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 інтерфейсів людино-машинної взаємодії для Індустрії 5.0

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

_____ Горішний М.О.
(підпис) (прізвище та ініціали)

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

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

Завідувач кафедри _____ Загородна Н.В.
(підпис) (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 Горішному Михайлу Орестовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження вразливостей інтерфейсів людино-машинної взаємодії для Індустрії 5.0.

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 Інтерфейсів людино-машинної взаємодії для Індустрії 5.0

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Область застосування та основні принципи роботи інтерфейсів взаємодії в Індустрії 5.0, 1.1 Принципи індустрії 5.0, 1.2 Обмін даними в системах Індустрії 5.0, 1.3 Типи людино-машинних інтерфейсів, їх особливості та застосування, 1.4 Особливості функціонування засобів віртуальної та доповненої реальності, 1.5 Висновк до першого розділу, 2 Проблеми безпеки інтерфейсів людино-машинної взаємодії, 2.1 Основні вразливості інтерфейсів людино-машинної взаємодії, 2.2 Розгортання VR-інтерфейсів та атаки на них, 2.3 Висновки до другого розділу, 3 Практичне дослідження вразливостей інтерфейсів, 3.1 Реалізація досліджуваного VR-інтерфейсу, 3.2 Реалізація досліджуваного AR-інтерфейсу, 3.3 Планування та проведення заходів з протидії вразливостей, 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 використанихджерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів) 1 Титульна сторінка. 2 Тема. Мета. Завдання дослідження. 3. Область застосування та основи роботи інтерфейсів в Індустрії 5.0. 4. Типи людино-машинних інтерфейсів, їх особливості та застосування. 5. Особливості функціонування віртуальної та доповненої реальності. 6. Основні вразливості інтерфейсів людино-машинної взаємодії. 7. Розгортання VR-інтерфейсів та атаки на них. 8. Розгортання AR-інтерфейсів та атаки на них. 9. Реалізація досліджуваного VR-інтерфейсу. 10. Реалізація досліджуваного AR-інтерфейсу. 11. Планування заходів з протидії вразливостям. 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 інтерфейси Індустрії 5.0	20.11.2023-23.11.2023	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	про інтерфейси Індустрії 5.0	24.11.2023-26.11.2023	*Виконано*
4.	Виконання дослідження щодо аналізу вразливостей інтерфейсів людино-машинної взаємодії для		
	Індустрії 5.0	27.11.2023-27.11.2023	*Виконано*
5.	Оформлення розділу «Область застосування та прин-		
	ципи роботи інтерфейсів взаємодії в Індустрії 5.0»	28.11.2023-30.11.2023	*Виконано*
6.	Оформлення розділу «Проблеми безпеки інтерфейсів		
	людино-машинної взаємодії»	01.12.2023-04.12.2023	*Виконано*
7.	Оформлення розділу «Практичне дослідження		
	вразливостей інтерфейсів»	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	29.12.2023	

Студент _____ Горішний М.О.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Дослідження вразливостей інтерфейсів людино-машинної взаємодії для Індустрії 5.0. // Кваліфікаційна робота освітнього рівня «Магістр» // Горішний Михайло Орестович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2023 // С. 60, рис. – 14, табл. – 3, додат. – 1, бібліогр. – 31.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ЛЮДИНО-МАШИННА ВЗАЄМОДІЯ, РОЗШИРЕНА РЕАЛЬНІСТЬ, ВРАЗЛИВОСТІ.

Кваліфікаційна робота присвячена аналізу ризиків при використанні інтерфейсів людино-машинної взаємодії, які використовуються або потенційно можуть використовуватися для потреб Індустрії 5.0.

У першому розділі зроблено аналіз особливостей роботи інтерфейсів людино-машинної взаємодії в Індустрії 5.0. Розглянуто типи людино-машинних інтерфейсів та їх застосування а також функціонування засобів віртуальної та доповненої реальності.

В другому розділі розглядаються проблеми безпеки інтерфейсів людино-машинної взаємодії, особливості розгортання VR- та AR-інтерфейсів та атаки на них.

У третьому розділі проведено дослідження вразливостей інтерфейсів людино-машинної взаємодії для Індустрії 5.0 та розроблено рекомендації щодо протидії вразливостям.

Четвертий розділ присвячено проблемам охорони праці при використанні VR- та AR-інтерфейсів людино-машинної взаємодії та їх безпека в надзвичайних ситуаціях.

ANNOTATION

Research on Vulnerabilities in Human-Machine Interface for Industry 5.0// Qualification work of the educational level “Master” // Mykhailo Horishnyy // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, СБмз-61 group // Ternopil, 2023 // P. 60, fig. - 14, tables - 3, annexes -1, references - 31.

Key words: information security, human-machine interaction, extended reality, vulnerabilities

The qualification work analyses risks related to use of interfaces of human-machine interaction, which are used or can potentially be used in the Industry 5.0.

The first section analyzes the features of the functioning of human-machine interaction interfaces in Industry 5.0. The types of human-machine interfaces and their application, as well as the functioning of virtual and augmented reality tools, are considered.

The second chapter deals with security issues of human-machine interaction interfaces, features of deployment of VR and AR interfaces and attacks on them.

In the third chapter, a study of the vulnerabilities of human-machine interaction interfaces for Industry 5.0 was carried out and recommendations for countering vulnerabilities were developed.

In the fourth chapter, the problems of labor protection when using VR- and AR-interfaces of human-machine interaction and their safety in emergency situations are considered.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AR – Augmented Reality (доповнена реальність).

CAD – Computer-Aided Design (автоматизоване проектування).

CAE – Computer-Aided Engineering (автоматизована розробка).

CAM – Computer-Aided Manufacturing (автоматизоване виробництво).

DT – Digital Twin (цифровий двійник)

IoT – Internet of Things (інтернет речей).

IT – Information Technology (інформаційні технології).

HMD – head-mounted display (окуляри або шолом віртуальної реальності).

VR – Virtual Reality (віртуальна реальність).

XR – eXtended Reality (розширена реальність).

ПЗ – програмне забезпечення.

ЛМІ – людино-машинний інтерфейс.

НС – надзвичайна ситуація.

ШІ – штучний інтелект.

ЗМІСТ

ВСТУП

Актуальність теми. Цифровізація та перехід до принципів і практик Індустрії 5.0 є ключовими факторами забезпечення сталого розвитку шляхом підвищення енергоефективності та кліматичної нейтральності промислових процесів, використання творчих здібностей людини та можливостей інформаційних систем на основі ШІ. Цифрові двійники (DT), яким сьогодні приділяється велика увага в контексті цифровізації промислових систем [1-7], є віртуальними копіями реальних об’єктів або систем, які можна створювати та керувати ними за допомогою віртуальної (VR) і доповненої реальності (AR). Вказані технології дозволяють створювати реалістичні 3D-моделі, які можуть взаємодіяти з реальним світом і надавати багату функціональність, та мають багато переваг для застосування в Індустрії 5.0. Для ефективної взаємодії з цифровою промисловою платформою необхідно використовувати інтерфейс, водночас зручний для людини-оператора і сумісний з цифровим двійником. У Індустрії 5.0 такі інтерфейси можна використовувати для моделювання, контролю та вдосконалення виробничих процесів, забезпечення прогнозованого обслуговування обладнання та покращення співпраці між працівниками. Разом з тим, промислове застосування інформаційно-комунікаційних платформ вимагає аналізу вразливостей безпеки та розробки засобів захисту, які гарантуватимуть забезпечення конфіденційності, незмінності та доступності даних, а також запобігання несанкціонованому доступу та маніпуляціям. Таким чином, запобігання несанкціонованому доступу до важливих промислових та особистих даних через вразливості інтерфейсів людино-машинної взаємодії стають суттєвими вимогами та заслуговують на детальний аналіз в контексті Індустрії 5.0.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є дослідження ризиків при використанні

інтерфейсів людино-машинної взаємодії, які використовуються або потенційно можуть використовуватися для потреб Індустрії 5.0.

Для досягнення поставленої мети було потрібно виконати такі завдання:

- проаналізувати завдання та предметну область;
- з’ясувати характерні особливості інтерфейсів людино-машинної взаємодії та виявити їх вразливості;
- проаналізувати способи запобігання загрозам, специфічним для інтерфейсів, які можуть застосовуватися в Індустрії 5.0;
- дослідити роботу та спланувати захисту для типових VR- та AR-інтерфейсів;
- розробити висновки стосовно можливих шляхів забезпечення конфіденційності, незмінності та доступності даних, які передаються через VR- та AR-інтерфейси.

Об’єкт дослідження. Процеси захисту інформації у новітних інтерфейсах людино-машинної взаємодії.

Предмет дослідження. Вразливості інтерфейсів людино-машинної взаємодії.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що проведено аналіз вразливостей інтерфейсів людино-машинної взаємодії в Індустрії 5.0.

Практичне значення одержаних результатів. Розроблено рекомендації щодо захисту інтерфейсів людино-машинної взаємодії в Індустрії 5.0.

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 додатка. Загальний обсяг кваліфікаційної роботи складає 60 сторінок, з них 50 сторінок основного тексту, який містить 14 рисунків та 3 таблиці.

1 ОБЛАСТЬ ЗАСТОСУВАННЯ ТА ОСНОВИ РОБОТИ ІНТЕРФЕЙСІВ ВЗАЄМОДІЇ В ІНДУСТРІЇ 5.0

Важливим аспектом Інтернету речей є можливість розробки гібридних рішень, які здатні поєднувати фізичні продукти з цифровими послугами, зокрема через мобільні пристрої [1-7]. Сучасні смартфони не лише діють як посередники між людьми, фізичними та цифровими об’єктами, а й дозволяють накопичувати цінну інформацію про когнітивні, емоційні та поведінкові моделі користувача, яку зрештою можна використовувати для розробки альтернативних пристроїв IoT, зокрема з використанням розширеної реальності. Складовими континууму Мілгрема змішаної реальності [8] та основними технологіями для полегшення інтеграції людини в таку систему є доповнена реальність (AR), та віртуальна реальність (VR) яка є цифровою моделлю, що повністю заміняє для користувача реальне оьочення. Ці засоби можуть надати людині-оператору інтерфейс для взаємодії з цифровим світом розумного виробництва, в тому числі через концепцію цифрових двійників [9].

1.1 Принципи Індустрії 5.0

Індустрія 5.0 – це нова парадигма промислового розвитку, яка базується на інтеграції людини та технологій, зеленому переході та стійкості ланцюгів доданої вартості. Ця концепція виникла як відповідь на виклики, які ставить сучасний світ перед виробниками, споживачами та суспільством в цілому [10, 11]. Індустрія 5.0 має на меті створити більш гармонійну, рівну та ефективну систему виробництва та споживання, яка б враховувала потреби людей, планети та процвітання.

На рисунку 1.1 відображені характерні риси кожної з промислових революцій та виділено людино-машинну взаємодію як особливість п’ятої

промислової революції, яка має привести до переходу до розумного виробництва (Індустрії 5.0).

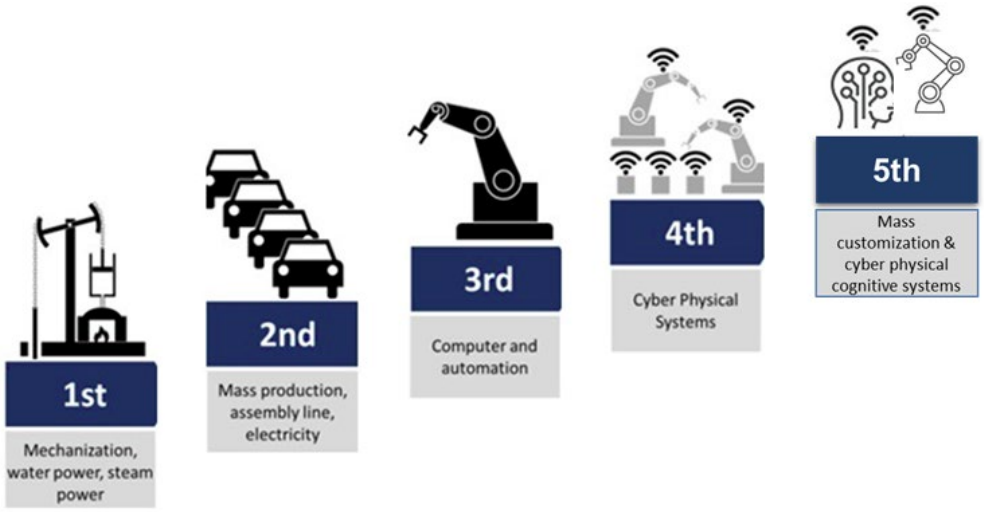


Рисунок 1.1 – Етапи розвитку та характерні особливості індустрії [12]

Основні принципи Індустрії 5.0 можна сформулювати так:

- Гуманоцентризм. Людина є головним актором та цінністю в Індустрії 5.0. Технології служать для підтримки, покращення та розширення людських можливостей, а не для їх заміни чи обмеження. Людина має право на гідну працю, освіту, здоров'я, безпеку та участь у прийнятті рішень. Людина також має відповідальність за свої дії, їх наслідки та дотримання етичних норм.
- Екологічність. Індустрія 5.0 зменшує негативний вплив на середовище, дозволяє зберігати природні ресурси, сприяє переходу на відновлювальні джерела енергії та циркулярну економіку. Це означає, що виробництво та споживання мають бути регенеративними та відновлювальними, а не екстрактивними та відходогенеруючими. Це також означає, що виробництво та споживання мають бути адаптивними та гнучкими, а не жорсткими та кризогенними.
- Соціальність. Індустрія 5.0 сприяє соціальній справедливості, рівності, інклюзії та різноманітності. Це означає, що виробництво та споживання мають бути орієнтовані на задоволення реальних потреб людей,

а не на створення штучного попиту та споживацької культури. Це також означає, що виробництво та споживання мають бути демократичними та учасними, а не авторитарними та маніпулятивними.

- Інноваційність. Індустрія 5.0 стимулює інноваційну діяльність, яка спрямована на вирішення глобальних та локальних проблем, а не на отримання короткострокового прибутку. Це означає, що виробництво та споживання мають бути креативними та експериментальними, а не рутинними та консервативними. Це також означає, що виробництво та споживання мають бути відкритими та співпрацюючими, а не закритими та конкуруючими.

Індустрія 5.0 - це не просто наступний етап промислової революції, а нова філософія та цивілізація, яка вимагає глибоких змін у свідомості, культурі та цінностях людства. Це виклик, але також можливість для України, яка має великий потенціал для розвитку Індустрії 5.0, якщо буде діяти активно та відповідально [13-15].

1.2 Обмін даними в системах Індустрії 5.0

Концепція Індустрії 5.0 вимагає ефективного та безпечного обміну даними між різними елементами системи виробництва та споживання, які можуть бути розподіленими, гетерогенними та динамічними. Обмін даними в системах Індустрії 5.0 має враховувати аспекти, висвітлені у попередньому пункті.

Оскільки Індустрія 5.0 це нова парадигма промислового розвитку, яка базується на інтеграції людини та технологій, зеленому переході та стійкості ланцюгів доданої вартості то вона вимагає ефективного та безпечного обміну даними між різними елементами системи виробництва та споживання, які можуть бути розподіленими, гетерогенними та динамічними. Обмін даними в системах Індустрії 5.0 має враховувати такі аспекти:

- Обмін даними має служити для підтримки, покращення та розширення людських можливостей, а не для їх заміни чи обмеження. Людина має право на контроль, захист та використання своїх даних, а також на участь у прийнятті рішень, які стосуються їх обробки та аналізу. Людина також має відповідальність за свої дії, їх наслідки та дотримання етичних норм.
- Обмін даними має сприяти мінімізації негативного впливу на навколишнє середовище, збереженню природних ресурсів, переходу на відновлювальні джерела енергії та циркулярної економіки. Це означає, що дані мають бути збирані, передавані, зберігані, оброблені та використовувані ефективно, економно та екологічно, а також відновлювані, перероблені та видаляні безпечно.
- Обмін даними має сприяти соціальній справедливості, рівності, інклюзії та різноманітності. Це означає, що дані мають бути доступними, прозорими, якісними, достовірними та сумісними для всіх зацікавлених сторін, а також враховувати потреби, інтереси, права та цінності різних груп та осіб.
- Обмін даними має стимулювати інноваційну діяльність, яка спрямована на вирішення глобальних та локальних проблем, а не на отримання короткострокового прибутку. Це означає, що дані мають бути використовувані для генерації нових знань, ідей, продуктів, послуг та рішень, які відповідають суспільним потребам та викликам.

Обмін даними - це один з ключових аспектів Індустрії 5.0, оскільки він забезпечує зв'язок, інтеграцію, оптимізацію та інновацію різних процесів, систем, пристроїв, сервісів та людей, які беруть участь у виробництві, споживанні та утилізації продуктів. Безпека даних – це комплекс заходів, які забезпечують захист даних від несанкціонованого доступу, втручання, модифікації, видалення або використання. Обмін даними в системах Індустрії 5.0 має такі особливості:

- Великий обсяг та різноманітність даних. Системи Індустрії 5.0 збирають, передають, зберігають, обробляють, аналізують та використовують великі обсяги даних з різних джерел, таких як сенсори, машини, обладнання, системи, хмарні сервіси, мобільні пристрої, соціальні мережі, інтернет речей, блокчейн, штучний інтелект, віртуальна та доповнена реальність тощо. Дані можуть бути структурованими, напівструктурованими або неструктурованими, статичними або динамічними, детермінованими або стохастичними, якісними або кількісними, однорідними або гетерогенними тощо.
- Висока швидкість та затримка даних. Системи Індустрії 5.0 потребують швидкої та надійної передачі даних між різними компонентами, оскільки вони виконують складні та критичні завдання, які вимагають високої точності, якості, продуктивності та безпеки. Затримка даних - це час, який потрібен для передачі даних від джерела до призначення, який залежить від відстані, пропускної здатності, навантаження, протоколів, шифрування, фільтрації, буферизації тощо. Затримка даних може впливати на якість та ефективність взаємодії людей та машин, а також на можливість виявлення, реагування та адаптації до змін у середовищі.
- Висока стійкість та безпека даних. Системи Індустрії 5.0 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.

Деякі розумного виробництва можна суттєво оптимізувати за рахунок використання сучасних цифрових систем та засобів людино-машинної взаємодії (таблиця 1.1) [16]. В умовах Індустрії 4.0 перелічені в таблиці завдання або виконуються без залучення персоналу, що робить неможливим отримання доданої вартості за рахунок особистого досвіду та креативності, або виконуються людьми в умовах, які знижують ефективність та безпечність виробництва.

Таблиця 1.1 – Галузі використання ЛМІ в Індустрії 5.0

	Доступ до даних і взаємодія з середовищем	**Діагностика проблеми**	**Діяльність**
Посилення людських можливостей	Монтаж, використання та обслуговування обладнання, Навчання персоналу	Віддалена підтримка, вимоги щодо виконання	Навігація за допомогою віртуального дисплея в автономних транспортних засобах і дронах
Управління простором	Функціональна оптимізація дизайну виробничих цехів, моніторинг запасів і транспортування, реагування на збої	Моніторинг простору, інспекція будівель і об'єктів	Просторова оптимізація для організації відвантаження, комплектування замовлень
Керування пристроями	Виробничий, будівельний та інфраструктурний дизайн	Моніторинг операцій, оптимізація виробничої лінії, контроль якості, моніторинг та діагностика обладнання	Інструкції оператора обладнання щодо послідовності виконання завдань, інструкції з технічного обслуговування

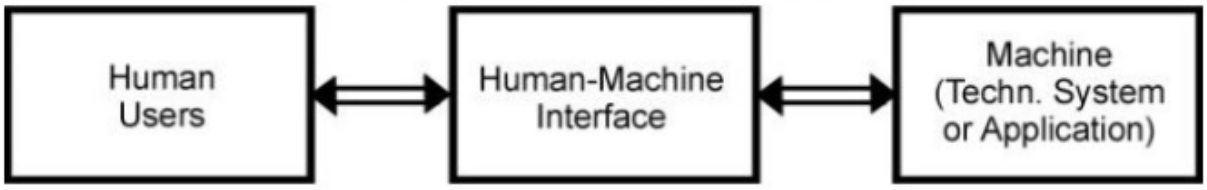
Прикладом застосування новітніх інтерфейсів які принциповим чином залежать від обміну великими обсягами даних є віртуальне прототипування – одна з сучасних цифрових технологій, вбудованих у «цифрове виробництво» – у промислові, виробничі і логістичні процесах. Віртуальне прототипування стосується створення та моделювання різних цифрових об’єктів перед їх фізичним створенням або впровадженням, експериментуючи у віртуальному середовищі з різними гіпотезами дизайну. Така технологія не є абсолютно новою, але вона являє собою безперервну еволюцію потреби в моделюванні об’єктів, яка почалася з появою програмного забезпечення автоматизованого проектування в 70-х роках, розвинулася в програмному забезпеченні для 3D-

моделювання в 90-х роках і зараз триває.

Віртуальне прототипування включає впровадження засобів автоматизованого проектування (CAD), автоматизованої розробки (CAE) і автоматизованого виробництва (CAM) для створення реалістичної та інтерактивної віртуальної моделі. Таким чином, віртуальне прототипування відноситься до інструментів розробки та моделювання, які постійно розвиваються.

1.3 Типи людино-машинних інтерфейсів, їх особливості та застосування

Людино-машинна взаємодія описується як взаємодія та спілкування між людьми-користувачами та машиною (динамічною технічною системою), через людино-машинний інтерфейс . Аспект реального часу розрізняє сфери систем людини-машини та взаємодії людини-комп'ютера, які в іншому випадку тісно пов'язані [17]. Основними категоріями людських завдань у



взаємодії людина-машина є контроль і вирішення проблем.

Рисунок 1.2 – Взаємодія між людиною та інформаційною компонентою індустріальної платформи [17]

Людино-машинна взаємодія є цілеспрямованою. Загальними цілями систем «людина-машина» в контексті Індустрії 5.0 є, головним чином, цілі продуктивності, цілі безпеки, цілі гуманізації та цілі екологічної сумісності. Цілі продуктивності включають економічні цілі, а також цілі якості продукту

та виробництва. Важливість цілей безпеки сильно залежить від сфери застосування. Цей клас цілей домінує над усіма іншими в багатьох великомасштабних системах. Цілі гуманізації включають інтереси команди та організацію роботи, задоволеність роботою, ергономічну сумісність та когнітивну сумісність.

Взаємодія «людина-машина» та дослідження систем «людина-машина» вимагають міждисциплінарних або міждисциплінарних поглядів і підходів. Наступні три області сприяють взаємодії людини та машини та дослідженню систем: когнітивна наука та ергономіка (як науки про людину), автоматизація та системна інженерія (як системні науки) та інформаційна та комунікаційна інженерія (як інформатика). Крім того, важливими є організаційні та культурні аспекти.

Обмін інформацією між комп'ютерною системою та людиною відбувається за допомогою певних технічних засобів відповідно до певного набору правил, які і визначають інтерфейс [18]. Отже людино-машинний інтерфейс (ЛМІ) – це засіб взаємодії між людиною та машиною, який дозволяє обмінюватися інформацією, командами та сигналами. ЛМІ може мати різні форми, залежно від типу машини, цілей взаємодії, характеристик користувача та контексту застосування. За способом подання інформації ЛМІ можна поділити на такі типи:

- Візуальні ЛМІ. Це ЛМІ, які використовують зорові елементи, такі як текст, графіка, анімація, відео, світлодіоди, індикатори тощо. Візуальні ЛМІ дозволяють передавати велику кількість інформації, а також візуалізувати стан, процеси та результати машини. Візуальні ЛМІ вимагають наявності дисплея, проектора або іншого пристрою відображення. Приклади візуальних ЛМІ: монітор комп'ютера, пульт дистанційного керування, електронна книга, автомобільна панель приладів тощо.
- Аудіальні ЛМІ. Це ЛМІ, які використовують звукові елементи, такі як мова, музика, звукові ефекти, тональні сигнали тощо. Аудіальні ЛМІ

дозволяють передавати інформацію, яка не потребує візуальної уваги, а також створювати емоційний настрій, підсилювати зворотний зв'язок та попереджати про небезпеку. Аудіальні ЛМІ вимагають наявності гучномовця, навушників або іншого пристрою відтворення звуку. Приклади аудіальних ЛМІ: телефон, радіо, музичний плеєр, голосовий асистент, сирена тощо.

- Тактильні ЛМІ. Це ЛМІ, які використовують тактильні елементи, такі як дотик, тиск, вібрація, температура, біль тощо. Тактильні ЛМІ дозволяють передавати інформацію, яка не потребує зорової або аудіальної уваги, а також стимулювати, релаксувати або заспокоювати користувача. Тактильні ЛМІ вимагають наявності сенсорів, актуаторів або іншого пристрою створення тактильних відчуттів. Приклади тактильних ЛМІ: клавіатура, миша, джойстик, смартфон тощо.
- Ольфакторні ЛМІ. Це ЛМІ, які використовують ольфакторні елементи, такі як запахи, аромати, феромони тощо. Ольфакторні ЛМІ дозволяють передавати інформацію, яка пов'язана з пам'яттю, емоціями та іншими аспектами людської психології. Ольфакторні ЛМІ вимагають наявності генераторів, дозаторів або іншого пристрою випускання запахів. Приклади ольфакторних ЛМІ: парфум, аромалампа, віртуальна реальність, біометрична ідентифікація тощо.

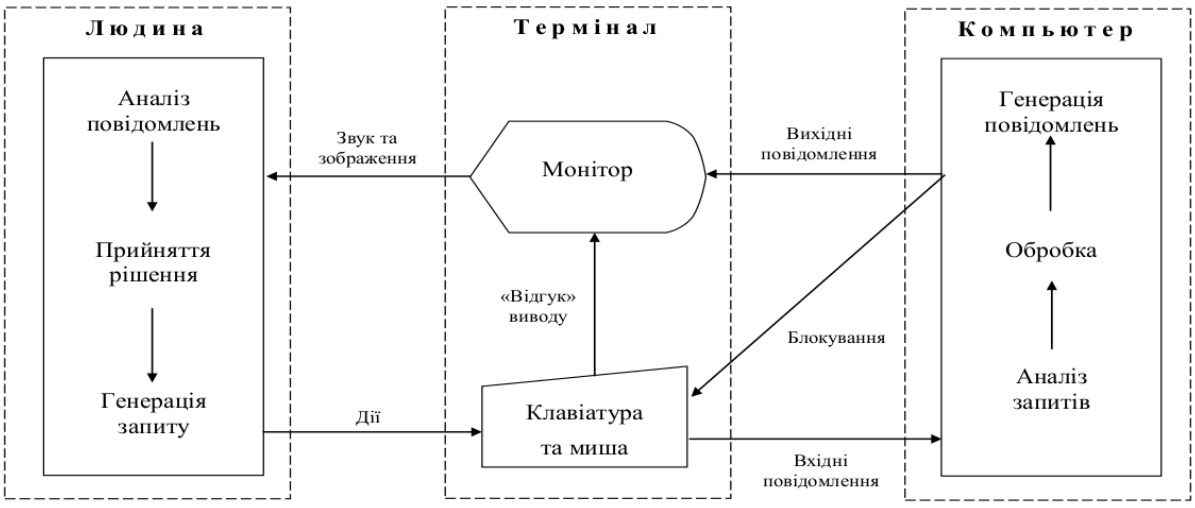


Рисунок 1.3 – Архітектура ЛМІ [18]

Кожен тип ЛМІ має свої особливості, переваги та недоліки, а також застосування в різних сферах діяльності. Вибір типу ЛМІ залежить від багатьох факторів, таких як ціль взаємодії, характеристики машини, вимоги користувача, умови середовища тощо. Оптимальний ЛМІ має бути простим, зручним, інтуїтивним, ефективним, безпечним та задовільняючим для користувача. Процес проектування користувацького інтерфейс характеризується суттєвою невизначеністю, оскільки немає алгоритму отримання конкретного результату за конкретними вихідними даними. При такому проектуванні, крім інформаційних та бузпекових аспектів, необхідно враховувати також психофізичні характеристики користувача, які визначають процеси сприйняття та опрацювання інформації, що є областю когнітивної психології.

Рисунок 1.4 – Модель взаємодії комп'ютерної системи та користувача [18]

Зокрема, для людини, незважаючи на індивідуальні особливості, яскравий колір є сильним подразником, а звук переважно є фоном чи

каналом надходження додаткової інформації. Це робить надзвичайно ефективними сучасні AR-інтерфейси.

1.4 Особливості функціонування засобів віртуальної та доповненої реальності

Розширена реальність заснована на принципі можливості перегляду цифрового вмісту, такого як 3D-моделі, зображення, тексти, відео тощо, контекстуалізовані до реального середовища. З практичної точки зору необхідно виконати три основні вимоги:

- візуальне накладання;
- просторова і часова узгодженість;
- взаємодія між реальними та цифровими об'єктами.

Пристрої, які відповідають цим трьом вимогам, можуть бути різних типів і часто містять усі технічні характеристики, які дозволяють людині самостійно керувати програмою доповненої реальності. Вони варіюються від пристроїв з низьким рівнем залучення, таких як, наприклад, планшети чи смартфони, до пристроїв з вищим рівнем залучення, таких як, наприклад, шоломи чи окуляри. У виробничому секторі доповнена реальність зазвичай асоціюється зі швидким і прямим доступом до даних, якими керують компанії, щоб забезпечити операторів необхідною інформацією. Це особливо важливо під час роботи зі складання, перевірки та обслуговування виробничого процесу. Застосування доповненої реальності призводить, серед іншого, до зменшення непорозумінь і помилок з боку оператора, а також до можливого скорочення витрат на допомогу для обслуговування.

Континуум розширеної реальності, який запропонували Мілгрем і Кішіно [8], показаний на рисунку 1.5. Граничними точками осі є, з одного боку, реальне середовище, що складається виключно з реальних об’єктів, а з

іншого – суто віртуальне середовища, що складається виключно з віртуальних об’єктів [Milgram and Kishino, 1994].

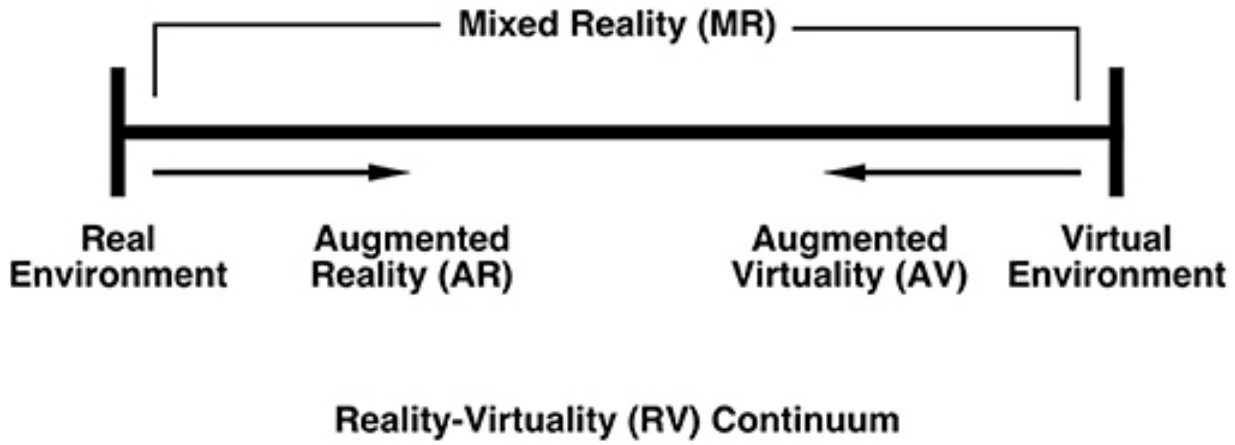


Рисунок 1.5 – Континуум Мілгрема [8]

Будь-яке середовище, яке частково складається із реальних і частково з віртуальних об’єктів, називають змішаною реальністю (MR). Середовища змішаної реальності, де реальний світ доповнено віртуальним вмістом, називаються доповненою реальністю (AR), тоді як ті, де більша частина вмісту є віртуальною, але є певне усвідомлення або включення об’єктів реального світу, називаються доповненою віртуальністю (AV). З точки зору практичного застосування, на сьогодні найбільш застосовними в людино-машинних інтерфейсах є віртуальна реальність та доповнена реальність.

1.5 Висновки до першого розділу

Обмін даними в системах Індустрії 5.0 – це не просто технічний процес, а складна соціотехнічна система, яка впливає на всі сфери людської діяльності. Це виклик, але також можливість для України, яка має великий потенціал для розвитку Індустрії 5.0, якщо буде діяти активно, відповідально та спільно. Взаємодія людини і машини з промисловими установками та іншими динамічними технічними системами в даний час визнана важливою для безпеки, якості та ефективності процесу. Ця задача охоплює всі аспекти

взаємодії та спілкування між людьми-користувачами та їхніми машинами через людино-машинні інтерфейси.

Програмні компоненти інтерфейсів можуть мати вразливості та зазнавати атак зловмисників, тому для забезпечення стійкого розвитку вітчизняних підприємств індустрії 5.0 необхідним є детальний аналіз вразливостей та розробка заходів захисту новітніх інтерфейсів людино-машинної взаємодії.

2 ПРОБЛЕМИ БЕЗПЕКИ ІНТЕРФЕЙСІВ ЛЮДИНО-МАШИННОЇ ВЗАЄМОДІЇ

2.1 Основні вразливості інтерфейсів людино-машинної взаємодії

Стабільна та безпечна робота інтерфейсів людино-машинної взаємодії має велике значення для ефективності, комфорту, безпеки та задоволення користувачів, які виконують функції контролю та управління виробничими процесами. Однак, вказані інтерфейси також мають ряд специфічнихвразливостей, які можуть призвести до помилок, несправностей, конфліктів, шахрайства, злому, кібератак, порушення приватності та інших негативних наслідків. Основні вразливості інтерфейсів людино-машинної взаємодії можна поділити на такі групи [18]:

- Вразливості, пов'язані з людським фактором. Це вразливості, які виникають через обмеженість, недосвідченість, невідповідальність, недбалість, знеособлення, стрес, емоції, упередженість, маніпуляцію, залежність або інші характеристики та стани людини, яка взаємодіє з машиною. Приклади таких вразливостей: неправильне введення даних, невміння користуватися інтерфейсом, недотримання інструкцій, втрата уваги, забуття, паніка, агресія, піддавання соціальному тиску, викрадення ідентифікаційних даних, зловживання привілеями тощо.;
- Вразливості, пов'язані з технічним фактором. Це вразливості, які виникають через недосконалість, складність, несумісність, нестабільність, вразливість, застарілість, відсутність захисту, контролю, аудиту або інші характеристики та стани машини, з якою взаємодіє людина. Приклади таких вразливостей: помилки програмування, дефекти обладнання, перевантаження системи, несумісність форматів, протоколів, стандартів, втрата даних, збій мережі, відмова апаратури, вразливість до вірусів, троянів, шпигунських програм, злому, кібератак тощо;

- Вразливості, пов'язані з контекстуальним фактором. Це вразливості, які виникають через невідповідність, непередбачуваність, небезпечність, конфліктність, незаконність, неетичність або інші характеристики та стани середовища, в якому відбувається взаємодія людини та машини.

2.2 Розгортання VR-інтерфейсів та атаки на них

VR-інтерфейси дзволяють користувачам занурюватися в імітаційні світи, створені комп'ютером, та взаємодіяти з ними за допомогою спеціальних пристроїв, таких як шоломи, рукавиці, контролери тощо. Однак, разом з розвитком VR-інтерфейсів зростає й ризик атак на них з боку зловмисників, які можуть мати різні мотиви та цілі.

Атаки на VR-інтерфейси можна класифікувати за такими критеріями:

- За типом атаки. Атаки можуть бути активними або пасивними. Активні атаки полягають у втручанні в роботу VR-інтерфейсу, зміні, видаленні або додаванні даних, викликанні збоїв, перехопленні контролю, внесенні шкідливого коду тощо. Пасивні атаки полягають у незаконному спостереженні, зборі, аналізі або копіюванні даних, що передаються або обробляються VR-інтерфейсом, без впливу на його функціонування.
- За типом даних. Атаки можуть бути спрямовані на різні типи даних, які використовуються VR-інтерфейсами, такі як відео, аудіо, текст, графіка, 3D-моделі, біометричні, локаційні, особисті та інші дані. Залежно від типу даних, атаки можуть мати різні наслідки, такі як порушення приватності, крадіжка інтелектуальної власності, шантаж, підробка, психологічний вплив тощо.
- За типом зловмисника. Атаки можуть бути здійснені різними суб'єктами, які мають різні ресурси, знання, навички, можливості та інтереси. Зловмисники можуть бути окремими особами, групами, організаціями,

корпораціями, державами або їхніми агентами. Залежно від типу зловмисника, атаки можуть мати різні масштаби, складність, тривалість, цілі та наслідки.

Використання окулярів віртуальної реальності (HMD) різко зменшує власні можливості користувачів помічати ознаки зловмисних маніпуляцій, такі як стан мережі, використання процесора, підключені фізичні пристрої або веб-переадресації [19].

Щоб зрозуміти природу кіберзагроз VR, важливо розглядати їх у порівнянні з двома фундаментальними концепціями занурення та присутності. VR-середовище розроблено для занурення шляхом представлення людському мозку штучно згенерованих стимулів, які є загальною сумою сенсорного зворотного зв'язку на основі апаратних і програмних компонентів VR, ізолюючи користувача від реального світу. Присутність – це суб'єктивний досвід перебування там або психологічна реакція користувача на світ віртуальної реальності, яка, у свою чергу, залежить від занурення та залучення. Завдяки присутності користувач усвідомлює, що він перебуває у світі віртуальної реальності, але реагує на віртуальні сутності так, як у реальному світі, дозволяючи просторову та соціальну взаємодію, подібну до поведінки людини в реальному світі.

Ці два аспекти можуть бути цілями або фасилітаторами кібератак. Були продемонстровані приклади таких атак [20] з використанням API OpenVR, щоб дезорієнтувати користувачів, увімкнути камеру HMD без їхнього відома, накласти небажані 2D-зображення в полі зору та змінити фактори навколишнього середовища VR, які змушували користувачів бити фізичні об'єкти та стіни. Вони придумали перевірку концепції атаки на «людський джойстик», коли користувача обманом змушували перейти до цільового фізичного місця без його відома. Занурення та придушення HMD візуальних підказок із реального світу робить людину вразливою до такої атаки так само, як було показано, що підробка GPS-атаки дозволяє дистанційно

керувати дроном або кораблем, ніби це джойстик. Користувач віртуальної реальності покладається на цілісність штучно створених стимулів майже таким же чином. За тією ж схемою обману, Рафік і Сен-Чінг [21] розробили пристрій, який використовує інфрачервоний світлодіод для блокування та маніпулювання системою відстеження HMD, а також атаку, яка маніпулює оцінкою пози, генеруючи фальшивий синхронізуючий імпульс.

З точки зору системи, атаки у VR можуть стосуватися графічного процесора, датчиків і дисплеїв, які разом визначають вихідну, вхідну та обчислювальну ефективність системи VR, тобто її глибину інформації [22]. У цьому документі ми особливо зосереджуємося на графічному процесорі, оскільки він безпосередньо визначає частоту кадрів і через неї взаємодію з користувачем. Як доказ концепції ми також націлюємося на частоту кадрів за допомогою мережевої атаки на відмову в обслуговуванні, особливо тому, що для спільного VR-середовища потрібне мережеве з’єднання, і зазвичай збої в мережі впливають на частоту кадрів. Обидві атаки спрямовані на зловмисне спричинення візуального дискомфорту через порушення рухів користувача, аудіо та зображення, оскільки порушення частоти кадрів є відомим основним фактором, що призводить до морської хвороби спричиненої VR [23].

Ключовою проблемою конфіденційності віртуальної реальності є дуже особистий характер зібраних даних, наприклад біометричних даних, таких як сканування райдужної оболонки або сітківки ока, відбитки пальців і рук, геометрія обличчя та відбитки голосу. Приклади:

- Відстеження пальців: у віртуальному світі користувач може використовувати жести руками так само, як і в реальному світі – наприклад, використовуючи пальці для введення коду на віртуальній клавіатурі. Однак це означає, що система записує та передає дані відстеження пальців, які показують, як пальці вводять PIN-код. Якщо зловмисник зможе отримати ці дані, він зможе відтворити PIN-код користувача.

- Відстеження очей: деякі гарнітури VR і AR також можуть включати відстеження очей. Ці дані можуть надати додаткову цінність зловмисникам. Якщо точно знати, на що дивиться користувач, зловмисник може отримати цінну інформацію, яку він може отримати, щоб відтворити дії користувача.

Майже неможливо анонімізувати дані відстеження VR, оскільки люди мають унікальні моделі руху. Використовуючи поведінкову та біологічну інформацію, зібрану в гарнітурах віртуальної реальності, дослідники з дуже високою точністю ідентифікували користувачів, що становить реальну проблему, якщо системи віртуальної реальності будуть зламані.

Зловмисники також можуть вводити в платформи VR функції, призначені для того, щоб змусити користувачів надати особисту інформацію. Це створює простір для атак програм-вимагачів, коли зловмисники саботують платформи перед тим, як попросити викуп. Технології машинного навчання дозволяють маніпулювати голосами та відео так, щоб вони виглядали як справжні кадри. Якщо хакер може отримати доступ до даних відстеження руху з VR-гарнітури, він потенційно може використати їх для створення цифрової копії (іноді відомої як deepfakes) і, отже, підірвати безпеку VR. Потім вони могли накласти це на чужий досвід VR, щоб здійснити атаку соціальної інженерії.

Окрім кібербезпеки, одна з найбільших небезпек віртуальної реальності полягає в тому, що вона повністю блокує зоровий і слуховий зв’язок користувача із зовнішнім світом. Завжди важливо спочатку оцінити фізичну безпеку та безпеку середовища користувача. Це також стосується доповненої реальності, де користувачі повинні добре пам’ятати про своє оточення, особливо в середовищах із більшим ефектом занурення.

2.3 Розгортання AR -інтерфейсів та атаки на них

Основною властивістю AR-технології, яку можна використовувати для інтелектуального виробництва, є система відстеження, яка дозволяє точно розміщувати цифрові моделі об’єктів у фізичному світі. Найпростішою для реалізації є технологія AR-трекінгу, заснована на фізичних маркерах, які локалізуються в певних місцях промислових ліній або установок і використовуються для визначення правильного положення цифрового зображення. Однак погіршення якості маркерів з часом або складні умови освітлення можуть значно перешкодити розпізнаванню маркерів. Тому часто використовуються природні маркери або безмаркерні системи, які не потребують додаткових фізичних об’єктів, накладених на реальний світ для визначення положення віртуальних об’єктів. Сфери, які дійсно можуть отримати найбільшу вигоду від використання AR-технології: допомога в складанні операцій на інтелектуальному виробництві, навчання інженерних спеціалістів, створення системи навігації для операторів. логістика складських операцій, обслуговування виробничих вузлів, контроль якості продукції та ін. У разі появи нетипових сценаріїв роботи обладнання або збоїв окремих вузлів усунення таких несправностей стає досить складним і трудомістким процесом, оскільки вимагає доступу до конкретної інформації, а їх фільтрація та відбір займає досить багато часу. Рівень доповненої реальності, який надає добре структуровану інформацію в реальному часі в конкретному місці, має значний потенціал для візуалізації та контекстуалізації даних, що дозволяє оптимізувати процес прийняття рішень оператором технічного обслуговування за допомогою дистанційних сервісів. Використовуючи AR, персонал може безпечно відпрацьовувати різні сценарії в контрольованому інтерактивному режимі. Збої обладнання можна моделювати в імерсивному середовищі, щоб дозволити охопити не лише технічні, а й психологічні аспекти. Методології розробки, такі як

проектування, орієнтоване на людину, можуть забезпечити вдосконалення навичок і знань персоналу на робочому місці з безпечним і ефективним навчанням AR.

Браузери AR спрощують процес розширення, але контент створюється та доставляється сторонніми постачальниками та програмами. Це піднімає питання про ненадійність, оскільки AR є відносно новою сферою, а механізми створення та передачі автентифікованого контенту все ще розвиваються. Досвідчені хакери можуть замінити AR користувача своїм власним, вводячи людей в оману або надаючи неправдиву інформацію.

Різноманітні кіберзагрози можуть зробити вміст ненадійним, навіть якщо джерело справжнє. До них належать спуфінг, сніффінг і маніпулювання даними. Враховуючи потенційну ненадійність контенту, системи доповненої реальності можуть бути ефективним інструментом для обману користувачів у рамках атак соціальної інженерії. Наприклад, хакери можуть спотворити сприйняття користувачами реальності за допомогою підроблених знаків або дисплеїв, щоб спонукати їх виконувати дії, які приносять користь хакерам.

Хакери AR можуть вставляти шкідливий вміст у програми за допомогою реклами. Нічого не підозрюючи користувачі можуть натискати оголошення, які ведуть на веб-сайти-заручники або заражені зловмисним програмним забезпеченням сервери доповненої реальності, які містять ненадійні візуальні ефекти, що підриває безпеку доповненої реальності.

Ще одна потенційна атака на безпеку AR – це відмова в обслуговуванні. Наприклад, користувачі, які покладаються на AR для роботи, раптово виявляються відрізаними від потоку інформації, яку вони отримують. Це особливо хвилює професіоналів, які використовують технологію для виконання завдань у критичних ситуаціях, коли відсутність доступу до інформації може мати серйозні наслідки. Одним із прикладів може бути раптова втрата хірургом доступу до важливої інформації в режимі реального часу на своїх окулярах доповненої реальності або водій, який

раптово втрачає з поля зору дорогу, оскільки його лобове скло доповненої реальності перетворюється на чорний екран. Мережеві зловмисники можуть підслуховувати зв’язок між браузером AR і постачальником AR, власниками каналів AR і сторонніми серверами. Це може призвести до атак типу "людина посередині".

Однією з найбільш значних вразливостей безпеки AR-пристроїв, що носяться, є фізичне пошкодження. Деякі пристрої для носіння довговічніші, ніж інші, але всі пристрої мають фізичну вразливість. Підтримуйте їх функціональність і безпеку – наприклад, не дозволяйте комусь піти з гарнітурою, яку можна легко втратити або вкрасти – є важливим аспектом безпеки.

2.4 Висновки до другого розділу

На сьогодні інтерфейси VR-та AR-типу вже достатньо широко впроваджені в різних галузях і атаки на ці інтерфейси вже не є рідкістю. Однак, немає єдиного підходу до моделювання загроз, характерних для промислових систем, які зараз лише впроваджуються. Вразливості інтерфейсів людино-машинної взаємодії потребують подальшого дослідження в рамках апробованих методологій.

3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ІНТЕРФЕЙСІВ

3.1 Реалізація досліджуваного VR-інтерфейсу

Більшість імерсивних комунікаційних систем можна подати як сукупність трьох компонент: модуль захоплення, модуль-клієнт і модуль-сервер. Щоб дослідити вразливості модульних програм для захоплення, розглянемо типову схему, яка інтегрує програму для захоплення (для 3D-фотореалістичних представлень об'єктів), комерційну програму VR та комунікаційну платформу Connec2. Додаток захоплення може складатися з таких модулів: ZED Frame Grabber (з роздільною здатністю 512 × 512 пікселів), ZED Hole Filling, Mediapipe ML FGBG, GrayAVG та віртуальна камера OBS з одним датчиком RGB і Oculus Quest 2. На рисунку 3.1 показано приклад візуалізації віддаленого користувача в комунікаційній програмі Connec2 VR.

Основною особливістю архітектури сучасних XR-систем є конвеєр захоплення та рендерингу, який є повністю модульним, щоб окремі блоки процесу легко було задіювати та розширювати. Це включає просте розширення для використання різних пристроїв захоплення та відкритий API для доступу до остаточного захоплення в будь-якій програмі. Усе це з основною метою — дозволити фотореалістичне 3D-представлення користувачів у випадках використання зв'язку в режимі реального часу.

Повна послідовність етапів створення VR-контенту, показана на рисунку 3.1, включає такі компоненти:

- Модульне захоплення;
- Клієнт Ingest, який отримує зображення RGBD від драйвера віртуальної веб-камери OBS і завантажує їх у систему Connec2;
- Connec2 використовує стиснення motion JPG, що надсилається через структуровані мережеві черги повідомлень;

- Клієнт візуалізації працює на пристрої Oculus Quest, надсилає/отримує аудіо та рендерить аудіо, а також 3D-хмару точок (через VFX-граф).

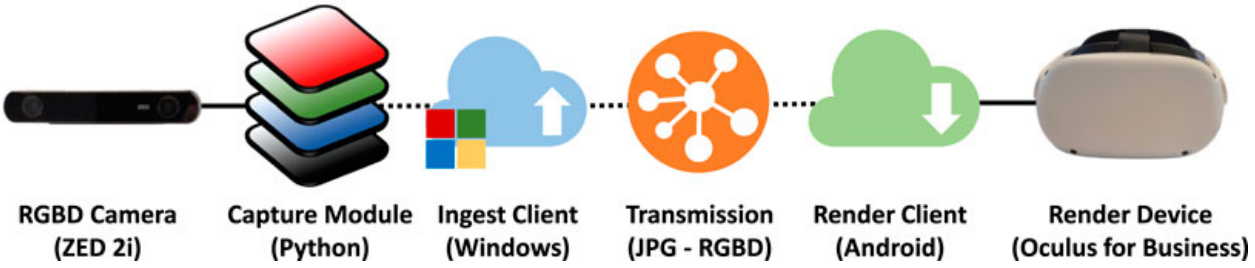


Рисунок 3.1 – Послідовність етапів створення VR-контенту [24]

В якості VR-інтерфейсу людино-машинної взаємодії було використано обладнання лабораторії кіберфізичних систем ТНТУ (рисунок 3.2) та обладнання, надане центром MADE Міланської політехніки в рамках міднародного проєкту “Smart Manufacturing Innovation, Learning-labs, and Entrepreneurship” (рисунок 3.3).

Рисунок 3.2 – Окуляри віртуальної реальності для відображення VR-контенту

Рисунок 3.3 – Використання окулярів віртуальної реальності

Досліджувалися інтерфейси промислового прототипування та розумного виробзицтва, надані центром MADE Міланської політехніки (рисунок 3.4) та лабораторією кіберфізичних систем ТНТУ (рисунок 3.5).

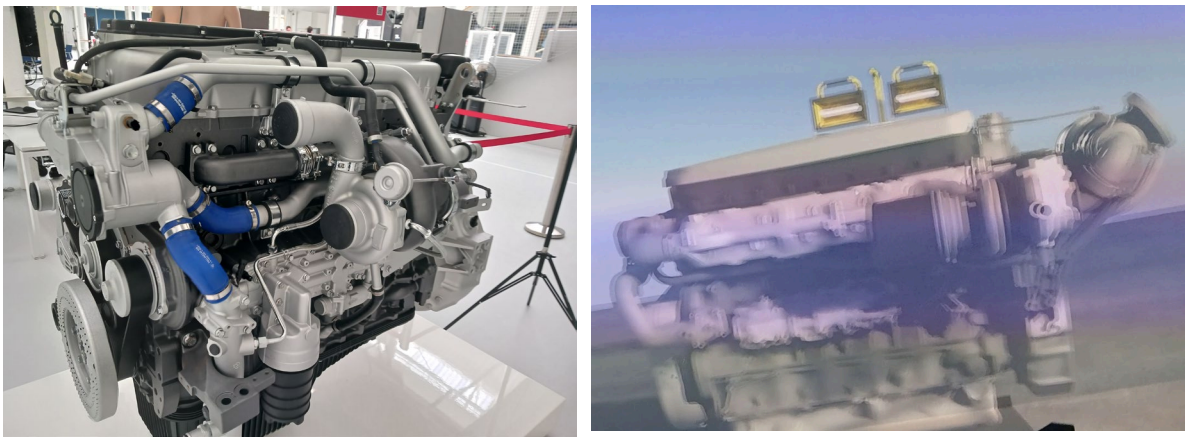


Рисунок 3.4 – Фізичний об’єкт (дизельний двигун) та його відображення у віртуальному просторі

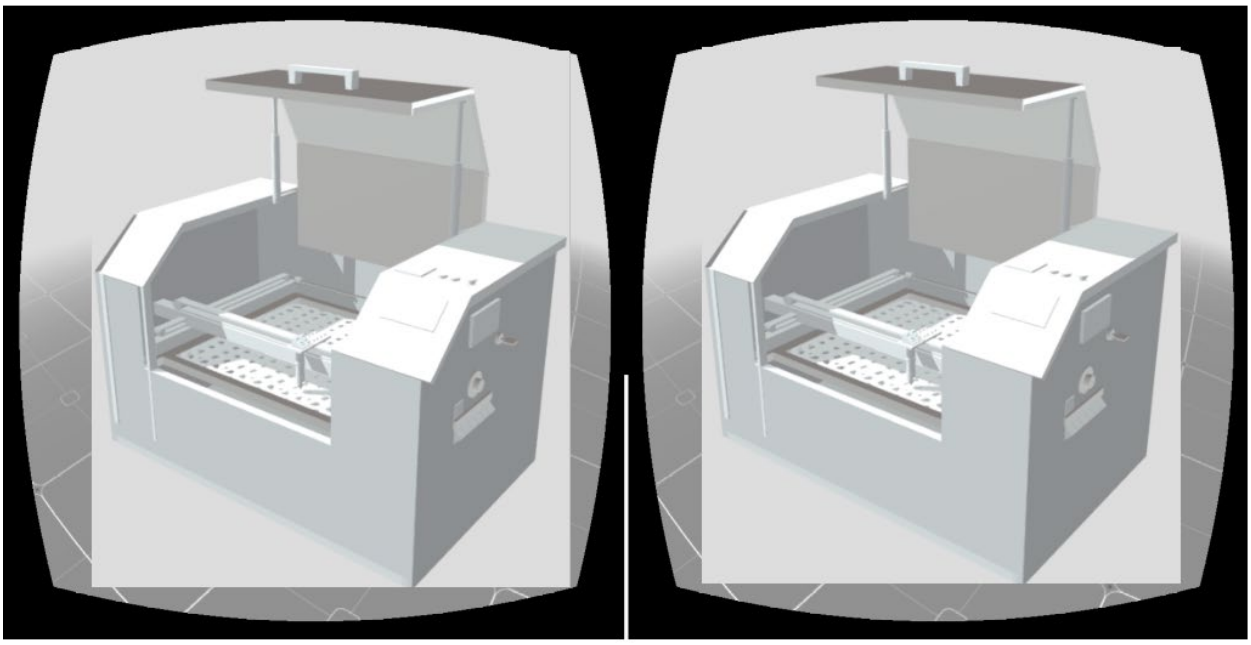


Рисунок 3.5 – Відображення цифрового двійника промислового обладнання (3D-фрезера) через VR-окуляри

З точки зору кібербезпеки всі досліджені інтерфейси людино-машинної взаємодії базуються на процесах, відображених на рисунку 3.1.

3.2 Реалізація досліджуваного AR-інтерфейсу

Щоб дослідити вразливості додатків AR, розглянемо в веб-платформу для занурення в комунікацію під назвою VRComm (рисунок 3.6). VRComm — це веб-система XR (WebXR), яка дозволяє відтворювати як VR, так і AR на пристроях OpenXR. Для відображення AR-контенту використовують окуляри доповненої реальності (рисунок 3.7). Щоб включити AR у VRComm, ми внесли незначні вдосконалення в систему, як-от нова конфігурація кімнати користувачів у AR. Користувачі розміщуються один навпроти одного в доповненій реальності, таким чином віддалений користувач з’являється у вашому власному середовищі з такими ж геометричними властивостями та розмірами, як і на зображенні. Для цієї інтеграції використовуються модулі захоплення: ZED Grabber (з роздільною здатністю

1024 × 1024 пікселів), Mediapipe, GrayAVG та віртуальна камера OBS. Остаточне налаштування користувача складається з одного датчика RGBD, комп'ютера для захоплення даних і HoloLens 2, на якому працює веб-клієнт Social XR. Приклад користувача, який спілкується з ефектом занурення в пристрій Hololens 2 AR, показаний на рисунку 3.8.

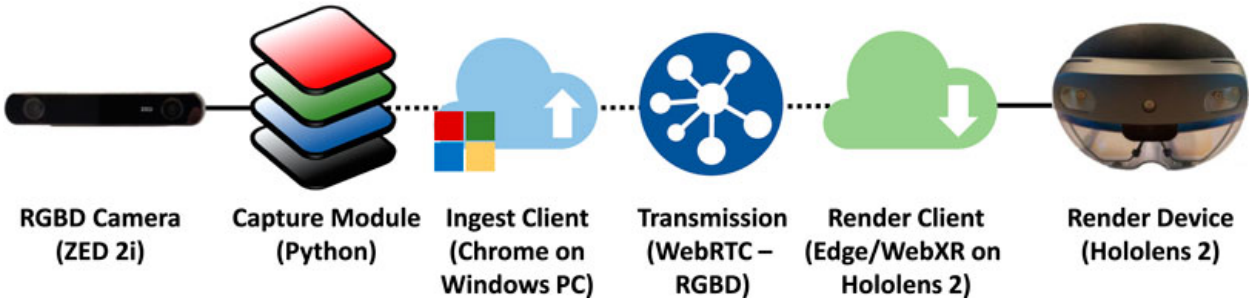


Рисунок 3.6 – Послідовність етапів створення AR-контенту [24]

Рисунок 3.7 – Окуляри доповненої реальності для відображення AR-контенту

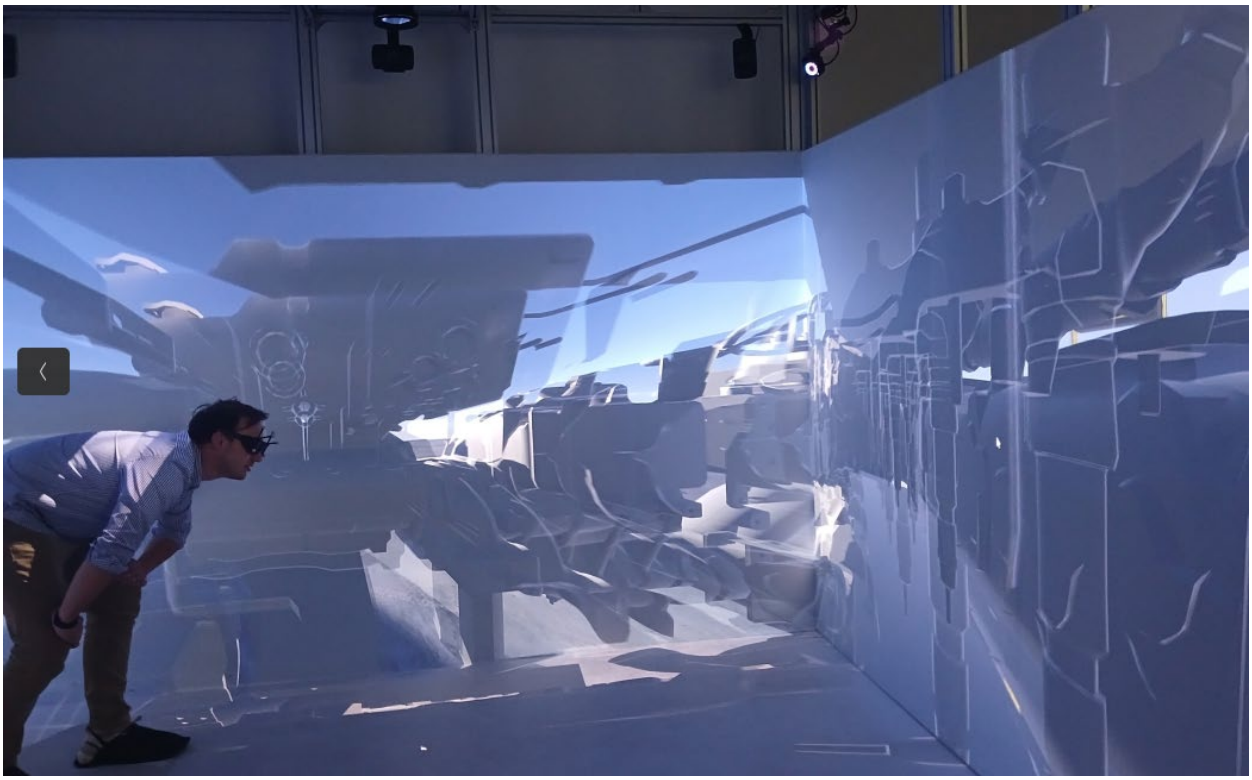
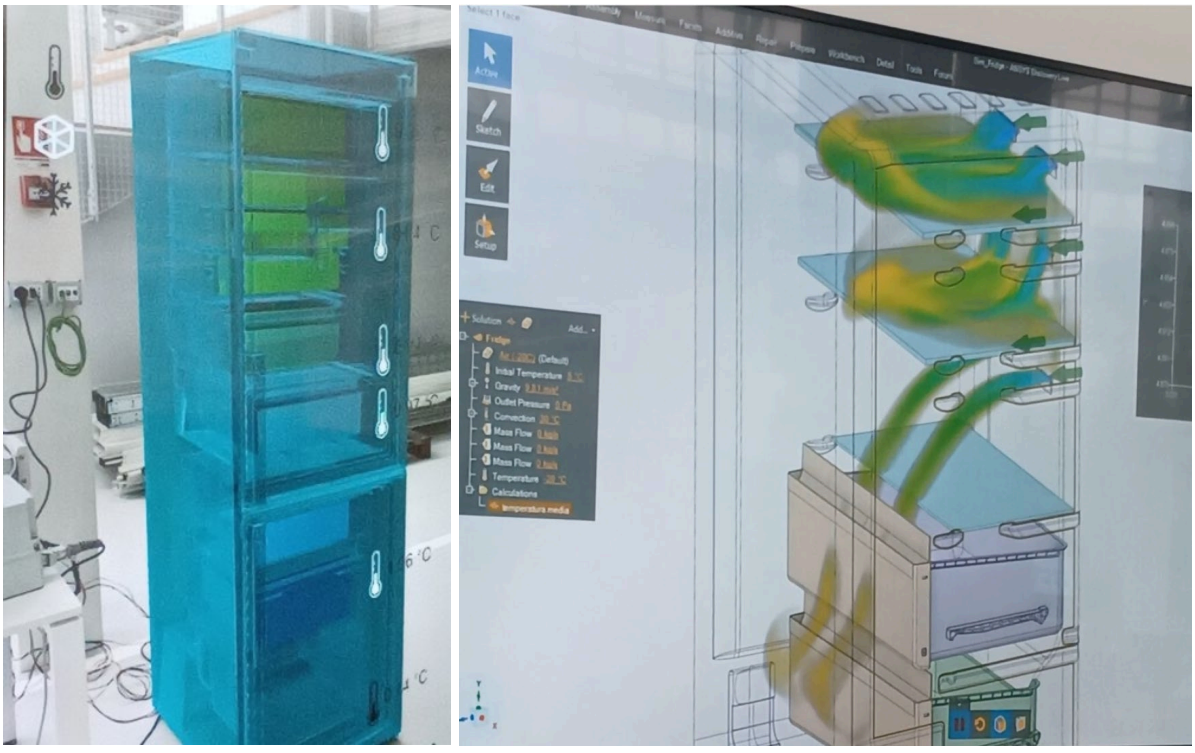


Рисунок 3.8 – Накладання AR-моделі будови двигуна на фізичний



простір в інтерактивному режимі

Рисунок 3.9 – Накладання даних IoT сенсорів на AR-модель морозильної установки (зліва) та відповідна VR-модель (справа)

Можливе також використання більш традиційних засобів (монітори, планшети, смартфони) для відображення як AR-, так і VR-контенту, як показано на рисунку 3.9.

3.3 Планування заходів з протидії вразливостей

Модель загроз визначається як структура, яка детально описує внутрішні та зовнішні вразливості, а також цілі та заходи протидії. Методологія моделювання загроз STRIDE [25] була використана для ідентифікації та характеристики загроз і вразливостей, притаманних інтерфейсам людино-машинної взаємодії та персональним даним користувачів. Діаграма потоку даних (рисунок 3.3) і модель загроз (таблиця 3.1) для інтерфейсів людино-машинної взаємодії, розглянутих у попередніх пунктах, дозволяють конкретизувати вразливості (таблиця 3.2) та запропонувати заходи щодо їх нейтралізації, слідуючи методу, розробленому у статті [9].

Порушення безпеки модулів може призвести до витоку конфіденційної інформації або може поставити під загрозу цілісність усієї виробничої системи. Такі загрози, як підвищення привілеїв (EOP), надають зловмисникам підвищений доступ до сеансів і дій, які дозволяють їм змінювати вміст системи або додавати шкідливі файли. Типова промислова платформа даних збирає великі обсяги конфіденційних даних, які сприйнятливі до маніпуляцій шляхом підробки даних через неавторизовані канали. Крім того, цілісність даних може бути порушена шляхом введення шкідливого коду для зміни об’єктів сеансу чи даних або навіть зміни конфігурації системи чи політики доступу. Помилка сеансу може виникати внаслідок зловмисних дій, які зловмисник виконує для збою сеансів віртуальної реальності, наприклад атак типу «Відмова в обслуговуванні» (DoS). Мережеві атаки, такі як DoS або DdoS, призводять до збоїв системи та

недоступності даних. Більше того, атаки з видаванням себе за іншу особу можуть відбуватися, коли самозванці входять із вкраденими обліковими даними та отримують доступ до конфіденційної інформації користувача.

Таблиця 3.1 – Загрози безпеці та заходи протидії

Тип загрози	**Компонент, для якого проаналізовано загрозу**	**Можливі протидії зламу**
Spoofing (підробка ідентичності)	Інтерфейси VR/AR Користувач	Криптографія (шифрування) Надійні протоколи: AES, SHA-2, TLS 1.2 / 1.3, Надійні механізми автентифікації: Багатофакторна автентифікація, біометрична автентифікація, OAuth
Tampering (зловмисні модифікації даних або процесу)	Дані для пристрою VR/AR, Інтерфейси VR/AR	Маркування безпеки, Захищені протоколи зв'язку, Належні механізми авторизації, Хешування та підписування даних
Repudiation (відмова від дії або розпізнавання настання події)	Інтерфейси VR/AR	Логування та аудити безпеки
Information Disclosure (витік конфіденційних даних)	Необроблені дані, Дані для пристрою VR/AR, Керування інтерфейсом VR/AR	Програмне забезпечення для захисту від зловмисних програм, надлишковість, резервне копіювання
Denial of Service (недоступність даних, сервісу чи мережевого ресурсу для користувачів)	Інтерфейси VR/AR	Функціональні політики безпеки vNET/VPC для контролю доступу або запобігання загрозам
Elevation of Privilege (отримання неавторизованих привілеїв)	Інтерфейси VR/AR	Належні механізми авторизації, Дотримання принципу найменших привілеїв, Сертифікація доступу

Загрози безпеці – це фактори, які безпосередньо впливають на добробут користувачів. Наприклад, захоплення сеансу дозволяє зловмиснику контролювати відтворення VR чи AR, впливаючи на активність користувача під час роботи. Крім того, будь-який мережевий збій, ініційований зловмисником, може спричинити раптові зміни у відтворенні VR, що призведе до дезорієнтації користувача. Ненавмисні дії також можуть спричинити проблеми з безпекою. Наприклад, помилки комп'ютера можуть викликати збої в програмному забезпеченні візуалізації віртуальної реальності, що призведе до раптової різниці у візуальному зображенні в гарнітурі. Розширені сеанси можуть спричинити кіберхворобу (подібну до морської хвороби) у оператора змушеного залишатися в сеансі VR протягом тривалого періоду часу.

Для гарнітур віртуальної реальності та пристроїв доповненої реальності життєво важливо підтримувати оновлення мікропрограми (firmware). Крім додавання нових функцій і вдосконалення наявних, оновлення допомагають виправляти недоліки безпеки. Ефективним способом керування апаратним забезпеченням VR є використання системи керування мобільними пристроями (або MDM), яка блокує гарнітури та забезпечує віддалене оновлення та підтримку. Деякі пристрої постачаються зі своїми системами MDM, як-от Think Reality від Lenovo, тоді як інші можуть використовувати незалежні системи MDM, орієнтовані на VR, як-от ArborXR і ManageXR. Хоча стандартні рішення існують, бажано мати спеціальне процедуру для оновлення мікропрограми та версій MDM з визначеним графіком оновлення мікропрограми та програмного забезпечення MDM кожні 3-6 місяців. Процес оновлення короткий, але нехтування ним може призвести до проблем із сумісністю та багатьох інших проблем. Щоб забезпечити успішне розгортання, бажано використовувати лише один тип апаратного забезпечення VR принаймні протягом життєвого циклу пристрою, який зазвичай триває близько 3-4 років. Це допоможе запобігти дублюванню або

потроєнню всієї роботи, необхідної для розгортання. Коли термін служби апаратного забезпечення закінчується, рекомендується оновити або переключити всю інфраструктуру VR, а не лише окремі частини.

Таблиця 3.2 – Вразливості та засоби протидії

Вразливість	**Можливі протидії**
Незахищені мережеві служби	Ізоляція мережі для пристроїв AR/VR Періодична оцінка вразливостей. Безпечні мережеві протоколи.
Відсутність безпечного механізму оновлення	Оновлення програмного забезпечення пристроїв AR/VR.
Незахищене передавання та зберігання даних	Використання шифрування для захисту даних під час передачі та зберігання. Використання захищених протоколів.
Невідповідне керування пристроєм	Інтеграція пристроїв AR/VR із системами управління ресурсами, відстеженням помилок і виправленнями. Контроль доступу.
Ненадійні налаштування за замовчуванням	Зміна конфігурацій за замовчуванням під час початкового налаштування пристроїв AR/VR . Відключення непотрібних служб.

Впровадження додаткових заходів безпеки для обробки розширеної поверхні атаки для платформ Індустрії 5.0 вимагатиме встановлення пріоритетів запропонованих контрзаходів і протидій, при чому проведений аналіз може сприяти кращому захисту інтерфейсів людино-машинної взаємодії на основі технологій AR/VR.

Запізніле залучення IT та мережевої безпеки часто є помилкою, яку роблять, щоб не уповільнити початок інноваційних проектів. Хоча це може допомогти прискорити запуск проектів, це може перетворитися на серйозну перешкоду в майбутньому. Якщо пристрій VR/AR потребує підключення до Інтернету, тоді безпека мережі має позначити ці IP-адреси мітками, які можуть часто змінюватися з часом. Це необхідно з різних причин, включаючи оновлення мікропрограми, інтеграцію з іншими системами,

можливості для кількох операторів, оновлення платформи та розгортання нових модулів. Практичний спосіб підключити ці пристрої до мережі та мінімізувати ризики для безпеки – створити спеціальну мережу WIFI лише для VR. Це також має додаткову перевагу контролю трафіку даних, оскільки трафік може бути досить значними за розміром і впливати на роботу звичайних користувачів та пристроїв промислового інтернету речей.

3.3 Висновки до третього розділу

В даному розділі наведено результати дослідження типових інтерфейсів людино-машинної взаємодії, які використовують новітні технології віртуальної та доповненої реальності. Визначено модель загроз за методологією STRIDE та на цій основі проаналізовано вразливості, характерні для ЛМІ, які можуть застосовуватися в Індустрії 5.0.

Сезед заходів, які необхідно здійснювати, щоб гарантувати конфіденційність, доступність та цілісність даних підприємства, можна виокремити ті, які стосуються власне даних, ті, які стосуються мережевої інфраструктури, ті, які стосуються людського фактора та ті, які стосуються специфічних пристроїв для захоплення, обробки та відображення VR- та AR-контенту.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Використання імерсивних інтерфейсів людино-машинної взаємодії може бути пов’язане з певними негативними наслідками за умови безвідповідального застосування. Насамперед слід звернути увагу на те, що основним каналом отримання інформації через VR-окуляри є візуальний, і ця інформація може на узгоджуватися від того, що особа отримує через слухове сприйняття, від рецепторів шкіри, від вестибулярної системи. Така неузгодженість може вивликати суттєвий дискомфорт, дезорієнтацію, запаморочення, нудоту та підвищену втому м’язів. Користувачі можуть бути перевантажені занадто великою кількістю інформації, а раптові або інтенсивні джерела стресу, наприклад несподівані звуки під час розмови перед віртуальною аудиторією, можуть послабити увагу та пам’ять.

Є багато факторів, які можуть впливати на частоту та тяжкість цих побічних ефектів [26]. Деякі з цих характеристик стосуються вмісту віртуального середовища, наприклад, наскільки складна сцена або спосіб, у який VR відтворює рухи користувача. Інші мають більше спільного з користувачем, наприклад вік або тривалість занурення в симуляцію VR. Рівень ризику для кожної людини унікальний, але є основні речі, які кожен може зробити, як-от робити регулярні перерви, не використовувати VR більше 30 хвилин за раз і негайно припиняти використання, коли з’являються будь-які симптоми.

Дослідження [27] показали, що 80% користувачів віртуальної реальності повідомляють про короткочасні побічні ефекти від легких до серйозних. Симптоми можуть ускладнювати ефективне виконання базових завдань, як-от читання та написання електронних листів.

Щоб уникнути цих ефектів, варто [28]:

- припинити використання пристроїв AR/VR, як тільки з’являться такі симптоми, як нудота, запаморочення, пітливість і блідість;
- відпочити одну-дві години після використання пристроїв AR/VR перш ніж продовжити діяльність, яка вимагає високого рівня концентрації, наприклад, водіння автомобіля;
- уникати будь-якого впливу екранів за дві години до сну, особливо для дітей і підлітків, які більш чутливі до синього світла;
- крім того, цих технологій слід уникати людям з епілепсією або будь-кому, кого вважають уразливими: вагітним жінкам, людям, які страждають на проблеми з рівновагою, або схильні до мігрені тощо.

Необхідно інформувати користувачів про потенційні наслідки для здоров’я та практику їх запобігання.

Окрім ефектів, пов’язаних із використанням пристроїв віртуальної та/або доповненої реальності, вплив цифрових інструментів на здоров’я в ширшому розумінні залежить від багатьох факторів і зокрема медіа, що використовується (телефони, планшети тощо), вміст, час, місця тощо контексти використання (удень чи ввечері, із сім’єю, з допомогою чи поодинці тощо), призначення використання або індивідуальна вразливість (соціальна чи біологічна).

4.2 Підвищення стійкості роботи VR та AR-інтерфейсів у випадку надзвичайної ситуації

Інтерфейси людино-машинної взаємодії є технологіями, які дозволяють людям спілкуватися з машинами, пристроями, системами або середовищами за допомогою різних каналів, таких як зір, слух, дотик, рух, мова тощо. Інтерфейси віртуальної реальності та інтерфейси доповненої реальності - це технології, які дозволяють користувачам занурюватися в імітаційні світи, створені комп'ютером, та взаємодіяти з ними за допомогою спеціальних пристроїв, таких

як шоломи, рукавиці, контролери тощо. VR-інтерфейси та AR-інтерфейси мають широкий спектр застосувань у різних галузях, таких як освіта, медицина, розваги, архітектура, туризм, військова справа та інші. Однак, разом з розвитком VR-інтерфейсів та AR-інтерфейсів зростає й ризик виникнення негативних явищ спричинених надзвичайними ситуаціями, які можуть призвести до порушення роботи, пошкодження, втрати даних чи навіть травмування користувачів чи третіх осіб. Надзвичайні ситуації можуть бути спричинені різними факторами [29], такими як:

- Помилки людського фактору. Це помилки, які виникають через невідповідність, недосвідченість, невідповідальність, недбалість, знеособлення, стрес, емоції, упередженість, маніпуляцію, залежність або інші характеристики та стани людини, яка взаємодіє з VR-інтерфейсом або AR-інтерфейсом. Приклади таких помилок: неправильне введення даних, невміння користуватися інтерфейсом, недотримання інструкцій, втрата уваги, забуття, паніка, агресія, піддавання соціальному тиску, викрадення ідентифікаційних даних, зловживання привілеями тощо;
- Помилки технічного фактору. Це помилки, які виникають через недосконаліть, складність, несумісність, нестабільність, вразливість, застарілість, відсутність захисту, контролю, аудиту або інші характеристики та стани VR-інтерфейсу, AR-інтерфейсу або пристроїв, які з ними взаємодіють. Приклади таких помилок: помилки програмування, дефекти обладнання, перевантаження системи, несумісність форматів, протоколів, стандартів, втрата даних, збій мережі, відмова апаратури, вразливість до вірусів, троянів, шпигунських програм, злому, кібератак тощо;
- Помилки контекстуального фактору. Це помилки, які виникають через невідповідність, непередбачуваність, небезпечність, конфліктність, незаконність, неетичність або інші характеристики та стани середовища, в якому відбувається взаємодія людини та VR-інтерфейсу або AR-інтерфейсу. Приклади таких помилок: шум, освітлення, температура, вологість, вібрація,

радіація, магнітне поле, погода, катастрофи, війна, тероризм, шпигунство, саботаж, порушення прав, норм, законів, етики тощо.

Важливо враховувати, що надзвичайна ситуація - це порушення нормальних умов життя і діяльності людей на об'єктах або територіях, спричинене аварією, катастрофою, епідемією, стихійним лихом, епізоотією, епіфітотією, великою пожежею, застосуванням засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат, а також до неможливості проживання населення на такій території чи об'єкті, провадження на ній господарської діяльності [30]. Залежно від характеру походження подій, що можуть зумовити виникнення НС на території України, визначаються такі види НС:

- Техногенні НС. Це НС, які виникають внаслідок транспортних аварій, катастроф, пожеж, вибухів, аварій з викидом (загрозою викиду) небезпечних хімічних, радіоактивних і біологічно небезпечних речовин, раптового руйнування споруд; аварій в електроенергетичних системах, системах життєзабезпечення, системах телекомунікацій, на очисних спорудах, у системах нафтогазового промислового комплексу, гідродинамічних аварій тощо. Техногенні НС можуть бути спричинені помилками людського фактору, несправностями технічних систем, зовнішніми впливами або зловмисними діями. Техногенні НС можуть мати різні наслідки, такі як: загибель і травмування людей, забруднення навколишнього середовища, пошкодження майна, порушення життєдіяльності населення та господарської діяльності, соціальні та економічні втрати тощо;
- Природні НС. Це НС, які виникають внаслідок небезпечних геофізичних, геологічних, метеорологічних або гідрологічних явищ, деградації ґрунтів чи надр, пожеж у природних екологічних системах, зміни стану повітряного басейну, інфекційної захворюваністю та отруєнням людей, інфекційним захворюванням свійських тварин, масовою загибеллю диких тварин, ураженням сільськогосподарських рослин хворобами та шкідниками

тощо. Природні НС можуть бути спричинені природними процесами, які відбуваються на Землі або в космосі, або антропогенною діяльністю, яка впливає на природні системи. Природні НС можуть мати різні наслідки, такі як: загибель і травмування людей, знищення або пошкодження майна, порушення життєдіяльності населення та господарської діяльності, зміна природних ландшафтів, біорізноманіття, клімату, екологічної рівноваги тощо;

- Соціальні НС. Це НС, які виникають внаслідок протиправних дій терористичного та антиконституційного спрямування, або пов’язане зі зникненням (викраденням) зброї та небезпечних речовин, нещасними випадками з людьми тощо. Соціальні НС можуть бути спричинені різними суб'єктами, які мають різні мотиви, цілі, ресурси та можливості, такими як: окремі особи, групи, організації, корпорації, держави або їхні агенти. Соціальні НС можуть мати різні наслідки, такі як: загибель і травмування людей, забруднення навколишнього середовища, пошкодження майна, порушення життєдіяльності населення та господарської діяльності, соціальні та економічні втрати, підірвання державної безпеки, суверенітету, територіальної цілісності, конституційного ладу тощо;
- Воєнні НС. Це НС, які виникають внаслідок застосування звичайної зброї або зброї масового ураження, під час якого виникають вторинні чинники ураження населення.

Стійкість даних - це здатність даних зберігати свою цілісність, доступність, конфіденційність та автентичність в різних умовах, а також відновлювати свою функціональність після виникнення збоїв, помилок, атак або надзвичайних ситуацій. Стійкість роботи ЛМІ - це здатність ЛМІ працювати надійно, безпечно, ефективно та гнучко в різних умовах, а також відновлювати свою функціональність після виникнення збоїв, помилок, атак або надзвичайних ситуацій. Для підвищення стійкості роботи VR-інтерфейсів та AR-інтерфейсів у випадку надзвичайної ситуації необхідно використовувати різні методи та заходи [31], такі як:

• Профілактика. Це комплекс дій, спрямованих на запобігання виникненню 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 надзвичайних ситуацій, забезпечення безпеки та відновлення роботи VR-інтерфейсів та AR-інтерфейсів. Реагування включає такі елементи, як: виявлення, ідентифікація, оцінка, інформування, сповіщення, мобілізація, евакуація, локалізація.

За умови відповідального ставлення до застосування інтерфейсів VR- та AR-типу ризики будуть мінімізовані, системи Індустрії 5.0 працюватимуть стійко та надійно.

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 впроваджують VR- та AR-інтерфейси, 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. Окрім ефектів, пов’язаних із використанням пристроїв віртуальної та/або доповненої реальності, вплив цифрових інструментів на здоров’я в ширшому розумінні залежить від багатьох факторів і зокрема медіа, що використовується

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 фарактеру.

ВИСНОВКИ

В цій кваліфікаційній роботі проведено аналіз літературних джерел в галузі кібербезпеки та досліджено вразливості інтерфейсів людино-машинної взаємодії. Розглянуто типи людино-машинних інтерфейсів та їх застосування а також функціонування засобів віртуальної та доповненої реальності. Ці технології дозволяють створювати реалістичні 3D-моделі, які можуть взаємодіяти з реальним світом і надавати багату функціональність, та мають багато переваг для застосування в Індустрії 5.0. В роботі також вивчено характерні загрози, які важливо враховувати при впровадженні інтерфейсів віртуальної та доповненої реальності у розумному виробництві. Для ефективної взаємодії з цифровою промисловою платформою необхідно використовувати інтерфейс, водночас зручний для людини-оператора і сумісний з цифровим двійником.

Для досягнення поставленої мети було виконано такі завдання:

- проаналізувати предметну область;
- з’ясувати типи та характерні особливості вразливостей інтерфейсів людино-машинної взаємодії;
- проаналізувати способи запобігання загрозам, специфічним для інтерфейсів, які можуть застосовуватися в Індустрії 5.0;
- дослідити роботу та спланувати заходи захисту для типових VR- та AR-інтерфейсів;
- зробити висновки щодо можливих шляхів забезпечення конфіденційності, незмінності та доступності даних, які передаються через VR- та AR-інтерфейси.

Промислове застосування інформаційно-комунікаційних платформ вимагає аналізу вразливостей безпеки та розробки засобів захисту, які гарантуватимуть забезпечення конфіденційності, незмінності та доступності даних, а також запобігання несанкціонованому доступу та маніпуляціям.

Таким чином, запобігання несанкціонованому доступу до важливих промислових та особистих даних через вразливості інтерфейсів людино-машинної взаємодії стають суттєвими вимогами та заслуговують на детальний аналіз в контексті Індустрії 5.0.

Крім цього, у розділі "Охорона праці та безпека в надзвичайних ситуаціях" проведено аналіз характерних ризиків для персоналу та впливу надзвичайних ситуацій на підприємства Індустрії 5.0, які впроваджують VR- та AR-інтерфейси.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Ilic, E. Fleisch, Augmented Reality and the Internet of Things. Auto-ID Labs White Paper WP-BIZAPP-068, 2016. DOI: 10.3929/ethz-a-010833302.
2. C. Qiu, S. Zhou, Z. Liu, Q. Gao, J.Tan, Digital assembly technology based on augmented reality and digital twins: a review. Virtual Reality & Intelligent Hardware 1 (2019) 597–610. 597–610. DOI: 10.1016/j.vrih.2019.10.002.
3. J. Egger, T. Masood, Augmented reality in support of intelligent manufacturing – A systematic literature review 2020 140 106195. DOI: 10.1016/j.cie.2019.106195.
4. O. Kramar, Y. Drohobytskiy, Y. Skorenkyy, O. Rokitskyi, N. Kunanets, V. Pasichnyk, O. Matsiuk. Augmented Reality-assisted Cyber-Physical Systems of Smart University Campus. 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 - Proceedings : Institute of Electrical and Electronics Engineers Inc., Vol. 2, pp. 309-313, 2020.
5. C. Baudoin, E. Bournival, E. Clauer. Global Industry Standards for Industrial IoT An Industrial Internet Consortium White Paper. [Електроннийресурс] – Режим доступу до ресурсу: https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf
6. Y. Yin, P. Zheng, C. Li, and L. Wang, A state-of-the-art survey on Augmented Reality-assisted Digital Twin for futuristic human-centric industry transformation. Robot. Comput.-Integr. Manuf. 81 (2023) 102515. URL: https://doi.org/10.1016/j.rcim.2022.102515.
7. Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, I. Baran. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, Vol. 1840, Issue 1, 012026, 2021.

8. Milgram, P., Takemura, H., Utsumi, A., and Kishino, F. (1994). Augmented reality: a class of displays on the reality-virtuality continuum. *Proc. SPIE* 2351, 282–292. doi: 10.1117/12.197321
9. 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.
10. 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.
11. 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.
12. 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.
13. Індустрія 5.0: напрями дій та шляхи розвитку. [Електронний ресурс]. URL: https://www.clusters.org.ua/blog-single/industry-5-0-napriamy-diy/
14. 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/
15. Індустрія 5.0: бачення трансформацій від Європейської комісії. [Електронний ресурс]. URL: https://www.clusters.org.ua/blog-single/industry-5-0/
16. Z. Yusuf, V. Lukic. Unleashing the Power of Data with IoT and Augmented Reality. Boston Consulting Group-BCG. 2020. [Електронний ресурс]. URL:

https://web-assets.bcg.com/img-src/BCG-Unleashing-the-Power-of-Data-with-IoT-Augmented-Reality-Mar-2020-Rev_tcm9-241247.pdf

17. G. Johannsen. Design of Visual and Auditory Human-Machine Interfaces with User Participation and Knowledge Support. In: Schlick, C. (eds) Industrial Engineering and Ergonomics. Springer, Berlin, Heidelberg. 2009. [Електронний ресурс]. URL: https://doi.org/10.1007/978-3-642-01293-8_37.
18. Доценко С. І. Людино-машинний інтерфейс: навч. посібник. – Харків: УкрДУЗТ, 2022. – 135 с.
19. B. Odeleye, G. Loukas, R.Heartfield, F. Spyridonis. Detecting framerate-oriented cyber attacks on user experience in virtual reality. 2021. [Електронний ресурс]. URL: https://www.researchgate.net/publication/354193624
20. P. Casey, I. Baggili, A. Yarramreddy. Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing. 2019 pp. 1-1. 10.1109/TDSC.2019.2907942.
21. M. U. Rafique and S.-C. S. Cheung.Tracking Attacks on Virtual Reality Systems. in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 41-46, 1 March 2020, doi: 10.1109/MCE.2019.2953741.
22. J. Steuer. Defining virtual reality: Dimensions determining telepresence. Journal of communication, 42(4): 73–93, 1992 DOI:10.1111/j.1460-2466.1992.tb00812.x
23. D.J. Zielinski, H.M. Rao, M.A. Sommer, R.Kopper. Exploring the effects of image persistence in low frame rate virtual environments. In 2015 IEEE Virtual Reality (VR), pages 19–26. IEEE, 2015.
24. S.N.B. Gunkel, S. Dijkstra-Soudarissanane, H.M. Stokking, O.A. Niamut. From 2D to 3D video conferencing: modular RGB-D capture and reconstruction for interactive natural user representations in immersive extended reality (XR) communication Front. Signal Process., 22 May 2023

Sec. Image Processing Volume 3 - 2023 | https://doi.org/10.3389/frsip.2023.1139897.

25. 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.
26. A.D. Souchet, D. Lourdeaux, J.-M. Burkhardt, P.A. Hancock Design guidelines for limiting and eliminating virtual reality-induced symptoms and effects at work: a comprehensive, factor-oriented review. Front. Psychol., Sec. Media Psychology, vol.14, 2023. [Електронний ресурс]. URL: https://doi.org/10.3389/fpsyg.2023.1161932.
27. K.M. Stanney, H. Nye, S. Haddad, K.S. Hale, C.K. Padron. EXTENDED REALITY (XR) ENVIRONMENTS. In HANDBOOK OF HUMAN FACTORS AND ERGONOMICS (eds G. Salvendy and W. Karwowski). 2021 [Електронний ресурс]. URL: https://doi.org/10.1002/9781119636113.ch30
28. Opinion of the French Agency for Food, Environmental and Occupational Health & Safety on the "health effects associated with exposure to virtual and/or augmented reality technologies", Maisons-Alfort, 1 June 2021 [Електронний ресурс]. URL: https://www.anses.fr/en/system/files/AP2017SA0076EN.pdf
29. Я.І. Бедрій Безпека життєдіяльності: Навч.посібн. – К.: Вид-во Кондор, 2009.
30. 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/.
31. Навчальний посібник «ТЕХНОЕКОЛОГІЯ ТА ЦИВІЛЬНА БЕЗПЕКА. ЧАСТИНА «ЦИВІЛЬНА БЕЗПЕКА»» / автор-укладач В.С. Стручок–

Тернопіль: ФОП Паляниця В. А., – 156 с. ОтримSimon N. B. Gunkel, Sylvie Dijkstra-Soudarissanane, Hans M. Stokking, Omar A. Niamut. From 2D to 3D video conferencing: modular RGB-D capture and reconstruction for interactive natural user representations in immersive extended reality (XR) communication Front. Signal Process., 22 May 2023 Sec. Image Processing Volume 3 - 2023 | https://doi.org/10.3389/frsip.2023.1139897

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.О. Горішний – ст. гр. СБмз-61, Ю.Л. Скоренький к.ф.-м.н., доц.
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ІНТЕРФЕЙСІВ ЛЮДИНО-МАШИННОЇ ВЗАЄМОДІЇ ДЛЯ ІНДУСТРІЇ 5.0

M. Horishnyy, Dr. Yu. Skorenkyy

STUDY OF VULNERABILITIES OF THE HUMAN-MACHINE INTERFACES FOR INDUSTRY 5.0

Ключові слова: інформаційна безпека, інтерфейс людино-машинної взаємодії, вразливості.
Key words: information security, human-machine interaction interface, vulnerability.

При переході до моделі Industry 5.0 виробнича компанія обов'язково впроваджує в усі процеси людино-орієнтований підхід. Це включає моделювання, інжиніринг, виробництво та управління, а також системи підтримки прийняття рішень. Людський фактор визначає ефективність як на рівні проектування, так і на рівні експлуатації, тим самим встановлюючи особливі вимоги до технологічного розвитку виробничого об'єкта. Серед різних аспектів, які слід враховувати, когнітивні особливості людей-операторів і осіб, які приймають рішення, мають величезне значення. Вони визначають, зокрема, продуктивність виробничого об'єкта, якість продукту, психологічну задоволеність персоналу. Надзвичайно важливо ефективні та інтуїтивно зрозумілі інтерфейси для взаємодії людини та машини. Як такий, інтерфейс із підтримкою доповненої реальності (AR) має неперевершений потенціал і може бути незамінним інструментом для впровадження цифрового двійника і керування фізичним обладнанням на заводі в реальному часі [1, 2]. Він може накладати інформаційний рівень з характеристиками, недоступними для людського сприйняття, але які надаються промисловому цифровому близнюку датчиками Інтернету речей і своєчасно відображаються в аналітичному рівні, важливому для прийняття обґрунтованих рішень.

Інформаційна безпека та кіберзахист, які передбачають забезпечення конфіденційності, незмінності та доступності даних, а також запобігання несанкціонованому доступу та маніпуляціям, стають найважливішими вимогами та заслуговують на особливу увагу в контексті Індустрії 5.0 при розробці інтерфейсів людино-машинної взаємодії.

В даній роботі представлено аналіз вразливостей інтерфейсів людино-машинної взаємодії, важливих для ефективного функціонування промислових цифрових платформ Індустрії 5.0.

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. P.K. Reddy, V.Q. Pham, B. Prabadevi, M. Liyanage. Industry 5.0: A Survey on Enabling Technologies and Potential Applications. Journal of Industrial Information Integration 26 (2021) 100257. DOI: 10.1016/j.jii.2021.100257