2020) 295-305.
15. Y. Drohobytskiy, V. Brevus, Y. Skorenkyy, Spark structured streaming: Customizing kafka stream processing. 2020 IEEE Third International Conference on Data Stream Mining Processing (2020) 296-299.
16. Industry 4.0 and OT security. A methodology for assessing and securing the operational technology (OT) environment [Електронний ресурс]. URL: https://www.cgi.com/belgium/en/brochure/cybersecurity/industry-40-and-ot-security
17. Я.І. Бедрій Безпека життєдіяльності: Навч.посібн. – К.: Вид-во Кондор, 2009.

18. 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/.
19. 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/.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.056
М.Р. Карпець – ст. гр. СБмз-61, Ю.Л. Скоренький к.ф.-м.н., доц.
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПЛАТФОРМ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

M. Karpets, Dr. Yu. Skorenkyy

STUDY OF VULNERABILITIES OF THE INDUSTRIAL INTERNET OF THINGS PLATFORMS

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

Широке впровадження цифрових платформ може призвести до нових спільних бізнес-моделей, які сприятимуть сталому розвитку [1, 2]. Питання безпеки застосування пристроїв інтернету речей має надзвичайну актуальність, оскільки дані є одним з найбільш важливих виробничих ресурсів Індустрії 5.0.

Інтелектуальне виробництво може надавати різноманітні дані, включаючи фізичні дані про матеріали та візуальні дані, дані керування процесом і дані про машину тощо. Щоб безпечно керувати даними з кіберфізичної системи пристроїв IoT з обмеженими ресурсами, потокова великомасштабна платформа обміну даними має бути належним чином розроблена. Інформаційна безпека та захист конфіденційності стають критичними вимогами та заслуговують на особливу увагу в контексті Індустрії 5.0.

Для інтелектуальних виробничих процесів і агрегатів в системах Індустрії 5.0 використовують цифрові двійники, які моделюють реальні виробничі лінії та процеси, дозволяють обробляти дані на місці або транслювати дані в хмарні сервіси для підтримки прийняття рішень на основі математичних моделей, що характеризують споживання ресурсів і якість і кількість результатів процесу. Рівень безпеки для промислового цифрового двійника в хмарних/граничних середовищах має бути ретельно спроектований і належним чином розроблений. Захист IDT в цілому та кожного пристрою IoT зокрема вимагає вирішення багатьох загроз інформаційній безпеці та кібербезпеці. Зібрані дані та оброблена інформація в IDT є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

В даній роботі представлено аналіз вразливостей промислових цифрових платформ, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Література

1. Skorenky Yu. et al. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. *CEUR Workshop Proceedings*, 2023, 3468, pp. 12–23.

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