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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Дослідження кіберзахисту “розумних” інформаційно-технологічних проектів**

Виконав(ла): студент(ка) курсу 6, груп и СТм-61
спеціальності 126 «Інформаційні системи та технології»
(шифр і назва спеціальності)

(підпис) Олійник В.Ю. (прізвище та ініціали)

Керівник (підпис) Марценко С.В. (прізвище та ініціали)
Нормоконтроль (підпис) Дуда О.М. (прізвище та ініціали)
Завідувач кафедри (підпис) Боднарчук І.О. (прізвище та ініціали)
Рецензент (підпис) Жаровський Р.О. (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 комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня МАГІСТР
(назва освітнього ступеня)

за спеціальністю 126 «Інформаційні системи та технології»
(шифр і назва спеціальності)

студенту Олійнику Владиславу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи **Дослідження кіберзахисту "розумних" інформаційно-технологічних проектів**

Керівник роботи **Марценко Сергій Володимирович, к.т.н., доц.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » листопада 2023 року № 4/7 1097 .

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічне завдання на дослідження кіберзахисту "розумних" інформаційно-технологічних проектів

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області; 2 Дослідження кіберзахисту "розумних" інформаційно-технологічних проектів; 3 Охорона праці та безпека в надзвичайних ситуаціях; Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета, об'єкт предмет дослідження; Завдання дослідження; Модель хмарної безпеки; Ризики безпеки "розумних" інформаційно-технологічних проектів; Стандарти безпеки для "розумних" проектів; Види тестування безпеки "розумних" проектів; Моделі безпеки "розумних" проектів; Реалізації моделей безпеки; Реалізації моделей безпеки; Загрози "розумного" виробництва; Захист операційних технологій на основі IIoT; Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Семчишин В.С., доц. каф. МТ		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст.викл.		

7. Дата видачі завдання _____

1.1 КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.23	*Виконано*
2.	Підбір наукових джерел щодо дослідження кіберзахисту	26.11.23-28.11.23	*Виконано*
	розумних інформаційно-технологічних проектів		
3.	Переклад та опрацювання наукових джерел щодо	29.11.23-1.12.23	*Виконано*
	теми роботи		
4.	Виконання дослідження кіберзахисту	2.12.23-4.12.23	*Виконано*
	“розумних” інформаційно-технологічних проектів		
5.	Оформлення розділу «Аналіз предметної області»	5.12.2023-7.12.2023	*Виконано*
6.	Оформлення розділу «Дослідження кіберзахисту	8.12.2023-13.12.2023	*Виконано*
	“розумних” інформаційно-технологічних проектів»		
	Виконання завдання до підрозділу «Охорона праці»	14.12.2023-15.12.2023	*Виконано*
7.	Виконання завдання до підрозділу «Безпека в	16.12.2023-17.12.2023	*Виконано*
8.	надзвичайних ситуаціях»		
	Оформлення кваліфікаційної роботи	18.12.2023-19.12.2023	*Виконано*
9.	Нормоконтроль	19.12.2023-20.12.2023	*Виконано*
10.	Перевірка на плагіат	21.12.2023	*Виконано*
11.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
12.	Захист кваліфікаційної роботи	29.12.2023	

Студент _____ Олійник В.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження кіберзахисту “розумних” інформаційно-технологічних проектів // Кваліфікаційна робота // Олійник Владислав Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СТм–61 // Тернопіль, 2023 // С. 75 , рис. – 9 , табл. – , кресл. – , додат. – 3 , бібліогр. – 60 .

Ключові слова: МЕРЕЖІ, МЕРЕЖЕВІ АРХІТЕКТУРИ, КІБЕРЗАХИСТ, “РОЗУМНІ” ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНІ ПРОЕКТИ, МОДЕЛІ БЕЗПЕКИ.

У роботі проведено дослідження кіберзахисту “розумних” інформаційно-технологічних проектів, що дало змогу визначити вимоги архітектур кіберзахисту, технології та стандарти, що допомагають протидіяти атакам в проектах даного типу.

В першому розділі кваліфікаційної роботи здійснено аналіз кіберзахисту “розумних” інформаційно-технологічних проектів, що виокремило аналіз загроз, створення заходів захисту, тестування безпеки, дотримання стандартів безпеки, здійснення оновлень.

Другий розділ кваліфікаційної роботи присвячений дослідженню кіберзахисту “розумних” інформаційно-технологічних проектів. Здійснено дослідження архітектур моделей кіберзахисту “розумних” інформаційно-технологічних проектів.

Метою дослідження є кіберзахист “розумних” інформаційно-технологічних проектів. Об’єкт дослідження – процес отримання, передавання та захисту даних в мережах критичних інфраструктур. Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

ANNOTATION

Research of cyber defense of “smart” information and technological projects // Diploma thesis Master degree // Oliinyk Vladyslav Y. // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2023 // P. 75 , Tables – , Fig. – 9 , Diagrams – , Annexes. – 3 , References – 60 .

The study of cybersecurity of smart information technology projects was conducted, which made it possible to determine the requirements of cybersecurity architectures, technologies and standards that help to counteract attacks in projects of this type.

The first section of the qualification work analyzes the cybersecurity of smart information technology projects, which includes threat analysis, creation of security measures, security testing, compliance with security standards, and updates.

The second chapter of the qualification work is devoted to the study of cyber defense of smart information technology projects. The author has studied the architectures of cybersecurity models for smart information technology projects.

The purpose of the study is to study the cybersecurity of smart information technology projects. The object of research is the process of receiving, transmitting and protecting data in critical infrastructure networks. The subject of the study is the theory of telecommunication network design, data transmission theory, and information security theory.

Keywords: NETWORKS, NETWORK ARCHITECTURES, CYBER SECURITY, SMART INFORMATION TECHNOLOGY PROJECTS, SECURITY MODELS.

ЗМІСТ

ВСТУП

Кіберзахист “розумних” інформаційно-технологічних проектів залишається надзвичайно актуальним і важливим у сучасному світі. Зростаюча кількість “розумних” рішень, Інтернет речей (IoT), штучний інтелект (AI), системи автоматизації, дрони та інші “розумні” технології стають все більш поширеними в різних галузях, збільшуючи потенційні точки входу для кіберзагроз.

Збільшення обсягу та цінності даних, які обробляються та зберігаються в “розумних” системах, робить їх більш привабливими для кіберзлочинців. Уразливість “розумних” систем може мати серйозні наслідки, включаючи проблеми з безпекою особистої інформації, ризики для здоров’я та безпеки, порушення операцій бізнесу тощо. Кіберзлочинці постійно вдосконалюють свої методи та атаки, щоб зламати захист “розумних” систем. Законодавство стає все більш жорстким у вимогах до кібербезпеки, що створює додатковий тиск на компанії для забезпечення належного захисту даних та систем.

У зв’язку з цим, розуміння, розробка та вдосконалення стратегій кіберзахисту для “розумних” інформаційно-технологічних проектів залишається вкрай актуальним. Тільки шляхом постійного вдосконалення заходів безпеки можна забезпечити надійний захист цих інноваційних технологій від кіберзагроз.

Мета і завдання дослідження. Метою дослідження є кіберзахист “розумних” інформаційно-технологічних проектів. Досягнення поставленої мети передбачає виконання наступних завдань: проаналізувати кіберзахист “розумних” інформаційно-технологічних проектів, здійснити аналіз загроз та ризиків кібербезпеці, проаналізувати протоколи та стандарти безпеки, дослідити архітектури, моделі, атаки та методи протидії в “розумних” інформаційно-технологічних проектах.

Об’єкт дослідження – процес отримання, передавання та захисту даних в мережах критичних інфраструктур.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

Практичне значення одержаних результатів. Здійснено аналіз кіберзахисту “розумних” інформаційно-технологічних проектів, що серед широкого кола завдань виокремило такі, як аналіз загроз, створення заходів захисту, тестування безпеки, дотримання стандартів безпеки, здійснення оновлень. Весь цей процес не є статичним, що потребує постійного моніторингу і прийняття мір. Проведено аналіз кіберзагроз в проектах “розумне” місто, що визначило кібербезпеку як ключовий фактор для його реалізації. Інформаційні системи, цифрові комунікації та навколишнє цифрове середовище є ключовими елементами для успішних процесів прийняття рішень, які мають на меті вироблення обґрунтованих рішень з важливих і чутливих питань. Аналіз ризиків кібербезпеки в “розумних” інформаційно-технологічних проектах включає в себе оцінку потенційних загроз і вразливостей, які можуть вплинути на безпеку цих систем. Стандарти безпеки для “розумних” інформаційно-технологічних проектів грають критичну роль у забезпеченні безпеки цих систем. Такі стандарти встановлюють рекомендації, вимоги та керівні принципи, які допомагають розробникам, виробникам та користувачам забезпечувати високий рівень кібербезпеки. Подано основні стандарти, що забезпечують кіберзахист “розумних” інформаційно-технологічних проектів. Тестування безпеки “розумних” інформаційно-технологічних проектів є важливою складовою для виявлення потенційних вразливостей і заходів забезпечення безпеки цих систем. Методи тестування допомагають ідентифікувати потенційні слабкі місця в “розумних” проектах та дають змогу розробникам приймати заходи для їх виправлення або підвищення рівня захищеності. Тестування безпеки

має бути постійним процесом, оскільки кіберзагрози постійно еволюціонують.

Наукова новизна розробки: досліджено кіберзахист “розумних” інформаційно-технологічних проектів. Здійснено визначення вимог архітектур кіберзахисту проектів даного типу, що дало змогу виокремити їх важливі елементи, які утворять основу архітектури. Досліджено архітектури моделей кіберзахисту “розумних” інформаційно-технологічних проектів, що на основі аналізу сильних та слабких сторін може бути використано при розгортанні конкретних випадків згідно вимог технічного завдання проекту. Досліджено розвиток технологій кіберзахисту “розумних” інформаційно-технологічних проектів в контексті Індустрії 4.0, що на основі стандарту NIST 1500-201 уможливило визначення областей захисту і на основі конкретного прикладу дало змогу надати рекомендації щодо їх захисту. Проведено дослідження кіберфізичних атак на “розумні” проекти, де проаналізовано останні виклики в індустрії кіберзахисту і показано наслідки їх діяльності. Досліджено методи кіберзахисту “розумних” інформаційно-технологічних проектів де поряд з традиційними методами захисту IT інфраструктури розглянуто спеціалізовані під операційні технології.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз кіберзахисту “розумних” інформаційно-технологічних проектів

Дослідження кіберзахисту в сфері “розумних” інформаційно-технологічних проектів – це важливий аспект сучасного технологічного світу. Воно охоплює аналіз потенційних загроз для смарт-технологій, таких як Інтернет речей (IoT), штучний інтелект, автономні системи і розробку стратегій захисту від цих загроз [1-6].

Технологічний прогрес надає безліч можливостей, але разом з цим і збільшується потенціал кіберзагроз. Дослідження в цій області включає в себе аналіз потенційних слабкостей у “розумних” системах, розробку заходів з кіберзахисту, тестування на вразливість, вдосконалення стандартів безпеки та впровадження заходів для запобігання кібератак.

Для досягнення поставлених цілей потрібно провести дослідження наступних аспектів кіберзахисту “розумних” інформаційно-технологічних проектів:

– аналіз загроз, який полягає в ідентифікації потенційних загроз для “розумних” проектів та їх систем безпеки;

– створення заходів захисту, що відбувається через розробку технічних, процесних і організаційних заходів для захисту від кіберзагроз;

– тестування безпеки, яке потребує проведення тестів на вразливість для виявлення потенційних слабкостей у системах;

– стандарти безпеки, вимагають постійної розробки та дотримання стандартів безпеки для “розумних” технологій;

– оновлення та удосконалення, повинне відбуватись через постійне вдосконалення заходів кіберзахисту для відповіді на нові та перспективні загрози.

Це важлива сфера, яка продовжує розвиватися, оскільки технології також стають все більш складними, і важливо залишатися в тренді за стосовно безпекових рішень.

1.2 Аналіз кіберзагроз в проектах “розумне” місто

Розумні міста – це міські простори, що характеризуються широким використанням інформаційно-комунікаційних технологій (ІКТ). Вони мають на меті підвищити політико-економічну ефективність та підтримати людський і соціальний розвиток, покращуючи таким чином якість життя своїх громадян. Місто вважається “розумним”, коли є рушійні сили сталого еколого-економічного зростання, високої якості життя та свідомого управління природними ресурсами через партисипативне та демократичне врядування. До рушійних сил “розумних” міст належать інвестиції в технологічну інфраструктуру, інвестиції в людський капітал та соціальні інвестиції. Крім того, інші аспекти, які слід враховувати при класифікації міст як розумних, включають міську мобільність, прихильність до екологічних питань та соціальних питань. Таким чином, розумні міста використовують технології та інновації для покращення якості життя своїх мешканців, збільшення економічної цінності, що створюється в громаді, та сприяння екологічній стійкості.

Розумні міста зосереджені на наданні комплексу ініціатив, заходів та послуг у різних сферах застосування в містах, які спрямовані на оптимізацію та покращення добробуту їх населення, як з точки зору здоров’я, так і з точки зору навколишнього середовища. У широкому сенсі, мета “розумних міст” полягає в динамічній оптимізації міста для забезпечення набору дій і послуг для більш інклюзивного і сталого міста. Основна роль, яку можуть взяти на себе ІКТ, полягає в інтеграції послуг інформаційних систем з кожної сфери діяльності міста, таких як охорона здоров'я, освіта, транспорт, енергетика,

водопостачання та утилізація відходів, для більш ефективного та повсюдного надання державних послуг громадянам. Крім того, ІКТ відіграють певну роль в об'єднанні та інтеграції різних складних систем на рівні технологічної інфраструктури, соціальних структур, політики та людської поведінки.

У той же час, роль ІКТ для бізнесу, громадян та громадянського суспільства у створенні, винаході та експериментуванні нового для покращення та оптимізації якості життя в містах також широко відома і визнана. Однак, беручи до уваги вплив цифрових послуг та допоміжних послуг різних сфер через комунікаційні мережі та використання ІКТ, важливо розглянути питання ідентифікації ризиків та викликів, пов'язаних з розумними містами, для зменшення або пом'якшення цих ризиків, зокрема в різних секторах діяльності, таких як системи управління промисловістю, інтелектуальні транспортні системи, Інтернет речей (IoT) та цифрова охорона здоров'я (e-health), на додаток до інших сфер втручання міст. Питання кібербезпеки та конфіденційності даних стають все більш актуальними, сумнівними і складними як для громадян, так і для технологічних компаній, що надають цифрові послуги, які усвідомлюють проблему кіберзлочинності та кібертероризму.

Кібербезпека відіграє ключову роль у "розумних" містах завдяки зростаючій взаємопов'язаності та широкому використанню ІКТ. У "розумних" містах системи та пристрої об'єднані в мережу для збору даних, моніторингу інфраструктури, оптимізації послуг та підвищення якості життя громадян. Однак така взаємопов'язаність наражає міста на низку кіберзагроз, що робить безпеку даних та інфраструктури критично важливою. Огляди літератури, проведені в галузі "розумних міст", визначили кібербезпеку як ключовий фактор для впровадження "розумного міста" []. Крім того, дослідження в цій галузі намагалися охарактеризувати різні ризики безпеки з урахуванням теоретичних моделей виявлення вразливостей та емпіричних сценаріїв на прикладі кількох "розумних міст", таких як Дубай, Барселона,

Шанхай. Основною прогалиною в дослідженнях є складність інтегративного огляду основних ризиків для безпеки з урахуванням міждисциплінарної перспективи, яка може доповнити бачення наукових і промислових партнерів. Поєднання наукових і промислових партнерів у розвитку “розумних” міст має першорядне значення, враховуючи, що проблеми “розумних” міст є складними і багатогранними. Тому, наукові дослідження можуть надати глибоке розуміння цих викликів, тоді як промислові партнери можуть поділитися своїм практичним досвідом і знаннями про динаміку ринку. Поєднання цих перспектив дасть змогу розробляти та реалізовувати проекти “розумних міст” у більш цілісний та комплексний спосіб. З огляду на це, при дослідженні потрібно використовувати комплексну перспективу, яка є результатом аналізу ролі кібербезпеки в “розумних” містах, розглядаючи проекти, в яких беруть участь європейські університети, дослідницькі центри і компанії. База проектів, що фінансуються ЄС, доступна на порталі CORDIS. При дослідженні кіберзагроз “розумних” інформаційно-технологічних проектів потрібно проаналізувати: характеристики вимірів ризиків безпеки, які можна знайти в розумних містах; потім визначити заходи, запропоновані в рамках цих проектів для пом’якшення раніше виявлених ризиків безпеки; дослідити нові ризики безпеки, які можуть виникнути в умовах недавнього технологічного і соціального розвитку.

Останніми роками потенційний і реальний вплив загроз безпеці в кіберпросторі став очевидним завдяки кільком інцидентам, що мали прямий вплив на безпеку країн і громадян. Цифрові технології та кіберпростір – це не лише ресурси і простір, де можна краще і ефективніше робити те, що раніше було складно, довго і дорого. Нова реальність створила потенціал для значної зміни впливу різних груп чи акторів на міжнародній та національній, соціальній чи діловій сценах.

Інформаційні системи, цифрові комунікації та навколишнє цифрове середовище є ключовими елементами для успішних процесів прийняття рішень, які мають на меті вироблення обґрунтованих рішень з важливих і чутливих питань. На рисунку 1.1 показано приклад цифрового середовища.

Рисунок 1.1 – Цифрове середовище

Сьогодні ми можемо створювати, оновлювати і зберігати більше інформації, ніж будь-коли в минулому, але ніколи ще ця інформація не була під такою загрозою, як сьогодні. Для підтримки стійкої і конкурентоспроможної інфраструктури, яка є життєво важливою для виживання націй у всьому світі, з’явилося прагнення інвестувати в механізми і процеси, які випливають з необхідності докладати всіх можливих зусиль для забезпечення безпеки цифрових ресурсів. Деякі автори підкреслюють, що світ дуже взаємопов’язаний, а ресурси пов’язані зі структурами і мережами в глобальному масштабі. Тому однією з головних проблем для забезпечення надійного захисту та збереження інформації стала безпека інформаційних систем, як державних, так і приватних, та їхньої інформації, яка має важливе значення для підтримки діяльності організацій. Також виявляється, що інформаційна безпека є життєво важливою для побудови та підтримки довіри клієнтів. Споживачі все більше стурбовані питаннями конфіденційності та

захисту своїх персональних даних. Демонструючи серйозну прихильність до інформаційної безпеки, організації можуть завоювати довіру клієнтів і встановити тривалі відносини. Це також є важливим елементом в контексті впровадження “розумних міст”, в якому встановлені відносини також проявляються у включенні нових послуг в “розумні міста”.

Інформаційна безпека охоплює кілька сфер. У широкому сенсі ми можемо розглядати інформаційну безпеку як захист даних та інформації окремих осіб, організацій та урядів від несанкціонованого доступу, неправильного використання, розкриття, зміни або знищення. Рисунок 1.2 відображає інформаційну безпеку.

Рисунок 1.2 – Інформаційна безпека

Важливість інформаційної безпеки можна розуміти в різних аспектах. Інформаційна безпека повинна забезпечувати конфіденційність даних, запобігаючи потраплянню конфіденційної інформації в чужі руки. Це особливо важливо, коли йдеться про персональні дані, фінансову інформацію, комерційну таємницю або державну інформацію. На основі огляду літератури можна дійти висновку, що порушення конфіденційності може призвести до серйозних наслідків, таких як крадіжка особистих даних, фінансові втрати або шкода репутації. Інформаційна безпека також має на меті забезпечити цілісність даних (тобто їхню точність, повноту та

узгодженість у часі). Важливо, щоб інформація не була змінена несанкціоновано або випадково, щоб вона залишалася надійною і точною. Відсутність цілісності даних може призвести до неправильних рішень, помилок у процесах і втрати довіри до інформації. Нарешті, інформаційна безпека повинна гарантувати, що дані та системи будуть доступні, коли це необхідно. Це означає захист інформації від технічних збоїв, кібератак або стихійних лих, які можуть поставити під загрозу доступність даних. Дослідження взаємозв’язку між доступністю та іншими питаннями безпеки показали, що відсутність доступності може спричинити перебої в роботі, зниження продуктивності та фінансові втрати. У контексті розумних міст це дослідження також підтверджує, що відсутність доступності може мати глибокий і далекосяжний вплив на різні аспекти міського життя. Розумні міста покладаються на мережу взаємопов'язаних пристроїв, датчиків і систем для надання критично важливих послуг і даних у режимі реального часу. Перебої в наданні послуг можуть призвести до незручностей для громадян, економічних втрат для бізнесу і навіть до загрози громадській безпеці.

Інформаційна безпека, наука про дані та технології є взаємопов’язаними сферами. Наука про дані передбачає вилучення знань та інсайтів з даних. Вона охоплює широкий спектр методів, включаючи збір даних, очищення даних, аналіз даних, візуалізацію даних, машинне навчання і статистичне моделювання. Технології слугують основою як для інформаційної безпеки, так і для науки про дані. Технологічний прогрес уможливив швидке зростання цифрових даних і розробку складних інструментів та алгоритмів для їх обробки та аналізу. Ключові технологічні компоненти, які підтримують інформаційну безпеку та науку про дані, включають платформи великих даних, хмарні обчислення, штучний інтелект, машинне навчання, криптографію, а також мережеві технології та комунікації. Використання хмарних технологій в організаціях зробили революцію в зберіганні, доступності та обробці даних. Вони надають

масштабовану інфраструктуру для розміщення великих наборів даних, а також для розміщення додатків з науки про дані та рішень для забезпечення безпеки. На рисунку 1.3 показано модель хмарної безпеки.

Рисунок 1.3 – Модель хмарної безпеки

Провайдери хмарних сервісів утримують величезні центри обробки даних з широким спектром серверів, сховищ і мережевих ресурсів. Вони можуть динамічно розподіляти і перерозподіляти ці ресурси залежно від попиту. Це дає змогу користувачам масштабувати (додавати більше ресурсів) або зменшувати (видаляти надлишкові ресурси) за потреби, без необхідності інвестувати у власне фізичне обладнання. Крім того, хмарні платформи пропонують еластичність, що означає, що вони можуть автоматично підлаштовувати ресурси у відповідь на зміну робочого навантаження. У періоди високого попиту хмара може швидко надати додаткові ресурси, а в періоди низького попиту – звільнити непотрібні ресурси. Динамічне масштабування забезпечує ефективне використання ресурсів та економічну ефективність. Хмарні обчислення і машинне навчання – це дві потужні

технології, які можна ефективно поєднувати, щоб використовувати їхні сильні сторони. Інтеграція машинного навчання з хмарними обчисленнями дозволяє створювати масштабовані та гнучкі рішення для обробки та аналізу великих масивів даних, побудови складних моделей і розгортання додатків на основі штучного інтелекту. Завдання машинного навчання часто вимагають значних обчислювальних ресурсів, особливо для навчання складних моделей. Бачення режиму програмування паралельних обчислень в контексті хмарних обчислень уможливив розподілені обчислення, які можуть значно прискорити процес навчання за рахунок розподілу робочого навантаження між декількома серверами або вузлами. Ця можливість паралельної обробки може бути актуальною при навчанні складних моделей на великих наборах даних.

1.3 Аналіз ризиків кібербезпеки “розумних” інформаційно-технологічних проектів

Аналіз ризиків кібербезпеки в “розумних” інформаційно-технологічних проектах включає в себе оцінку потенційних загроз і вразливостей, які можуть вплинути на безпеку цих систем. До ключових аспектів, які часто враховуються під час аналізу ризиків можна віднести:

– потенційні загрози, що включає в себе різноманітні види кіберзагроз, такі як хакерські атаки, віруси, витоки даних, фішинг, деніал-оф-сервіс (DDoS) тощо. Дослідження ризиків орієнтується на ідентифікацію цих загроз і їх потенційний вплив на “розумні” проекти;

– вразливості систем, що полягає в аналізі безпеки і виявляє можливі слабкі місця в системі, через які можуть проникнути атаки. Це може бути пов’язане з програмним забезпеченням, апаратними компонентами, нестачею оновлень тощо;

– вплив на функціонування, який оцінює можливий вплив кібератак на роботу “розумних” систем. Наприклад, якщо система контролю транспорту атакуватимуть, це може призвести до небезпечних ситуацій на дорозі;

– заходи захисту – це оцінка ефективності існуючих заходів захисту та їх достатності для запобігання атакам. Вони включають політики безпеки, шифрування, аутентифікацію, моніторинг і т. д.;

– стратегії відновлення, полягають в розробці планів відновлення в разі успішної кібератаки. Як швидко можна відновити систему після порушення безпеки.

Аналіз ризиків кібербезпеки допомагає розуміти потенційні загрози та відповідні заходи, які слід прийняти для захисту “розумних” проектів від кібератак. Це не лише створює більш безпечне середовище для технологій, а й допомагає забезпечити стабільну та безпечну роботу систем у майбутньому.

ІКТ відіграють ключову роль у розвитку “розумних” міст, які об’єднують інфраструктуру, архітектуру, об’єкти та людей для вдосконалення процесів і вирішення соціальних, економічних та екологічних проблем. У розумних містах використовуються такі технології, як хмарні технології, великі дані, штучний інтелект, блокчейн та Інтернет речей. Використання нових технологій сприяє інноваціям у контексті розумних міст, і що це не обмежується технологічною перспективою міст, а дозволяє створити розумне середовище, розумне управління та розумну економіку. З огляду на вищесказане, можна зробити висновок, що не існує розумного міста без технологій та інновацій, оскільки саме ці фактори відрізняють його від звичайного міста. Впровадження нових технологій та високий рівень взаємозв’язку між ними та людиною робить розумні міста вразливими до різних кіберзагроз. Тому захист інфраструктури, систем і даних від зловмисних дій має важливе значення для забезпечення безпеки,

конфіденційності та надійності послуг розумних міст. Відповідно, існує потреба у вивченні та знанні стратегій пом'якшення наслідків, які можуть вирішити ці проблеми.

Важливо підкреслити, що проблеми безпеки і конфіденційності “розумних” міст не є новими і що багато з них вже існують при ізольованому використанні кожної з технологій, але зараз вони набувають більшого впливу у взаємопов'язаному контексті “розумних” міст. Інфраструктура розумного міста складається з тисяч пристроїв і додатків, які покликані поліпшити процеси і принести користь громадянам. Однак використання цих додатків і систем може спричинити низку проблем, пов’язаних з безпекою та конфіденційністю. Вразливості виникають при впровадженні розумних систем на основі штучного інтелекту, оскільки вони не лише збирають різноманітну конфіденційну інформацію від людей та їхніх соціальних кіл, а й контролюють міські об'єкти та впливають на життя громадян.

Безпека розглядається як динамічна, а не застійна концепція, в якій прагнемо запобігти шкоді за допомогою цифрових і фізичних засобів, як прямих, так і непрямих. У розумному місті безпека розглядається як загальний компонент, що охоплює всі особливості міста, але вона також включена в усі аспекти, які його складають. Таким чином, безпека охоплює більше, ніж просто технічні фактори, маючи сильний залежний від людини аспект, включаючи також суб’єктивні фактори, пов’язані зі сприйняттям людей. Отже, передбачається існування об’єктивного і суб’єктивного вимірів безпеки. Роль людської поведінки також широко висвітлюється в цьому дослідженні як окремий вимір.

Кібербезпека відіграє ключову роль у захисті критичної інфраструктури, до якої належать системи та активи, що мають важливе значення для функціонування суспільства та економіки. Ця інфраструктура може включати електромережі, транспортні мережі, водоочисні споруди, системи зв’язку тощо. Захист цих життєво важливих компонентів від

кіберзагроз має вирішальне значення для запобігання збоям, несанкціонованому доступу або саботажу, які можуть вплинути на роботу всього міста. Підхід “приватність за дизайном”, має важливе значення для “розумних” міст, які повинні підтримуватися безпечною архітектурою та дизайном. Тому міркування кібербезпеки повинні бути інтегровані в архітектуру і дизайн систем критичної інфраструктури з самого початку. Це передбачає дотримання найкращих практик безпеки, проведення оцінки ризиків та впровадження відповідних засобів контролю безпеки.

Захист конфіденційності даних є ще однією сферою, що викликає занепокоєння в середовищі “розумних” міст. Розумні міста генерують величезні обсяги даних з датчиків, систем спостереження та підключених пристроїв. Ці дані часто містять конфіденційну інформацію про людей, включаючи їхнє місцезнаходження, поведінку та особисті уподобання. Шифрування даних є фундаментальною технікою, що використовується для захисту даних під час передачі та у стані спокою. У розумних містах конфіденційні дані, такі як особиста інформація, фінансові записи та записи з камер спостереження, повинні бути зашифровані, щоб запобігти несанкціонованому доступу або перехопленню зловмисниками. Важливість мінімізації та анонімізації даних пов’язана з появою шифрування даних. Деякі автори рекомендують розумним містам практикувати мінімізацію даних, збираючи лише необхідні дані для виконання своїх функцій та зменшуючи ризик, пов'язаний зі зберіганням надмірної особистої інформації. Крім того, розумні міста повинні впроваджувати надійний контроль доступу, щоб обмежити доступ до чутливих систем і даних. Це передбачає впровадження безпечних механізмів автентифікації, таких як багатофакторна автентифікація та контроль доступу на основі ролей (RBAC), щоб гарантувати, що лише уповноважені особи можуть отримати доступ до певних даних. Крім того, розумні міста повинні включати в себе механізми безпечного зв’язку. Зв’язок між пристроями і системами в інфраструктурі

розумного міста повинен бути захищеним, щоб запобігти підслуховуванню або втручанню. Прийняття безпечних протоколів, таких як захист транспортного рівня (TLS) і віртуальні приватні мережі (VPN), може забезпечити зашифровані та автентифіковані канали зв’язку. Ці пропозиції відповідають підходу нашого дослідження, яке визначає виклики кібербезпеки, пов'язані з вразливістю мережі, що стосується несанкціонованого доступу та перехоплення комунікацій.

Пристрої Інтернету речей є основою розумних міст, забезпечуючи зв'язок та обмін даними між різними системами та пристроями. Однак ці пристрої часто вразливі до кібератак через обмежені заходи безпеки. Отже, для захисту пристроїв Інтернету речей необхідні надійні методи кібербезпеки, включаючи впровадження безпечної автентифікації, шифрування та регулярне оновлення програмного забезпечення для запобігання несанкціонованому доступу або контролю. У літературі пропонується кілька підходів до підвищення безпеки пристроїв Інтернету речей. Впровадження надійних механізмів автентифікації, таких як багатофакторна автентифікація (MFA), щоб гарантувати, що тільки авторизовані користувачі або пристрої можуть отримати доступ до пристроїв IoT. Це допомагає запобігти несанкціонованому доступу і захищає від атак грубої сили. Впровадження безпечних протоколів зв’язку, таких як Transport Layer Security (TLS) або Secure Shell (SSH), для шифрування даних, що передаються між пристроями IoT та внутрішніми системами. Це запобігає підслуховуванню та фальсифікації конфіденційної інформації. Регулярне оновлення прошивки рекомендують, щоб підтримувати прошивку пристроїв IoT в актуальному стані, застосовуючи регулярні виправлення та оновлення безпеки, що надаються виробниками. Це допомагає усунути вразливості і гарантує, що пристрої захищені від відомих ризиків безпеки. Застосовують підхід з використанням тестових даних з різних наборів даних, щоб запропонувати впровадження сегментації мережі для ізоляції пристроїв IoT

від інших систем критичної інфраструктури. Таким чином, навіть якщо один пристрій буде скомпрометований, він не надасть прямого доступу до всієї мережі, що зменшить потенційний вплив атаки. Наше дослідження підтверджує, що безпека Інтернету речей відіграє вирішальну роль у захисті не тільки пристроїв і систем, підключених до Інтернету, але й усієї цифрової інфраструктури та екосистеми даних.

1.4 Аналіз протоколів безпеки “розумних” інформаційно-технологічних проектів

Стандарти безпеки для “розумних” інформаційно-технологічних проектів грають критичну роль у забезпеченні безпеки цих систем. Такі стандарти встановлюють рекомендації, вимоги та керівні принципи, які допомагають розробникам, виробникам та користувачам забезпечувати високий рівень кібербезпеки. До основних стандартів, що забезпечують кіберзахист “розумних” інформаційно-технологічних проектів можна віднести:

– ISO/IEC 27001 – це один з найвідоміших стандартів у сфері інформаційної безпеки. Він встановлює систему управління інформаційною безпекою та надає рамки для визначення, реалізації, контролю та вдосконалення заходів безпеки даних;

– NIST Cybersecurity Framework – розроблений Національним інститутом стандартів і технологій (NIST) США, цей фреймворк надає напрямок з вдосконалення кібербезпеки для організацій, зокрема для критичних інфраструктур та приватного сектору;

– ENISA (European Union Agency for Cybersecurity) розробляє різноманітні рекомендації та стандарти у сфері кібербезпеки, які сприяють удосконаленню захисту інформаційно-технологічних проектів у Європейському союзі;

– IEC 62443 (Industrial Security) – це стандарт спрямований на кібербезпеку промислових автоматизованих систем (IAS). Він визначає вимоги до кібербезпеки для систем автоматизації, які використовуються в промисловості;

– стандарти конкретних галузей часто застосовуються як специфічні стандарти безпеки для певних секторів, таких як медицина (HIPAA), фінанси (PCI DSS) та інші.

Ці стандарти встановлюють базові вимоги та принципи, які організації можуть використовувати для розробки політик, процедур та технічних заходів забезпечення безпеки для своїх “розумних” проектів. Застосування відповідних стандартів може значно підвищити рівень захищеності цих проектів від кіберзагроз.

1.5 Аналіз тестування безпеки “розумних” інформаційно-технологічних проектів

Тестування безпеки “розумних” інформаційно-технологічних проектів є важливою складовою для виявлення потенційних вразливостей і заходів забезпечення безпеки цих систем. Основними типами тестування безпеки, які часто використовуються є:

– Penetration Testing (Pen Testing). Цей тип тестування полягає в спробі активно проникнути в систему або мережу для виявлення слабких місць. Це може включати спроби зламу або використання вразливостей для отримання несанкціонованого доступу;

– Vulnerability Assessment. Це сканування системи для виявлення вразливостей, які можуть бути використані для атак. Це може включати в себе автоматизовані сканери для перевірки на відомі вразливості;

– Security Audits. Періодичні аудити системи на предмет відповідності стандартам безпеки та політикам організації;

– Security Code Review. Аналіз програмного коду на предмет потенційних вразливостей або неправильного використання безпеки;

– Social Engineering Tests. Це тестування, в якому випробовується людський фактор шляхом спроб отримати доступ до системи за допомогою маніпулювання користувачами;

– IoT Security Testing. Спеціалізовані тести для виявлення вразливостей в пристроях Інтернету речей (IoT), оскільки вони часто стають об’єктом кібератак.

Ці методи тестування допомагають ідентифікувати потенційні слабкі місця в “розумних” проектах та дають змогу розробникам приймати заходи для їх виправлення або підвищення рівня захищеності. Тестування безпеки має бути постійним процесом, оскільки кіберзагрози постійно еволюціонують.

1.6 Висновки до першого розділу

В першому розділі кваліфікаційної роботи здійснено аналіз кіберзахисту “розумних” інформаційно-технологічних проектів, що серед широкого кола завдань виокремило такі, як аналіз загроз, створення заходів захисту, тестування безпеки, дотримання стандартів безпеки, здійснення оновлень. Весь цей процес не є статичним, що потребує постійного моніторингу і прийняття мір. Проведено аналіз кіберзагроз в проектах “розумне” місто, що визначило кібербезпеку як ключовий фактор для його реалізації. Інформаційні системи, цифрові комунікації та навколишнє цифрове середовище є ключовими елементами для успішних процесів прийняття рішень, які мають на меті вироблення обґрунтованих рішень з важливих і чутливих питань. Аналіз ризиків кібербезпеки в “розумних” інформаційно-технологічних проектах включає в себе оцінку потенційних загроз і вразливостей, які можуть вплинути на безпеку цих систем. Стандарти

безпеки для “розумних” інформаційно-технологічних проектів грають критичну роль у забезпеченні безпеки цих систем. Такі стандарти встановлюють рекомендації, вимоги та керівні принципи, які допомагають розробникам, виробникам та користувачам забезпечувати високий рівень кібербезпеки. Подано основні стандарти, що забезпечують кіберзахист “розумних” інформаційно-технологічних проектів. Тестування безпеки “розумних” інформаційно-технологічних проектів є важливою складовою для виявлення потенційних вразливостей і заходів забезпечення безпеки цих систем. Методи тестування допомагають ідентифікувати потенційні слабкі місця в “розумних” проектах та дають змогу розробникам приймати заходи для їх виправлення або підвищення рівня захищеності. Тестування безпеки має бути постійним процесом, оскільки кіберзагрози постійно еволюціонують.

2 ДОСЛІДЖЕННЯ КІБЕРЗАХИСТУ “РОЗУМНИХ” ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНИХ ПРОЕКТІВ

2.1 Вимоги архітектур кіберзахисту “розумних” інформаційно-технологічних проектів

Архітектура кіберзахисту для “розумних” інформаційно-технологічних проектів має за мету створення безпечного середовища для цих систем. До важливих вимог архітектури кіберзахисту потрібно віднести наступні:

– захист даних, що включає в себе шифрування даних, захист від несанкціонованого доступу, контроль доступу до інформації та забезпечення конфіденційності, цілісності та доступності даних;

– мережева безпека, яка вимагає застосування заходів безпеки для мережевої інфраструктури, включаючи захист від DDoS-атак, застосування брандмауерів, моніторинг мережевої активності тощо;

– безпека програмного забезпечення, що досягається через високий рівень безпеки в програмному забезпеченні, потребує проводити аудит коду на вразливості, використовувати патчі безпеки, вдосконалювати системи на вразливість;

– захист від кібератак. Враховуючи різноманітність кіберзагроз, важливо мати заходи для виявлення, відповіді та запобігання кібератакам, таким як системи виявлення вторгнень (IDS/IPS), системи моніторингу безпеки тощо;

– фізична безпека. Захист фізичних компонентів системи, включаючи сервери, датчики, пристрої IoT тощо;

– управління доступом. Визначення рівнів доступу, автентифікація користувачів, керування правами доступу до системи;

– навчання та освіта користувачів. Важливо навчати персонал правилам безпеки, фішингу, парольної гігієни тощо;

– резервне копіювання та відновлення. Регулярне створення резервних копій даних та плани відновлення в разі виникнення проблем.

Ці вимоги утворюють основу для архітектури кіберзахисту “розумних” інформаційно-технологічних проектів, допомагають забезпечити повноцінний та надійний рівень захисту від різноманітних кіберзагроз. Важливо застосовувати ці вимоги від початкової фази проектування та протягом усього життєвого циклу системи для максимальної ефективності та безпеки.

2.2 Дослідження архітектур моделей кіберзахисту “розумних” інформаційно-технологічних проектів

Архітектура кіберзахисту “розумних” інформаційно-технологічних проектів може бути побудована на різних моделях та концепціях. Наведемо декілька основних моделей:

– модель “Захист у глибину” (Defense in Depth). Ця модель передбачає застосування різноманітних заходів безпеки на кожному рівні системи. Вона базується на ідеї, що кожен рівень має свої заходи захисту, починаючи від фізичної безпеки і закінчуючи захистом даних та програмного забезпечення;

– модель “Zero Trust”. Ця концепція базується на ідеї, що жоден елемент мережі або користувач не може бути довіреним наперед. У цій моделі кожен запит на доступ до ресурсів перевіряється та автентифікується перед наданням доступу;

– модель “Assume Breach” (Припускати Порушення). Ця модель передбачає те, що організація завжди вважає, що її системи вже були

скомпрометовані. Такий підхід спрямований на те, щоб підготуватися до виявлення та відповіді на можливі порушення;

– модель “DevSecOps”. Ця модель вбудовує безпеку в процес розробки програмного забезпечення (DevOps). Забезпечення безпеки входить у всі етапи розробки, від початкового проектування до впровадження та підтримки;

– Модель “Бізнес-орієнтованої безпеки”. Ця модель фокусується на ризиках та загрозах, які найбільш критичні для бізнесу. Вона орієнтована на забезпечення безпеки з урахуванням впливу на бізнес-процеси та стратегічні цілі організації.

Наведені моделі можуть використовуватися окремо або комбінуватися в залежності від потреб, ризиків та характеристик конкретного “розумного” проекту. Кожна з них має свої переваги та може бути використана для створення ефективної архітектури кіберзахисту.

Модель “Захист у глибину” є цілком відповідною для “розумних” інформаційно-технологічних проектів через їх складність та потенційність для різноманітних кіберзагроз. Вона передбачає використання кількох заходів безпеки на кожному рівні системи, щоб створити мережу захисту, що має більш високий ступінь надійності та ефективності.

До цієї моделі входять наступні елементи:

– фізичний рівень, де відбувається захист фізичних пристроїв, серверів, датчиків IoT. Це може включати заходи фізичної безпеки, контроль доступу до обладнання тощо;

– мережевий рівень, де відбувається встановлення брандмауерів, сегментація мережі, моніторинг мережевої активності, застосування шифрування для захисту передачі даних;

– рівень застосунків та даних, що надає захист програмного забезпечення за допомогою регулярних аудитів на вразливості, шифрування даних, вдосконалення політики безпеки;

– ідентифікація та автентифікація, що відбуваєиться через використання багаторівневої аутентифікації, управління ідентифікацією та контроль доступу;

– моніторинг та реагування, за допомогою встановлення систем моніторингу безпеки для виявлення аномалій, реагування на потенційні загрози, інцидентний реагування та відновлення після атаки;

На рисунку 2.1 подано архітектуру моделі “Захист у глибину” для “розумних” проектів.

Рисунок 2.1 - Архітектура моделі “Захист у глибину” для “розумних” проектів

Застосування моделі “Захист у глибину” для “розумних” проектів допоможе створити комплексну систему захисту, яка працює на кількох рівнях і зменшує можливість кіберзагроз, забезпечуючи більш високий рівень безпеки для цих технологічних проектів.

Модель “Zero Trust” є дуже цікавим підходом до кібербезпеки, особливо в контексті “розумних” інформаційно-технологічних проектів, де

складність і потенційні загрози можуть бути значними. Ця модель базується на принципі, що ніхто та ніщо не повинні автоматично довіряти в мережі, навіть якщо це внутрішня частина мережі або користувач. На рисунку 2.2 подано елементи цієї моделі.

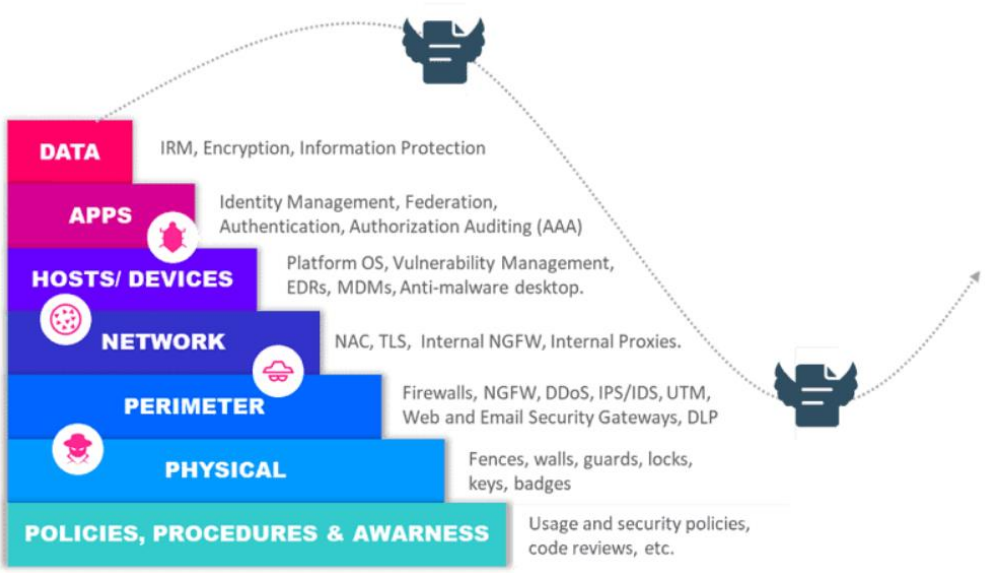

Рисунок 2.2 – Архітектура моделі “Zero Trust”

Основні аспекти моделі “Zero Trust” для “розумних” проектів включають:

– мікросегментація мережі. Розділення мережі на дрібні сегменти з обмеженим доступом. Це дає змогу контролювати та обмежувати доступ до різних частин мережі;

– строга автентифікація. Вимагати багаторівневу аутентифікацію для доступу до систем та ресурсів;

– неперервна авторизація. Контроль доступу на основі контексту та стану користувача або пристрою, забезпечуючи постійну перевірку доступу;

– обмеження привілеїв. Використання принципу найменших привілеїв, коли користувачам надаються тільки необхідні права для виконання їх робочих обов’язків;

– моніторинг та аналіз активності. Постійний моніторинг мережевої активності та аналіз подій для виявлення аномальної поведінки та потенційних загроз;

– шифрування даних. Використання шифрування для захисту конфіденційності даних під час передачі та зберігання.

Значна частина витоків даних, а саме 34% за даними Verizon, відбувається через внутрішніх користувачів мережі (незадоволені співробітники, недбалість, людські помилки, колишні співробітники, які викрадають конфіденційні дані тощо).

Якщо говорити про зовнішніх зловмисників, то вони проникають в мережу і докладають усіх зусиль, щоб залишитися непоміченими. Вони часто обирають конкретні компанії та цілі і не поспішають отримати доступ до бажаного (інтелектуальна власність, фінансова інформація, особиста інформація тощо) або просто, як програми-вимагачі, шифрують інформацію, а потім вимагають викуп.

Значна частина інформації повинна бути доступною для зовнішніх користувачів. Інформація зберігається не тільки в мережі, але й за її межами, на різних платформах і в хмарних додатках. Існує потреба дозволити доступ до інформації внутрішнім користувачам не тільки з мережі, але й ззовні, навіть з їхніх особистих пристроїв.

Ці принципи можуть бути впроваджені для “розумних” проектів з урахуванням їх особливостей та потреб. Модель “Zero Trust” може забезпечити більш високий рівень безпеки, оскільки вона активно контролює доступ до ресурсів та систем, навіть у внутрішній мережі, що може значно знизити ризик від різноманітних кіберзагроз.

Модель “Assume Breach” є цікавим підходом до кібербезпеки, особливо у випадку “розумних” інформаційно-технологічних проектів, оскільки вона ґрунтується на припущенні, що система вже була скомпрометована або може бути скомпрометована.

На рисунку 2.3 показано архітектуру моделі “Assume Breach” для “розумних” інформаційно-технологічних проектів на базі рішень від Microsoft.

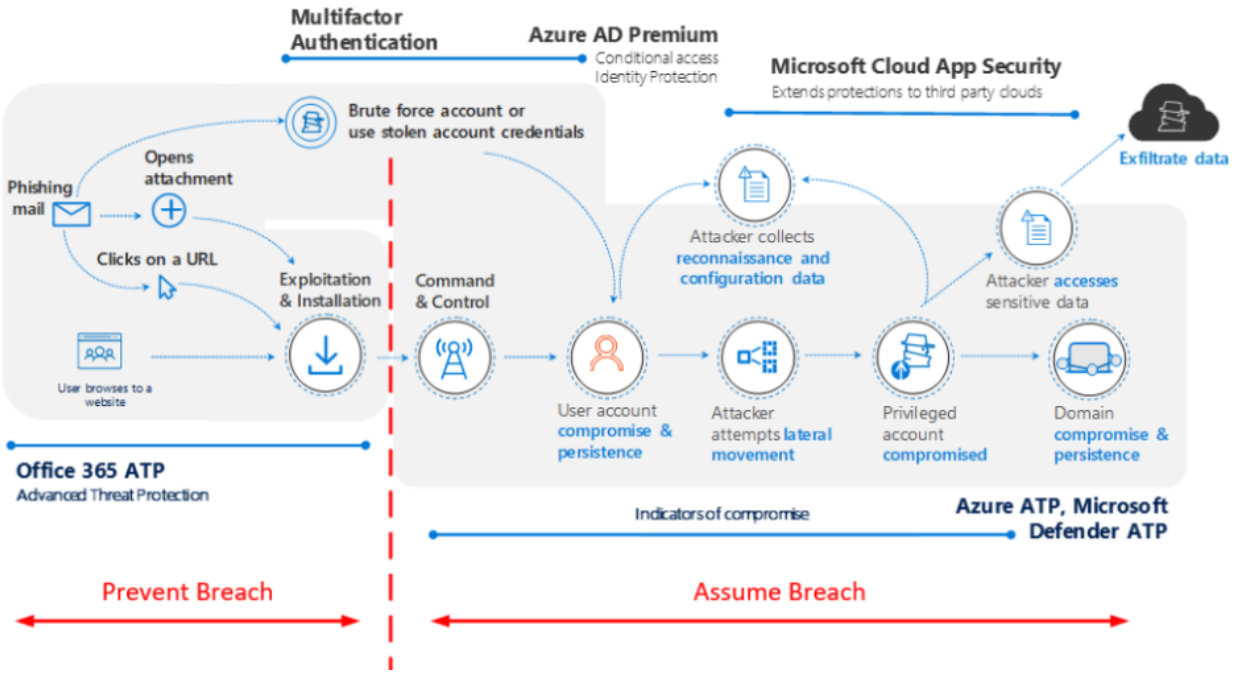

Рисунок 2.3 – Архітектура моделі “Assume Breach” для “розумних” інформаційно-технологічних проектів

Ключові аспекти моделі “Assume Breach” для “розумних” проектів включають:

– фокус на виявленні та реагуванні. Ця модель покладає великий акцент на виявленні аномальних активностей та швидкій реакції на потенційні загрози. Це може включати постійний моніторинг та аналіз подій для виявлення незвичних паттернів;

– запобігання поширенню. Важливо мати заходи для обмеження поширення атак всередині мережі. Сегментація мережі та застосування принципу “мінімальних прав доступу” можуть допомогти у зменшенні поширення потенційних загроз;

– постійне вдосконалення. Підходить концепція постійного вдосконалення системи захисту, оскільки кіберзагрози постійно змінюються.

Регулярні аудити, вдосконалення процедур виявлення та реагування – це ключові складові моделі;

– плани відновлення та інцидентного реагування. Готовність до негативних ситуацій через розробку планів відновлення після атаки або компрометації системи;

Ця модель не передбачає повної недовіри до всіх елементів мережі, але ставить у центр уваги підготовку до виявлення та реагування на можливі компрометації. Це дозволяє швидко реагувати та мінімізувати наслідки потенційних атак чи порушень безпеки для “розумних” інформаційно-технологічних проектів.

Модель “DevSecOps” – це підхід до розробки програмного забезпечення, який вбудовує кібербезпеку (Security - Sec) у культуру та процеси DevOps (Development and Operations). Для “розумних” інформаційно-технологічних проектів цей підхід може бути особливо корисним, оскільки вони зазвичай швидко розвиваються та потребують постійних оновлень та інновацій. На рисунку 2.4 показано архітектуру моделі “DevSecOps”.

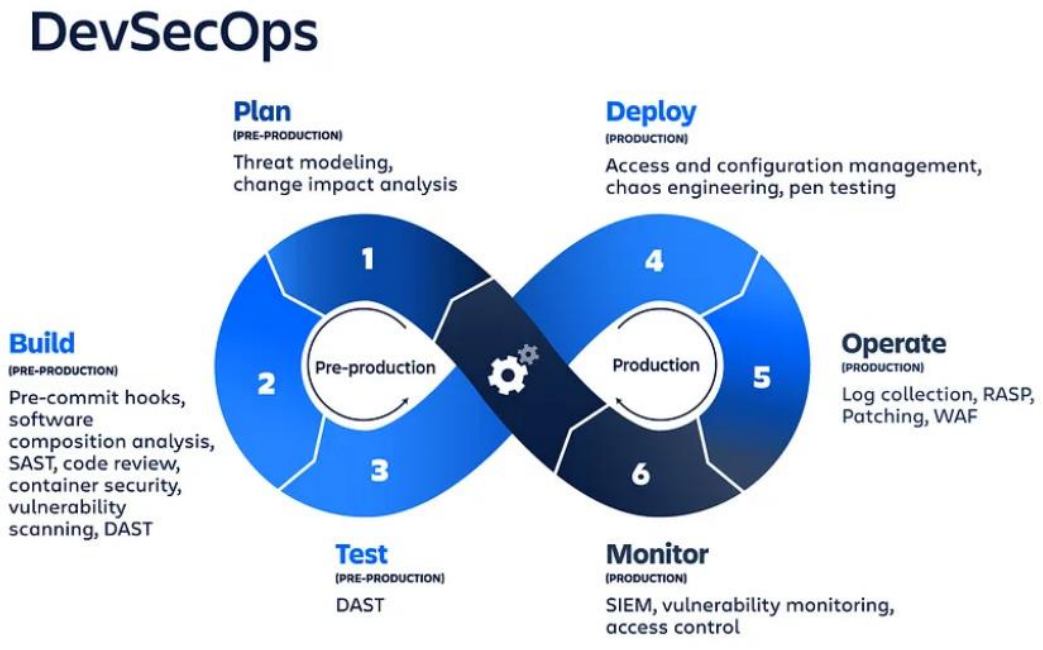

Рисунок 2.4 – Архітектура моделі “DevSecOps”

Основні аспекти моделі “DevSecOps” для “розумних” проектів включають:

– інтеграція безпеки з самого початку. Вбудовування кібербезпеки в кожен етап циклу розробки – від планування до впровадження та моніторингу;

– автоматизація тестування безпеки. Використання автоматизованих інструментів для виявлення потенційних вразливостей під час розробки, що дозволяє виправляти їх на ранніх етапах;

– культура безпеки. Підвищення обізнаності та відповідальності усіх членів команди щодо кібербезпеки, створення безпечних стандартів розробки;

– швидка реакція та вдосконалення. Швидке виявлення, відповідь та виправлення вразливостей під час розробки та експлуатації;

– застосування інструментів для безпеки. Використання спеціалізованих інструментів для контролю за безпекою, моніторингу та виявлення вразливостей.

Автоматизація є наріжним каменем успішного DevSecOps. Автоматизація рутинних завдань і процесів допомагає прискорити процес доставки, дозволяючи командам зосередитися на більш складних аспектах життєвого циклу розробки.

Зсув безпеки вліво – це процес інтеграції практик безпеки на більш ранніх стадіях процесу розробки. Це допомагає зменшити ризики, пов’язані з виробничим середовищем.

Безперервна інтеграція (CI) і безперервна доставка (CD) важливі для DevSecOps. CI та CD гарантують, що код тестується, переглядається та розгортається швидко та послідовно.

Співпраця та комунікація є ключем до успішного DevSecOps. Командам важливо мати можливість ділитися ідеями, обговорювати проблеми та працювати разом, щоб забезпечити належну реалізацію безпеки.

Вимірювання та моніторинг мають важливе значення для DevSecOps. Команди повинні вимірювати і контролювати свої системи, процеси і продуктивність, щоб виявляти потенційні проблеми з безпекою і швидко їх вирішувати.

DevSecOps надає організаціям більш безпечний процес розробки програмного забезпечення шляхом включення безпеки на кожному етапі процесу розробки. Це гарантує, що будь-які проблеми з безпекою виявляються та вирішуються набагато раніше в циклі розробки, зменшуючи ймовірність дорогих інцидентів безпеки.

DevSecOps дає змогу організаціям оптимізувати процеси розробки, автоматизуючи завдання та усуваючи ручні дії, що призводить до швидшої та надійнішої доставки програмного забезпечення.

DevSecOps заохочує співпрацю між командами розробників і службами безпеки, дозволяючи розробникам і фахівцям з безпеки працювати разом над виявленням і вирішенням проблем безпеки. Це призводить до покращення комунікації та співпраці, що робить процес розробки більш безпечним.

DevSecOps полегшує відстеження та моніторинг проблем безпеки протягом усього процесу розробки програмного забезпечення. Це забезпечує організаціям більшу видимість безпеки їхніх додатків і допомагає їм виявляти потенційні ризики набагато раніше в циклі розробки.

Модель “DevSecOps” спрямована на інтеграцію кібербезпеки в усі аспекти розробки, дозволяючи забезпечити більш високий рівень захищеності для “розумних” інформаційно-технологічних проектів. Це дає змогу підтримувати безпеку на високому рівні під час швидкої розробки та постійних змін у таких проектах.

Модель “Бізнес-орієнтованої безпеки” фокусується на тому, як кібербезпека може підтримувати стратегічні цілі та бізнес-процеси організації. Для “розумних” інформаційно-технологічних проектів ця модель

особливо важлива, оскільки вони часто пов’язані з різними аспектами бізнесу та мають стратегічне значення для компанії.

Ключові аспекти моделі “Бізнес-орієнтованої безпеки” для “розумних” проектів включають:

– розуміння бізнес-процесів. Глибоке розуміння та ідентифікація критичних бізнес-процесів, що дає змогу зорієнтувати кібербезпеку на їх захист;

– оцінка ризиків з точки зору бізнесу. Врахування ризиків для бізнесу при оцінці та прийнятті рішень щодо кібербезпеки;

– забезпечення відповідності до стандартів та регулятивних вимог. Спрямування зусиль на відповідність з правовими нормами, стандартами та регулятивами у сфері кібербезпеки;

– забезпечення бізнес-континуітету. Розробка планів відновлення, які дозволяють бізнесу продовжувати роботу після кібератаки або подібних інцидентів;

– підтримка стратегічних цілей. Вирішення кібербезпеки таким чином, щоб сприяти досягненню стратегічних цілей та успіху проектів.

Ця модель дає змогу зв’язати кібербезпеку з важливими аспектами бізнесу, забезпечуючи вирішення кібербезпеки таким чином, щоб воно підтримувало ключові цілі організації та бізнес-процеси. Вона допомагає визначити пріоритети та напрямки дій у сфері кібербезпеки, що найбільш ефективно впливатимуть на успіх “розумних” інформаційно-технологічних проектів з погляду бізнесу.

2.3 Дослідження кіберзахисту “розумних” інформаційно-технологічних проектів в контексті Індустрії 4.0

Згідно зі спеціальною публікацією NIST 1500-201 “Концепція кіберфізичних систем: Том 1”, “кіберфізичні системи – це інтелектуальні

системи, які включають інженерні взаємодіючі мережі фізичних і обчислювальних компонентів”. Ці системи тісно взаємопов’язані та інтегровані, надають нові функціональні можливості для підвищення якості життя і сприяють технологічному прогресу в таких важливих сферах, як персоналізована охорона здоров’я, реагування на надзвичайні ситуації, управління транспортними потоками, інтелектуальне виробництво, оборона і національна безпека, а також постачання і використання енергії. CPS мають великий потенціал для створення інноваційних застосувань і впливу на різні сектори світової економіки.

CPS зазвичай поєднують датчики і сенсорні мережі з вбудованими обчислювальними засобами для моніторингу і контролю фізичного середовища, з петлями зворотного зв’язку, які дозволяють зовнішнім стимулам активувати систему за допомогою зв'язку, управління або обчислень. З точки зору промислового виробництва, CPS – це фізичний об’єкт, підключений до Інтернету, наприклад, насос або компресор, з вбудованими комп’ютерами і компонентами управління, що складаються з датчиків і виконавчих механізмів.

IoT – це мережа пристроїв, які містять апаратне, програмне, мікропрограмне забезпечення та виконавчі механізми, що дозволяють пристроям з’єднуватися, взаємодіяти і вільно обмінюватися даними та інформацією. IoT – це підключення “речей”, таких як об’єкти і машини, до інтернету і, в кінцевому підсумку, один до одного.

У той час як IoT збирає дані з фізичних об’єктів, таких як датчики, великі дані дозволяють більш ефективно і раціонально обробляти і зберігати ці дані. Поєднання IoT та великих даних робить збір та аналіз даних доступними для покращення виробництва.

Використання як внутрішніх, так і зовнішніх хмарних додатків на виробництві може перетворити ресурси та можливості на послуги. Цими послугами можна керувати та експлуатувати в уніфікований спосіб,

забезпечуючи спільне використання та циркуляцію ресурсів і можливостей. Хмарне виробництво (CMfg) може забезпечити безпечні та надійні, високоякісні, недорогі виробничі послуги на вимогу протягом усього життєвого циклу виробництва.

CMfg – це тип паралельної, мережевої та розподіленої системи, що складається з інтегрованого та взаємопов'язаного віртуалізованого пулу послуг, відомого як "виробнича хмара", виробничих ресурсів та можливостей. Це також включає в себе можливості інтелектуального управління та використання послуг на вимогу для надання рішень для всіх типів користувачів, залучених до виробництва продукту.

Всі системи, які збирають і передають дані, існують для того, щоб зробити промисловість і виробництво більш ефективними та автономними. Це фундаментальна частина Індустрії 4.0.

Технології слугують для об'єднання раніше розрізнених систем за допомогою апаратного та програмного забезпечення, забезпечують прозорість інформації, розширюють можливості людини у прийнятті рішень, дозволяють приймати рішення в режимі реального часу та децентралізують рішення всередині технологічних систем, що зменшує частоту людського втручання.

Усі чотири складові Індустрії 4.0 залежать від взаємозв'язку між:

- машинами та системами управління виробництвом;
- інформацією у виробничих процесах;
- інформацією протягом усього життєвого циклу виробництва.

Взаємозв'язки залежать від комунікації між машинами, датчиками та людьми. Комунікації повинні бути захищені і є життєво важливими для успішного впровадження Індустрії 4.0.

В Індустрії 4.0 комунікації та кібербезпека не можуть розглядатися як ізольовані процеси. Щоб повною мірою скористатися можливостями, які

пропонує Індустрія 4.0, виробники будь-якого розміру повинні розуміти її можливості та потенційні ризики.

Розглянемо приклад впровадження Індустрії 4.0 для середнього виробника.

Компанія AthCo є виробником спортивного одягу і нещодавно досягла стрімкого зростання після запуску нової колекції одягу для активного відпочинку. Наразі AthCo використовує систему планування ресурсів підприємства (ERP) та систему управління взаємовідносинами з клієнтами (CRM). З ERP, CRM та "бек-офісу" генерується велика кількість даних, включаючи інформацію про транзакції. Ці дані дають змогу AthCo спілкуватися як всередині компанії, так і з клієнтами, постачальниками та діловими партнерами. Навіть маючи всі ці дані, AthCo намагається передбачити результати на фабриці. На перший погляд здається, що фабрика працює добре, але є деякі виробничі проблеми, які стали очевидними. Швейні машини часто припиняють роботу без попередження або майже без нього, системи контролю видають помилки під час виробництва, а неточні виробничі витрати випливають з даних, зібраних у кількох системах. Бізнес є складним, і помилки при зборі даних часто виникають через те, що різні системи вимірюють різні речі по-різному.

Підхід Індустрії 4.0 допоможе AthCo досягти більшої продуктивності та усунути проблеми з відмовами машин і систем управління. Додавши датчики на заводі, AthCo може:

- моніторинг виробничого потоку в режимі реального часу;
- зменшити відходи та переробку продукції;
- контролювати виробництво запасів.

Дані, зібрані датчиками, можуть надсилатися в хмару для аналізу, допомагаючи створювати прогнозні моделі і розробляти попередження про технічне обслуговування на основі стану.

Інженери заводу можуть скоротити час простою обладнання і збільшити обсяг виробництва за рахунок точного прогнозування відмов обладнання. Менеджери заводу можуть віддалено контролювати і керувати виробничими процесами. Змінні, такі як температура, можна контролювати для економії енергії та зменшення накладних витрат. Операційні менеджери можуть використовувати дані з датчиків для перегляду стану виробничої лінії і внесення необхідних коректив для управління витратами. Відділ досліджень і розробок може отримати уявлення про закономірності від декількох клієнтів, відстежувати збої в роботі обладнання і реінжинірингувати проблеми для поліпшення продуктивності заводу. Менеджери з обслуговування на місцях можуть визначити, коли задіяти ресурси для профілактичного обслуговування, що дозволить мінімізувати відмову обладнання та витрати на його обслуговування.

Індустрія 4.0 забезпечить краще використання даних у всіх відділах AthCo. Дані будуть представлені у зручному для сприйняття форматі, надаватимуть дієву інформацію та сприятимуть модернізації бізнесу. Це дозволить покращити комунікацію як між внутрішніми відділами, так і з клієнтами та постачальниками.

Хоча впровадження Індустрії 4.0, як видається, вирішує багато виробничих проблем AthCo, можуть з’явитися нові проблеми з кібербезпекою. Використання датчиків і віддаленого доступу може надати хакерам, кіберзлочинцям або конкурентам в галузі можливість отримати доступ до систем AthCo. Перш ніж впроваджувати нові технології, слід провести оцінку кіберризиків, щоб забезпечити повне розуміння потреб і можливостей компанії у сфері кібербезпеки. Керівництво компанії повинно розуміти переваги та потенційні ризики для кібербезпеки, які може спричинити впровадження Індустрії 4.0.

На рисунку 2.5 показано області де можуть виникнути проблеми на “розумному виробництві”.

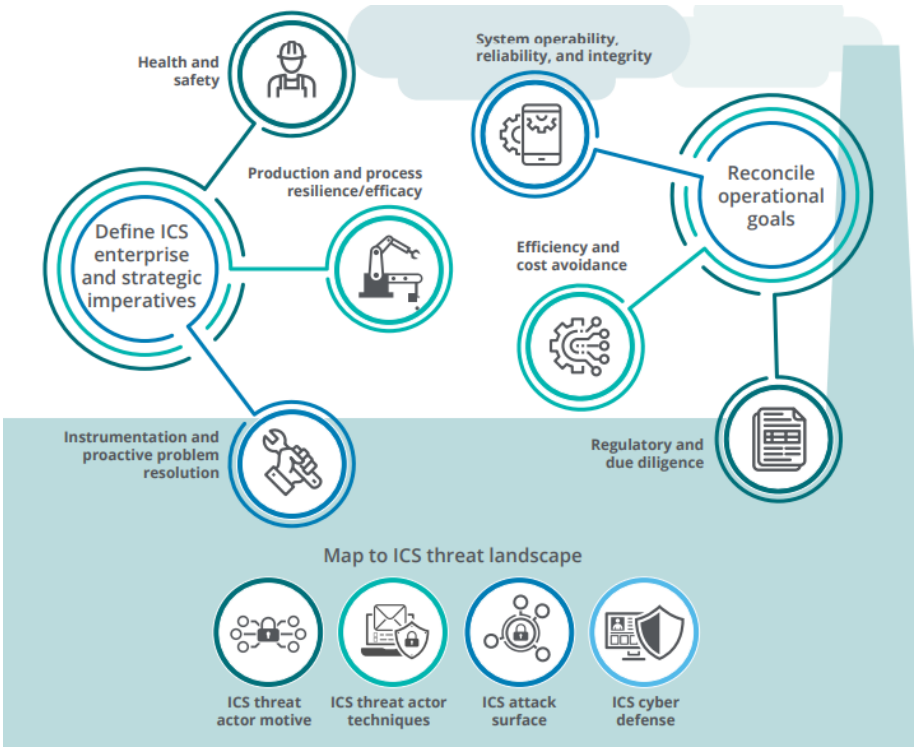

Рисунок 2.5 – Можливі області виникнення загроз при “розумному” виробництві

Безпека як для працівників, так і для навколишнього середовища, як правило, має першорядне значення на кожному об’єкті. З розвитком технологій інтелектуальне обладнання для забезпечення безпеки може бути модернізоване в до майбутніх умов.

Часто дуже важливо забезпечити безперервне виробництва в будь-який час. На практиці, будь-який простій виробництва відображає втрату грошей, але відновлення критично важливих процесів може призвести до ще більших втрат, враховуючи час, необхідний для відновлення та перезапуску.

Інструментарій та проактивна проблема вирішення проблем, корпоративний бренд і репутація відіграють все більшу роль на глобальному бізнес-ринку ринку. На практиці, несправності на виробничих майданчиках можуть мати вирішальне значення для репутації і на зміни в навколишньому середовищі слід реагувати, щоб захистити бренд і репутацію організації.

Організації повинні реагувати на різні операційні цінності у своїй повсякденній діяльності – працездатність, надійність і цілісність систем має

вирішальне значення. Щоб зменшити вартість володіння та полегшити заміну компонентів, компанії можуть інвестувати в інтероперабельні системи, які підтримують використання різних постачальників і версій програмного забезпечення.

У міру того, як промисловість продовжує впроваджувати Індустрію 4.0, вона стає все більш привабливою мішенню для зловмисників, які мають можливість переміщатися по виробничій мережі, перестрибуючи через IT- та OT-системи для здійснення своєї зловмисної діяльності. Без надійного захисту зловмисники можуть скористатися системами для промислового шпигунства, крадіжки інтелектуальної власності, витоку інформації або навіть саботажу виробництва.

Виробництво є другою за кількістю атак галуззю, проте виробничий сектор відстає, коли мова заходить про безпеку.

Розумні заводи можуть піддаватися тим же вразливостям, шкідливому програмному забезпеченню, відмові в обслуговуванні (DoS), злому пристроїв та іншим поширеним методам атак, з якими стикаються інші мережі. А розширена поверхня атак на “розумні” фабрики ускладнює для виробників виявлення та захист від кібератак. З появою Інтернету речей ці загрози виходять на абсолютно новий рівень і можуть призвести до серйозних фізичних наслідків, особливо в сфері IIoT.

Наведемо кілька нових викликів безпеці, з якими стикаються організації в епоху Індустрії 4.0:

– кожен підключений пристрій являє собою потенційний ризик;

– виробничі системи, такі як промислові системи управління (ПСУ), мають унікальні вразливості, які роблять їх особливо вразливими до кібератак;

– Індустрія 4.0 об’єднує раніше ізольовані системи, що збільшує поверхню атаки;

– оновлення часто встановлюються по частинах, оскільки системи дуже складні;

– виробництво має набагато менше регульованих стандартів відповідності, ніж інші сектори;

– окремі системи та ізольовані середовища погано проглядаються.

У той час як організації повинні захищати широку смугу технологій на дуже великій поверхні атаки, зловмисникам потрібно лише визначити найслабшу ланку.

2.4 Дослідження кіберфізичних атак на “розумні” проекти

Оскільки кількість інтелектуальних виробничих пристроїв, які використовуються в промисловості, значно менша, ніж кількість звичайних виробничих пристроїв, кількість зареєстрованих і задокументованих атак на ці системи є відносно низькою. Те ж саме стосується порівняння типових розмірів мережевих систем OT та IT-мережевих систем, де кількість розгорнутих IT-мережевих систем на порядки перевищує кількість розгорнутих мережевих систем OT. Однак є кілька відомих задокументованих випадків кібер-фізичних атак.

У серпні 2005 року 13 заводів з виробництва автомобілів Daimler Chrysler (серед понад 170 інших великих корпорацій) були атаковані хробаком під назвою Zotob. Хробак спричинив тимчасову (від 5 до 50 хвилин) зупинку всієї виробничої лінії на кожному з цих заводів, що зачепило понад 50 000 виробничого персоналу і призвело до фінансових збитків у розмірі тисяч доларів США, окрім фінансових збитків, спричинених втратою людино-годин більш ніж 50 000 персоналу.

Хробак Zotob почав діяти невдовзі після того, як компанія Microsoft оголосила про вразливість в операційній системі Windows 2000. Протягом декількох днів після оголошення про вразливість, код хробака Zotob вже був

розроблений і розповсюджений в комп'ютерних мережах декількох установ до того, як співробітники служби IT-безпеки змогли застосувати необхідний патч безпеки. Зокрема, хробак Zotob використовував уразливість Microsoft Windows Plug and Play Buffer Overrun Vulnerability на TCP-порті 445, яка відкривала чорний хід до операційної системи (ОС), що дозволяло хакеру виконувати зловмисні дії з повними правами та привілеями користувача. Вразливість також давала можливість хакерам встановлювати шкідливе програмне забезпечення в операційну систему. Звідти черв'як може холодно реплікуватися і просуватися далі в комп'ютерну мережу, і таким чином вражати будь-які системи, підключені до виробничої мережі. Саме це сталося під час атаки на заводи Daimler Chrysler.

Хробак Zotob вдало проілюстрував, як швидко хакерська спільнота "чорних капелюшників" може відреагувати на повідомлення про вразливість системи безпеки, перш ніж фахівці з кібербезпеки встигнуть вжити превентивних заходів у певній галузі.

Хробак Stuxnet, розроблений у 2010 році, мав репутацію одного з найбільш загрозливих і складних комп'ютерних черв'яків, коли-небудь створених на момент його появи. Написаний в першу чергу для промислових систем управління, хробак поширювався через комп'ютерну мережу і розмножувався непомітно, щоб перепрограмувати Programmable logic controller (PLC) та інші подібні пристрої промислових систем управління. Шкідливі інструкції, складені хакером, могли потім виконуватися на заражених системах, в той час як зміни в програмуванні обладнання були приховані, щоб уникнути їх виявлення персоналом, який експлуатує або обслуговує обладнання. Компанія Symantec вважає Stuxnet однією з найскладніших загроз безпеці, які коли-небудь аналізувалися, і боротьба з нею вимагала значних зусиль великої кількості аналітиків з безпеки.

Використовуючи величезну кількість компонентів для максимізації можливих векторів атаки, включаючи, серед іншого, численні вразливості

“нульового дня”, методи обходу антивірусів, ін’єкцію процесів і пірингові оновлення, хробаку Stuxnet вдалося заразити тисячі комп’ютерів по всьому світу, щоб максимізувати шанси в кінцевому підсумку проникнути в мережі систем управління з “повітряними проміжками”. Це стало можливим, зокрема, завдяки його здатності ховатися на знімних дисках. Використовуючи вразливість у способі обробки ярликів і .lnk-файлів на комп’ютері (ідентифікована Microsoft як MS10-046), хробак міг самостійно розмножуватися і поширюватися всередині комп’ютера і на зовнішні пристрої. Оскільки багато промислових систем управління не були розроблені з урахуванням вимог безпеки, той факт, що не виконувалася перевірка цілісності повідомлень, отриманих цими системами, зіграв ключову роль у здатності хробака заражати системи непомітно для них. Після того, як він проявив себе на інфікованих машинах, хробак регулярно надсилав зашифровані оновлення на командно-контрольні сервери Stuxnet з ідентифікаційною інформацією про інфіковані системи, такою як IP-адреси, операційні системи та імена комп’ютерів.

Перший варіант хробака Stuxnet з’явився в червні 2009 року. Цей варіант не використовував жодних підписаних файлів драйверів, але в січні 2010 року було виявлено, що черв’як Stuxnet використовує драйвер, який був підписаний скомпрометованим сертифікатом корпорації Realtek Semiconductor. У березні 2010 року було виявлено, що черв’як Stuxnet використовує вразливість, яка була ідентифікована як MS10-046 компанією Microsoft лише в серпні 2010 року.

На той час, коли компанія Symantec опублікувала всебічний аналіз Stuxnet, було інфіковано приблизно 100 000 хостів у більш ніж 25 країнах, причому швидкість інфікування сягала 6000 хостів на день.

Після того, як Stuxnet проклав шлях для розробки надзвичайно складних і потужних кібератак, дві нові загрози, дуже схожі на Stuxnet, з’явилися менш ніж через рік після того, як черв’як Stuxnet став вірусним.

Загроза Duqu, хоч і дуже схожа на кодову базу Stuxnet, була розроблена в першу чергу для викрадення інформації з промислових підприємств, щоб полегшити розробку більш специфічних і цілеспрямованих атак на інших третіх осіб. Складаючись переважно з файлу драйвера, бібліотеки динамічних посилань (DLL) та конфігураційного файлу, які встановлювалися виконуваним файлом через документ Microsoft Word, що містив експлойт ядра нульового дня, ця загроза шукала детальну інформацію про дизайн (серед іншої інформації, що є власністю компанії) та використовувала протоколи HTTP і HTTPS для завантаження та вивантаження інформації між зараженими пристроями та серверами управління та контролю. Один з варіантів загрози мав особливо новий спосіб приховування DLL, що містить основні функції загрози. Ця DLL була прихована у вигляді зашифрованих даних, що містилися у файлі JPEG, який містив зображення, зроблене космічним телескопом Хаббл. Ще однією новою особливістю загрози Duqu в цілому було те, що вона видаляла себе з зараженого пристрою приблизно через 30 днів, що зводило до мінімуму можливість її виявлення.

Перша атака вірусу Duqu була зафіксована на початку квітня 2011 року, а додаткові його різновиди з’явилися в жовтні 2011 року. На той час, коли в листопаді 2011 року компанія Symantec опублікувала всебічний аналіз загрози Duqu, більше восьми країн стали жертвами 15 варіантів цієї загрози.

Подібно до загрози Duqu, загроза Flamer також має глибоке коріння в кодовій базі Stuxnet і існує з 2010 року. На момент виявлення та аналізу компанія Symantec вважала загрозу Flamer найскладнішим шкідливим програмним забезпеченням, яке коли-небудь було написано, і очікується, що вона збереже цю репутацію на довгі роки. Її розмір перевищує 20 мегабайт, а архітектура програмного забезпечення не поступається професійно розробленому програмному забезпеченню. Мета загрози Flamer була схожа на мету загрози Duqu, тобто промислове шпигунство, але в набагато більших масштабах.

Кібератака на українську енергосистему в грудні 2015 року стала першим задокументованим випадком кібер-фізичної атаки на енергосистему. Черв'як BlackEnergy3, імовірно розроблений російською групою кібершпигунів Sandworm, діяв як троянський кінь, що містив можливості розподіленої відмови в обслуговуванні (DDoS). Хробак вперше з'явився у 2007 році (під назвою BlackEnergy), а у 2010 році його було модернізовано з додаванням більш досконалих функцій (під назвою BlackEnergy2). Нарешті, навесні 2015 року, після виходу версії BlackEnergy3, почалися атаки на енергорозподільні компанії за допомогою шкідливих електронних листів. Коли в грудні 2015 року зловмисники проникли в мережу систем управління розподільчого центру "Прикарпаттяобленерго", вони вивели з ладу всю станцію, скомандувавши всім автоматичним вимикачам відкритися, залишивши понад 200 000 людей без електрики. Цей інцидент був особливо катастрофічним, оскільки люди, що залишилися без електрики, не могли користуватися системами опалення посеред зими. Хоча електропостачання було відключено лише приблизно на шість годин, технічні працівники станції все одно намагалися повністю відновити електропостачання в усіх постраждалих регіонах.

У випадку кібератаки на українську електромережу зловмисник поширювався за допомогою шкідливого програмного забезпечення за допомогою класичних методів розповсюдження кібератак, таких як інфіковані електронні листи та скомпрометовані мережі. DDoS-атаки перешкоджали належному функціонуванню та відновленню інфікованих промислових систем, а хробак заважав технічному персоналу станції отримати доступ до системи управління, виводячи їх з облікових записів користувачів та змінюючи їхні паролі.

Термін "атака нульового дня" означає кібер-фізичну атаку, яка використовує вразливість системи безпеки, яка ще не була оприлюднена публічно. Оскільки така вразливість не була розкрита публічно, існує висока

ймовірність того, що знання про неї є лише у декількох обраних осіб, яким якимось чином вдалося знайти таку вразливість. Хоча це може означати, що ймовірність негайної серйозної загрози не така висока, не менш висока ймовірність того, що суб'єкти кібербезпеки також не знають про вразливість. Це означає, що до тих пір, поки така вразливість не буде публічно розкрита (якщо тільки вона не буде розкрита приватно через конфіденційні канали), шанси на розробку патчу безпеки, який би її усунув, практично нульові. Історичні випадки показують, що користувачі комерційно популярного програмного забезпечення, такого як Adobe Reader, WinRAR і Microsoft Word, особливо вразливі до атак "нульового дня", не маючи навіть найменшого уявлення про те, що вони можуть легко стати жертвами загрози. Як наслідок, до моменту розкриття атаки може бути вже занадто пізно виправляти будь-які шкідливі дії, виконані за допомогою такої атаки.

Наслідки такої атаки в промислових масштабах можуть бути катастрофічними для такої галузі, особливо якщо вона стосується виробничої лінії, яка була скомпрометована, а шкідливе програмне забезпечення чинить опір будь-яким спробам встановити патч безпеки, який би його відключив.

Зловмисники можуть отримати конфіденційну та секретну інформацію, підслуховуючи канали зв'язку, які, як відомо, використовуються окремими особами або установами для передачі такої інформації. Підслуховування може мати різні форми, наприклад, прослуховування телефонних ліній, фішинг та моніторинг мережевого трафіку. Якщо будь-яка інформація, що містить конфіденційні дані про функціонування певної системи або виробничого процесу, передається незахищеним каналом зв'язку, зловмиснику може бути дуже корисно підслуховувати такі комунікації, щоб заздалегідь спланувати атаку.

Мабуть, один з найпоширеніших типів атак, атаки на відмову в обслуговуванні (DoS), спеціально спрямовані на виведення систем з ладу шляхом відмови в доступі до будь-якої форми обчислювальних ресурсів, що

фактично призводить до зупинки процесу, який контролюється системою. Наприклад, серверу, який керує промисловими процесами, можна перешкодити спілкуватися з системами управління нижчого рівня, відмовивши цим системам у доступі до мережі сервера. Були навіть випадки, коли DoS-атаки використовувалися кіберзловмисниками як приманка, щоб замести сліди після проведення атаки в іншій формі.

Інша форма DoS-атак, а саме розподілені атаки на відмову в обслуговуванні (DDoS-атаки), використовує декілька заражених систем для поширення кібератак у більших масштабах. Це викликає особливе занепокоєння щодо безпеки промислових систем управління наступного покоління. Оскільки багато промислових датчиків та елементів обладнання систем управління нового покоління мають можливість прямого підключення до комп'ютерних мереж та Інтернету, DDoS-атака в такому середовищі може мати катастрофічні наслідки для виробничих ліній, де таке обладнання є критично важливим для ефективної та безпечної роботи.

У системах, де механізмів автентифікації мало або вони взагалі відсутні, атаки на введення неправдивих даних можуть бути використані для впровадження шкідливого коду та команд у мережі систем управління. Відсутність механізмів автентифікації означає, що обладнання, на яке спрямована атака, не може перевірити автентичність будь-якої команди, яку воно отримує. Таким чином, це вразливість, якою кібер-зловмисники зі зловмисними намірами можуть відносно легко скористатися. Такі атаки можуть варіюватися від керування промисловими системами управління до виконання дій, що виходять за межі безпечної роботи, до повної реконфігурації обладнання систем управління, щоб воно працювало зовсім не так, як це було заплановано спочатку (прикладом такої атаки є черв'як Stuxnet).

Якщо зловмисники можуть отримати непомічений доступ до промислової мережі систем управління зі слабким захистом, вони можуть

скомпрометувати цілі виробничі лінії, даючи виробничому обладнанню команду на неправильну збірку готової продукції, що поставить під загрозу належну функціональність продукту.

Хоча механізми автентифікації можуть значною мірою запобігти виконанню зловмисних команд обладнанням, на яке спрямовані кібератаки, автентифікований пакет даних може бути повторно переданий, але зі зміненими даними або інструкціями. Оскільки пакет даних має легітимне походження, все ще існує ймовірність того, що такий пакет може бути змінений таким чином, що він буде переданий і оброблений електронним обладнанням без підозри на зловмисні наміри.

Повторних атак можна уникнути, включивши механізм відстеження, наприклад, використання послідовного номера, для виявлення пакетів, які вже були оброблені, але були повторно передані з можливо шкідливими командами і даними. Ці пакети можуть пройти перевірку автентичності і виконати атаку, для якої вони були сформульовані.

Атаки побічних каналів передбачають збір даних через витік інформації через промислове обладнання. Наприклад, коливання споживання електроенергії через обробку даних можуть витікати і надавати зловмисникам цінну інформацію про внутрішню роботу системи. Більш складні атаки можуть здійснюватися за допомогою поглибленого моніторингу промислового виробничого обладнання, наприклад, моніторингу позиційних характеристик роботизованої руки під час виробництва, щоб сформулювати майже точне відтворення виробничих інструкцій, надісланих роботизованим маніпуляторам.

Оскільки смартфони постійно еволюціонують у високотехнологічні та все більш складні пристрої, можливості розширення платформ, на яких здійснюються атаки побічних каналів за допомогою смартфонів, зростають. Вже проводяться дослідження, в яких вивчається вплив атак на 3D-принтери за допомогою вбудованих сенсорів смартфонів на 3D-принтери. Основна

увага в цих дослідженнях зосереджена на акустичних і магнітних побічних каналах.

Вищезгадані атаки не є вичерпним і повним переліком. Існує безліч різних методів, які кібер-зловмисники можуть використовувати для атак на кібер-фізичні системи. Також можна зробити висновок, що багато з відомих атак, знайдених в області IT-мереж, можуть бути однаково загрозливими для пристроїв в області OT-мереж.

2.5 Дослідження методів кіберзахисту “розумних” інформаційно-технологічних проектів

Архітектура цифрової виробничої інформації представляє велику кількість векторів атак, кожен з яких є унікальним у своєму роді. Оскільки перехоплення виробничої інформації відбувається через мережу зв’язку, існує дві можливості для захисту інформаційного потоку. Перший – захистити всю мережу, спрямувавши весь трафік через єдину структуру, яка об’єднує все відповідне обладнання у виробничій архітектурі, як у випадку з типовою архітектурою IT-мережі, наприклад, за допомогою брандмауерів та програмного забезпечення для виявлення вторгнень. Хоча такий підхід звучить правдоподібно, з ним пов’язана низка проблем. Першою з них є той факт, що архітектура цифрового виробництва складається з комбінації IT- та OT-пристроїв. Як правило виробниче обладнання, не має такої ж обчислювальної потужності, як IT-обладнання. Тому будь-яка форма рішення для управління мережею та безпеки, що зазвичай реалізується в IT-середовищі, не буде практичною в мережі з комбінацією IT- та OT-обладнання.

Хоча обчислювальні можливості багатьох вбудованих платформ, що використовуються в OT-обладнанні, значно зросли з моменту появи перших вбудованих платформ, вони все ще можуть стати вузьким місцем, що

призведе до періодичних затримок або перебоїв у виробничому процесі. Обладнання ОТ, особливо в перспективі IIoT, як правило, не розраховане на високу пропускну здатність, оскільки існує обмеження пропускної здатності. Тому більшість обладнання, що використовується сьогодні, взаємодіє за простими протоколами зв'язку, де між платформами передається відносно невелика кількість інформації.

У багатьох виробничих процесах, де час виконання процесу має важливе значення, несподівана затримка в порядку мілісекунд може мати значний вплив на результат виробничого процесу. Тому зрозуміло, що будь-який захід безпеки, який може призвести до такої затримки, не є життєздатним рішенням у цьому контексті. Через постійну еволюцію зловмисних тактик, що використовуються для компрометації мереж безпеки, необхідне регулярне оновлення програмного забезпечення для забезпечення безпеки, щоб гарантувати, що мережа залишається захищеною від новітніх форм атак. У типовій ІТ-інфраструктурі це передбачає завантаження останніх оновлень безпеки, а іноді навіть перезавантаження системи. Таке перезавантаження системи може призвести до незапланованого простою обладнання, що може суттєво вплинути на виробничий процес. Такі оновлення безпеки мають бути заплановані заздалегідь, щоб гарантувати, що вплив на виробничу лінію буде обмеженим. Це ще раз підкреслює несумісність заходів ІТ-безпеки, що використовуються в середовищі ОТ. Таким чином, життєздатним рішенням для забезпечення безпеки буде те, яке розглядає доступність системи як найвищий пріоритет.

Ще один важливий аспект, який необхідно враховувати при пропозиції рішення проблеми безпеки в ОТ-мережах – це поточна інфраструктура, яка використовується виробниками. На відміну від підходу до побудови ІТ-мережі з ІТ-обладнанням, яке можна легко замінити або модернізувати в міру зміни вимог, виробничі організації зазвичай закуповують обладнання для ОТ, орієнтуючись на довговічність і надійність

в довгостроковій перспективі. Якщо деяке IT-обладнання можна замінити або модернізувати протягом п’яти років, то обладнання для OT, як правило, залишається в експлуатації набагато довше, іноді протягом десятиліть. Звідси можна зробити висновок, що значна частина обладнання для OT, яке зараз використовується виробниками, може бути вже десятиліттями застарілою. У таких випадках, найімовірніше, існує набагато досконаліше і складніше обладнання, яке могло б стати ідеальною заміною цьому старому обладнанню. Однак модернізувати інфраструктуру OT за допомогою новішого обладнання не так просто, як встановити новий принтер та оновити деякі драйвери. Будь-які зміни в інфраструктурі OT потребують ретельного планування та ретельного тестування, щоб переконатися, що нове обладнання функціонує в межах застосовних параметрів контролю і не впливає на технологічний процес. Витрати, пов’язані з модернізацією обладнання, в тому числі для резервування на перехідний період, також є важливим питанням.

Якщо обладнання OT на виробничому підприємстві не можна легко і регулярно модернізувати, а традиційні рішення для захисту IT-мереж не підходять для OT-додатків, яке тоді може бути життєздатне рішення для вищезгаданих проблем? Відповідь полягає в поєднанні механізму безпеки на основі IT-технологій, адаптованого для OT-додатків, з дотриманням критичних вимог OT-мереж. Запропоноване рішення цієї проблеми представляє концепції контролера і виробничого пристрою забезпечення безпеки (manufacturing security enforcement device (MSED)) як комбіноване рішення проблеми.

Контролер – це пристрій, на якому працює програмне забезпечення, що виконує завдання безпеки на льоту під час обміну інформацією між IT-обладнанням та обладнанням OT. Такими завданнями можуть бути перехоплення вихідних даних однієї системи, призначених як вхідні дані для іншої системи, виконання криптографічних процесів, таких як авторизація у

вигляді цифрових підписів, і генерування вихідних даних, які можуть бути відправлені на обладнання призначення в зашифрованому форматі. Потім MSED буде підключений безпосередньо в лінію і перед будь-яким обладнанням, яке використовує інформацію, надіслану через мережу, щоб будь-яка інформація, надіслана на обладнання, могла бути криптографічно підтверджена і перевірена її цілісність. MSED виконуватиме дешифрування в режимі реального часу в міру надходження даних від контролера. Крім того, він виконуватиме будь-яку додаткову криптографічну автентифікацію, необхідну для того, щоб гарантувати, що дані, які він отримує, є справді автентичними та дійсними. Таким чином, MSED буде кінцевою структурою, яка надсилає команди до обладнання призначення. Рисунок 2.6 ілюструє концепцію контролера і MSED в мережі ОТ.

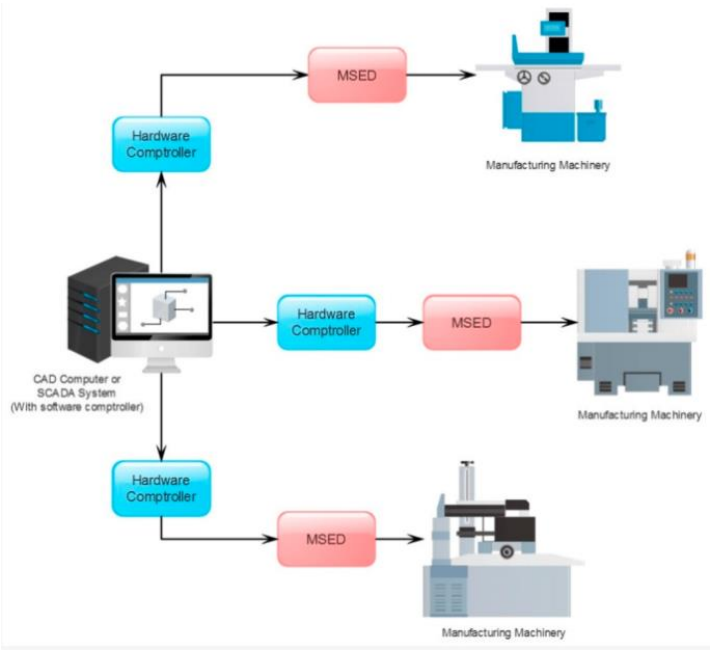

Рисунок 2.6 – Концепція контролера і MSED в мережі ОТ

Будь-яка інформація, надіслана до MSED для перевірки, буде відкинута, якщо її цілісність не може бути підтверджена. Це зробить майже неможливим для зловмисника ввести зловмисно змінену виробничу інформацію в мережу ОТ, призначену для обладнання, яке виконує

несанкціоновані дії. Хоча принцип поєднання контролера і MSED є відносно простим за своєю концепцією, він може по суті усунути проблему зловмисного злому обладнання для ОТ.

Архітектурний підхід до інтеграції заходів безпеки та захисту в рамках інтегрованої системи ґрунтується на тому, що в кожній наступній підсистемі впроваджуються рівні безпеки для виконання локалізованого (і унікального) аналізу даних, замість того, щоб покладатися на єдиний, всеохоплюючий захід безпеки. Такий підхід має значну перевагу, оскільки заходи безпеки можуть застосовуватися на декількох функціональних рівнях, забезпечуючи багаторівневу систему захисту від кібератак. Наприклад, кібератака може використовувати певну комбінацію відомих методів атаки, щоб зламати окремий рівень безпеки, але їй може запобігти наступний рівень безпеки, який виконує більш ретельний аналіз потоку даних і сигналів. І навпаки, єдиний спеціальний захід безпеки може стати єдиною слабкою ланкою в системі безпеки, якщо його буде порушено.

Ще однією додатковою перевагою розподілу заходів безпеки на декілька рівнів є те, що більш надійне загальне рішення безпеки досягається за рахунок забезпечення локального захисту від декількох векторів атак у більш широкому масштабі всієї системи. Крім того, можна навіть забезпечити захист від атак, про які ще не відомо, за допомогою ретельного і періодичного аналізу сигналів і даних, які в кінцевому підсумку блокують атаку через, наприклад, комбінацію вимірювань, які не відповідають певній комбінації системних команд.

Однією з останніх розробок у сфері бездротових технологій і найближчим часом наступником дуже успішної технології 4G і технології “довгострокової еволюції” (LTE) є 5G. Хоча нинішня технологія 4G LTE забезпечує швидкість передачі даних до 1 гігабіта на секунду (Гбіт/с), вона все ще відносно чутлива до перебоїв через перешкоди, спричинені іншими бездротовими сигналами та фізичними перешкодами, такими як будівлі.

Технологія 5G зможе передавати дані зі швидкістю до 10 Гбіт/с і включатиме механізми, які забезпечать ще більш надійне з’єднання. Крім того, 5G забезпечить відповідну платформу для безпечного з’єднання мільярдів пристроїв Інтернету речей в рамках гнучкої мережевої архітектури, яка особливо підходить для з’єднання такої великої кількості пристроїв.

Повноцінні мережі з підтримкою 5G у всьому світі, як очікується, будуть активні до 2025 року. Таким чином, технологія все ще перебуває в зародковому стані, але існуючі ранні мережі 5G, які вже працюють, мають дуже перспективні функції, що матимуть значний вплив на мережі, керовані Інтернетом речей. Тому зараз найкращий час для розробників і дослідників зосередитися на розробці нових мережевих стратегій і заходів безпеки, які повністю відповідають вимогам і сумісні з 5G. Це призведе до розробки мережевих технологій і технологій безпеки, які можна буде негайно впровадити в мережі 5G, а співпраця з розробниками і постачальниками може забезпечити необхідний вплив на кінцевих користувачів цих технологій, щоб вони змінили своє ставлення до мережевої безпеки як до другорядного пріоритету, тим самим усунувши проблему в самому її корені.

2.6 Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений дослідженню кіберзахисту “розумних” інформаційно-технологічних проектів. Здійснено визначення вимог архітектур кіберзахисту проектів даного типу, що дало змогу виокремити їх важливі елементи, які утворять основу архітектури. Досліджено архітектури моделей кіберзахисту “розумних” інформаційно-технологічних проектів, що на основі аналізу сильних та слабких сторін може бути використано при розгортанні конкретних випадків згідно вимог технічного завдання проекту. Досліджено розвиток технологій кіберзахисту “розумних” інформаційно-технологічних проектів в контексті Індустрії 4.0,

що на основі стандарту NIST 1500-201 уможливило визначення областей захисту і на основі конкретного прикладу дало змогу надати рекомендації щодо їх захисту. Проведено дослідження кіберфізичних атак на “розумні” проекти, де проаналізовано останні виклики в індустрії кіберзахисту і показано наслідки їх діяльності. Досліджено методи кіберзахисту “розумних” інформаційно-технологічних проектів де поряд з традиційними методами захисту IT інфраструктури розглянуто спеціалізовані під операційні технології.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Освітлення робочого місця

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: “Про охорону праці”, “Про охорону здоров’я”, “Про пожежну безпеку” [51-55].

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в СНиП II-4-79.

Штучне освітлення в приміщеннях з робочими місцями має здійснюватись системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення). Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати відблисків на поверхні екрана, а освітленість екрана має не перевищувати 300лк. Як джерела світла в разі штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ. У разі влаштування відбитого освітлення у приміщеннях, де переважним чином працюють з документами, допускається застосування металогалогенних ламп потужністю

250Вт. Допускається застосування ламп розжарювання у світильниках місцевого освітлення. Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч), паралельно лінії зору працюючих.

Допускається використання світильників таких класів світлорозподілу:

– прямого світла — П;
– переважно прямого світла — Н;
– переважно відбитого світла — В.

Для загального освітлення слід застосовувати світильники серії ЛПО 3б із дзеркальними гратами, що укомплектовані високочастотними пускорегулювальними апаратами (ВЧ ПРА). Допускається застосовувати світильники цієї серії без ВЧ ПРА тільки в модифікації «Кососвітло».

При відсутності світильників серії ЛПО36 з ВЧ ПРА і без ВЧ ПРА модифікації «Кососвітло» допускається застосування світильників загального освітлення серії:

– ЛПО13 — 2×40/Б — 01;
– ЛПО13 — 4×40/Б — 01;
– ЛПО13 — 2×40 — 06;
– ЛПО13 — 2×65 — 06;
– ЛСО05 — 2×40 — 001;
– ЛСО05 — 2×40 — 003;
– ЛСО04 — 2×36 — 008;
– ЛПО34 — 4×36 — 002;
– ЛПО34 — 4×58 — 002;
– ЛПО31 — 2×31 — 002,

а також їх вітчизняні та зарубіжні аналогів.

Застосування світильників без розсіювачів та екрануючих грат заборонено. Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 градусів з вертикаллю в повздовжній та

поперечній площинах має становити не більше ніж 200 кд/м2, захисний кут світильників — не менше ніж 40 градусів. Світильники місцевого освітлення повинні мати відбивач, що просвічує, із захисним кутом, не меншим ніж 40 градусів.

Слід передбачити обмеження прямої блискості від джерел природного та штучного освітлення. При цьому яскравість світлих поверхонь (вікна, джерела штучного освітлення), що розташовані в полі зору повинна бути не більше ніж 200 кд/м2. Необхідно обмежувати відбиту блискість на робочих поверхнях відносно джерел природного і штучного освітлення. При цьому яскравість відблисків на екрані ВДТ має не перевищувати 40 кд/м2, а яскравість стелі в разі застосування системи відбитого освітлення – 200 кд/м2.

Показник осліпленості у разі використання джерел загального штучного освітлення у виробничих приміщеннях має не перевищувати 20, а показник дискомфорту в адміністративно-громадських приміщеннях має бути не більше за 40. Необхідно обмежувати нерівномірність розподілу яскравості в полі зору працюючих з ВДТ. При цьому співвідношення яскравостей робочих поверхонь має бути не більшим ніж 3:1, а співвідношення яскравостей робочих поверхонь та поверхонь стін, обладнання тощо — 5:1. Коефіцієнт запасу для освітлювальних установок загального освітлення має дорівнювати 1,4. Коефіцієнт пульсації має не перевищувати 5%, що забезпечується застосуванням газорозрядних ламп у світильниках загального та місцевого освітлення з ВЧ ПРА для світильників будь-яких типів. Якщо не має світильників з ВЧ ПРА, то лампи багатолампових світильників або світильники загального освітлення, розташовані поруч, слід вмикати на різні фази трьохфазної мережі. Для забезпечення нормованих значень освітленості у приміщеннях з ВДТ ЕОМ та ПЕОМ слід чистити шибки і світильники принаймні двічі на рік і вчасно замінювати лампи, що перегоріли.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Основні принципи і способи забезпечення життєдіяльності

Можна виділити ряд важливих проблем, які постійно перебувають у полі зору людства для забезпечення нормальних умов життя і праці.

Дотримання параметрів середовища перебування людини в необхідних для життєдіяльності межах – це одна із складних проблем, які стоять перед світовим співтовариством. Це пов’язано з тим, що трудова діяльність людей з року в рік активізується, ускладнюється, вводяться новіші знаряддя праці і технології. Виникає проблема технологічної безпеки [56-60].

Це означає, що збільшується навантаження на всі структурні частини навколишнього середовища, є очевидною небезпека виснаження природних ресурсів, незворотних забруднень і зміни безпечних параметрів середовища, за якими створюються реальні умови для виникнення різного роду небезпек.

Отже, кожна держава повинна мати професійно придатні структури і системи захисту від наслідків імовірних небезпек. Головною метою таких систем є захист населення та зниження рівня ризику при виникненні певних небезпек шляхом запобігання, реагування і ліквідації їх наслідків. Можна навести основні принципи та способи забезпечення життєдіяльності:

– забезпечення населення всіма видами енергоресурсів (електроенергією, газом, нафтопродуктами, кам’яним вугіллям, водою тощо). Енергетична криза, що існує сьогодні, суттєво впливає на життєдіяльність людей. Це одна з найбільш актуальних проблем забезпечення безпеки будь-якої країни світу;

– забезпечення населення всіма необхідними параметрами і нормами матеріального середовища життя. Гострою проблемою для багатьох людей у різних країнах є недостатня кількість житла, комунального транспорту, суспільних закладів, спортивних комплексів, медичних закладів та інших елементів системи життєзабезпечення;

– забезпечення продуктами харчування. Продукти харчування є фізіологічною основою життєдіяльності. Із збільшенням чисельності населення ця проблема стає особливо гострою. Якщо людство не розробить нові перспективні технології вирощування продуктів харчування і своєчасно не адаптується до них, може виникнути небезпечна ситуація глобального масштабу;

– наявність і раціональне використання питної (прісної) води. Йдеться про охорону прісної води від забруднення, що може призвести до непридатності її використання для потреб населення. Звідси випливає важливість очищення води, боротьба з промисловим і побутовим забрудненням, виснаженням водойм;

– ліквідація, переробка або використання відходів виробництва. Особливо небезпечними є відходи атомних, хімічних, біологічних виробництв, кількість яких щорічно зростає і, відповідно, збільшується кількість відходів.

Дотримання основних принципів і способів забезпечення життєдіяльності є необхідною умовою для успішного функціонування людини.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи розглянуто питання освітлення робочого місця. В безпеці в надзвичайних ситуаціях висвітлено питання основних принципів та способів забезпечення життєдіяльності.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи здійснено дослідження кіберзахисту “розумних” інформаційно-технологічних проектів. До основних результатів отриманих в роботі можна віднести:

– здійснено аналіз кіберзахисту “розумних” інформаційно-технологічних проектів, що серед широкого кола завдань виокремило такі, як аналіз загроз, створення заходів захисту, тестування безпеки, дотримання стандартів безпеки, здійснення оновлень. Весь цей процес не є статичним, що потребує постійного моніторингу і прийняття мір;

– проведено аналіз кіберзагроз в проектах “розумне” місто, що визначило кібербезпеку як ключовий фактор для його реалізації. Інформаційні системи, цифрові комунікації та навколишнє цифрове середовище є ключовими елементами для успішних процесів прийняття рішень, які мають на меті вироблення обґрунтованих рішень з важливих і чутливих питань;

– аналіз ризиків кібербезпеки в “розумних” інформаційно-технологічних проектах включає в себе оцінку потенційних загроз і вразливостей, які можуть вплинути на безпеку цих систем;

– стандарти безпеки для “розумних” інформаційно-технологічних проектів грають критичну роль у забезпеченні безпеки цих систем. Такі стандарти встановлюють рекомендації, вимоги та керівні принципи, які допомагають розробникам, виробникам та користувачам забезпечувати високий рівень кібербезпеки. Подано основні стандарти, що забезпечують кіберзахист “розумних” інформаційно-технологічних проектів;

– тестування безпеки “розумних” інформаційно-технологічних проектів є важливою складовою для виявлення потенційних вразливостей і заходів забезпечення безпеки цих систем. Методи тестування допомагають ідентифікувати потенційні слабкі місця в “розумних” проектах та дають

змогу розробникам приймати заходи для їх виправлення або підвищення рівня захищеності. Тестування безпеки має бути постійним процесом, оскільки кіберзагрози постійно еволюціонують.;

– здійснено визначення вимог архітектур кіберзахисту проектів даного типу, що дало змогу виокремити їх важливі елементи, які утворять основу архітектури;

– досліджено архітектури моделей кіберзахисту “розумних” інформаційно-технологічних проектів, що на основі аналізу сильних та слабких сторін може бути використано при розгортанні конкретних випадків згідно вимог технічного завдання проекту;

– досліджено розвиток технологій кіберзахисту “розумних” інформаційно-технологічних проектів в контексті Індустрії 4.0, що на основі стандарту NIST 1500-201 уможливило визначення областей захисту і на основі конкретного прикладу дало змогу надати рекомендації щодо їх захисту;

– проведено дослідження кіберфізичних атак на “розумні” проекти, де проаналізовано останні виклики в індустрії кіберзахисту і показано наслідки їх діяльності;

– досліджено методи кіберзахисту “розумних” інформаційно-технологічних проектів де поряд з традиційними методами захисту IT інфраструктури розглянуто спеціалізовані під операційні технології.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання освітлення робочого місця. В безпеці в надзвичайних ситуаціях висвітлено питання основних принципів та способів забезпечення життєдіяльності.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Critical Infrastructure Security and Resilience [Електронний ресурс]. – https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/chemical-sector – Назва з екрану. – Дата звернення: 1.12.2023.

2. Critical Infrastructure [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/whatis/definition/critical-infrastructure – Назва з екрану. – Дата звернення: 4.12.2023.

3. Critical Infrastructure [Електронний ресурс]. – Режим доступу: https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en – Назва з екрану. – Дата звернення: 4.12.2023.

4. Defining critical infrastructure [Електронний ресурс]. – Режим доступу: https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/defining-critical-infrastructure – Назва з екрану. – Дата звернення: 4.12.2023.

5. What is network functions virtualization nfv [Електронний ресурс]. – Режим доступу: https://www.juniper.net/ru/ru/research-topics/what-is-network-functions-virtualization-nfv.html – Назва з екрану. – Дата звернення: 4.12.2023.

6. Prospects of Cybersecurity in Smart Cities [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/1999-5903/15/9/285 – Назва з екрану. – Дата звернення: 4.12.2023.

7. Solution brief vmware cloud packs [Електронний ресурс]. – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-solution-brief-vmware-cloud-packs.pdf – Назва з екрану. – Дата звернення: 5.12.2023.

8. Cloud packs [Електронний ресурс]. – Режим доступу: https://www.vmware.com/cloud-solutions/cloud-packs.html – Назва з екрану. – Дата звернення: 5.12.2023.

9. NSX [Електронний ресурс]. – Режим доступу: https://www.vmware.com/products/nsx.html – Назва з екрану. – Дата звернення: 5.12.2023.

10. Industry 5.0 – Towards a sustainable, human-centric and resilient European inustry [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en – Назва з екрану. – Дата звернення: 5.12.2023.

11. Industry 5.0, a transformative vision for Europe [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-transformative-vision-europe_en – Назва з екрану. – Дата звернення: 6.12.2023.

12. Enabling Technologies for Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/enabling-technologies-industry-50_en – Назва з екрану. – Дата звернення: 6.12.2023.

13. A Comprehensive Guide to Cloud Security (Risks, Best Practices, Certifications) [Електронний ресурс]. – Режим доступу: https://kinsta.com/blog/cloud-security/ – Назва з екрану. – Дата звернення: 6.12.2023.

14. Cybersecurity for Industrial Internet of Things: Architecture, Models and Lessons Learned [Електронний ресурс]. – Режим доступу: https://paris1.hal.science/hal-03967801/file/Cybersecurity_for_Industrial_Internet_of_Things_Architecture_Models_and_Lessons_Learned.pdf – Назва з екрану. – Дата звернення: 6.12.2023.

15. Дослідження мережевих архітектур для критичних інфраструктур / [Марценко С.В. та ін.]. // Матеріали XI міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі

сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 7 – 8 грудня 2022 р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2022. – С. 137.

16. Models and Methods of Information and Control System Cyber-security for Smart Buildings [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/371044780_Models_and_Methods_of_Information_and_Control_System_Cyber-security_for_Smart_Buildings – Назва з екрану. – Дата звернення: 6.12.2023

17. Industry 4.0 [Електронний ресурс] – Режим доступу: https://www.quuppa.com/industry-4-0/?gclid=Cj0KCQiAm5ycBhCXARIsAPldzoWU20ocJRPYn64SA4xbl_dJgOXqvXcCHd96pTFxRRYJMibIFGEu-7EaAmzaEALw_wcB – Назва з екрану. – Дата звернення: 7.05.2023

18. Дослідження ролі IoT-технологій в промислових комп'ютерних мережах / [Марценко С.В. та ін.]. // Матеріали XI міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 7 – 8 грудня 2022 р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2022. – С. 138.

19. Дослідження процесів автоматизації керування мережевими пристроями / [Марценко С.В. та ін.]. // Матеріали X міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 24 – 25 листопада 2021 р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2021. – С. 140.

20. Amobile solutions [Електронний ресурс]. – Режим доступу: https://www.amobile-solutions.com/en/?gclid=Cj0KCQiAm5ycBhCXAR

IsAPldzoXq_gttAexROGuPD1BpFlttz_iRWPHwGHfJYkZCsHITrnzAGp00qRwaAkK_EALw_wcB – Назва з екрану. – Дата звернення: 7.05.2023

21. Digital transformation in manufacturing [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/manufacturing/how-is-digital-transformation-in-manufacturing-bridging-the-gap-to-productivity-security-resiliency-and-sustainability – Назва з екрану. – Дата звернення: 7.12.2023

22. Internet of Things [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/internet-of-things/modern-manufacturing-does-your-network-have-what-it-takes – Назва з екрану. – Дата звернення: 7.12.2023

23. Infographic: Defense-in-Depth [Електронний ресурс]. – Режим доступу: https://colohouse.com/infographic-defense-in-depth/ – Назва з екрану. – Дата звернення: 7.12.2023

24. Assume Breach: Where Microsoft 365 Business misses on Security (and how to fix it) [Електронний ресурс]. – Режим доступу: https://www.itpromentor.com/assume-breach/ – Дата звернення: 7.12.2023

25. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

26. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

27. What is the Zero Trust Security model? How to implement this strategy with SealPath? [Електронний ресурс]. – Режим доступу: https://www.sealpath.com/blog/zero-trust-security-model-implement-strategy/ – Дата звернення: 7.12.2023

28. DevSecOps Definition, Best Practices and Tools [Електронний ресурс]. – Режим доступу: https://medium.com/@cloud_tips/devsecops-definition-best-practices-and-tools-1789587d165a – Дата звернення: 8.12.2023

29. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв'язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

30. Hermann, M. Pentek, T. Otto, B. "Design Principles for Industrie 4.0 Scenarios." Presented at the 49th Hawaii International Conference on System Sciences. 2016

31. Industry 4.0 and cybersecurity [Електронний ресурс]. – Режим доступу: https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf – Дата звернення: 8.12.2023

32. A Review of Industry 4.0 Manufacturing Process Security Risks [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/2076-3417/9/23/5105 – Дата звернення: 8.12.2023

33. Kagermann, H. Anderl, R. Gausemeier, J. Schuch, G. Wahlster, W. "Industrie 4.0 in a Global Context." ACATECH 2016.

34. Industrial-Internet-of-Things-IIoT [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT – Назва з екрану. – Дата звернення: 8.05.2023.

35. Industrial-internet-of-things-complete-guide [Електронний ресурс]. – Режим доступу: https://www.imperosoftware.com/blog/industrial-internet-of-things-complete-guide/ – Назва з екрану. – Дата звернення: 8.05.2023.

36. Top trends and priorities focus on optimized, sustainable and protected operations [Електронний ресурс]. – Режим доступу: https://www.cgi.com/en/manufacturing/voice-of-our-clients – Назва з екрану. – Дата звернення: 8.05.2023.

37. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу:

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 8.05.2023.

38. Internet-of-things [Електронний ресурс]. – Режим доступу: https://www.wi-fi.org/discover-wi-fi/internet-of-things – Назва з екрану. – Дата звернення: 8.05.2023.

39. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 8.05.2023.

40. Best Network Automation Tools [Електронний ресурс]. – Режим доступу: https://www.dnsstuff.com/network-automation-tools – Назва з екрану. – Дата звернення: 9.05.2023

41. What is network automation? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/automation/network-automation.html – Назва з екрану. – Дата звернення: 9.05.2023.

42. Network automation and orchestration tools review and ratings [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/network-automation – Назва з екрану. – Дата звернення: 9.05.2023.

43. Network automation tools [Електронний ресурс]. – Режим доступу: https://www.pcwdld.com/network-automation-tools-and-software#wbounce-modal – Назва з екрану. – Дата звернення: 9.05.2023.

44. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 9.05.2023.

45. IoT devices separate wi-fi network [Електронний ресурс]. – Режим доступу: https://csolutionsit.com/iot-devices-separate-wi-fi-network/ – Назва з екрану. – Дата звернення: 9.05.2023.

46. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

47. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

48. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

49. Types of IoT networks [Електронний ресурс]. – Режим доступу: https://euristiq.com/types-of-iot-networks/ – Назва з екрану. – Дата звернення: 10.05.2023.

50. Cellular vs wi-fi for IoT [Електронний ресурс]. – Режим доступу: https://www.particle.io/iot-guides-and-resources/cellular-vs-wifi-for-iot/ – Назва з екрану. – Дата звернення: 10.05.2023.

51. Private LTE or 5G [Електронний ресурс]. – Режим доступу: https://www.iplook.com/solutions/private-lte-5g-solution_s0013.html?gclid=CjwKCAiAs8acBhA1EiwAgRFdw6QjenpP7DfgJ_DFKVNMc0lE4cQmgOIAfmsWoDUoRxFFQN1kGpYc8BoCQJMQAvD_BwE – Назва з екрану. – Дата звернення: 10.05.2023.

52. Державні будівельні норми України. Інженерне обладнання будинків і споруд. Природне і штучне освітлення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/95.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-28-2006.%20%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%BD%D0%B5%20%D1%96%20%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B5%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

53. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text – Назва з екрану. – Дата звернення: 06.05.2022.

54. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/31562/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_0.00-1.28-10 – Назва з екрану. – Дата звернення: 06.05.2022.

55. Про затвердження Правил охорони праці під час виконання робіт на висоті [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0573-07#Text – Назва з екрану. – Дата звернення: 06.05.2022.

56. Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці та Переліку робіт з підвищеною небезпекою [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0231-05#Text – Назва з екрану. – Дата звернення: 06.05.2022.

57. Проектування електрообладнання об’єктів цивільного призначення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/92.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-23~2010.%20%D0%86%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%BD%D0%B5%20%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B1%D1%83%D0%B4%D0%B8%D0%BD%D0%BA%D1%96%D0%B2%20%D1%96.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

58. Правила улаштування електроустановок [Електронний ресурс]. – Режим доступу: https://art-

energetyka.com.ua/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D1%83%D0%BB%D0%B0%D1%88%D1%82%D1%83%%B0%D0%BD%D0%BE%D0%B2%D0%BE%D0%BA.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

59. Про затвердження "Правил будови електроустановок. Електрообладнання спеціальних установок" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0272203-01#Text – Назва з екрану. – Дата звернення: 06.05.2022.

60. Про затвердження державних будівельних норм ДБН В.2.5-56:2010 "Інженерне обладнання будинків і споруд. Системи протипожежного захисту" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0537738-10#Text – Назва з екрану. – Дата звернення: 06.05.2022.

Додатки

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів

6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

УДК 004.72

С. А. Жураковський, В. Ю. Олійник, В. Р. Ковалишин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ СВІТОВОГО ДОСВІДУ ВПРОВАДЖЕННЯ НОВИХ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ ІНДУСТРІЇ 5.0

S. A. Zhurakovskyi, V. Y. Oliinyk, V. R. Kovalyshyn

STUDY OF THE WORLD EXPERIENCE OF IMPLEMENTING NEW NETWORK TECHNOLOGIES IN THE CONTEXT OF INDUSTRY 5.0

Концепція індустрії 5.0 [1] визначає наступну фазу розвитку виробництва, де промислові процеси взаємопов'язані з новітніми мережевими технологіями, до яких можна віднести Інтернет речей (IoT), штучний інтелект (AI), блокчейн, розширена реальність (AR) та інші.

Світовий досвід впровадження нових мережевих технологій в контексті Індустрії 5.0 є дуже важливим для України, оскільки більшість технологій є іноземного виробництва, а їх різноманіття і динамічність появи - величезна. Останнім часом лідери світового ринку активно впроваджують новітні технології для створення "розумних" фабрик, де автоматизація промислових процесів відбувається за допомогою даних з IoT-датчиків, аналізу даних з використанням штучного інтелекту (AI) та інших інструментів для прийняття рішень.

Прикладом одного з лідерів впровадження Індустрії 5.0 може бути Японія. В межах дослідження тут розвиваються концепції "Фабрики майбутнього" та "Соціальні інновації", де активно впроваджуються новітні мережеві технології, що покликані покращити виробничі процеси та підвищити якість життя населення.

У Німеччині широко впроваджувались ініціативи концепції попередника Індустрії 4.0 для створення "фабрик майбутнього" з використанням цифрових технологій.

Розробки в області мережевих технологій значною мірою проводяться у США, які спрямовані на створення "інтелектуальних" систем виробництва та новітніх методів управління процесами.

До основних питань, що потребують глибшого дослідження можна віднести: стандартизацію, кібербезпеку, інтеграцію цих технологій у виробничі процеси та кадровий потенціал для використання цих нововведень.

У контексті Індустрії 5.0 питання безпеки можна віднести до одного з ключових, оскільки багато систем стають пов'язаними інтернетом. Кібератаки стали звичним явищем, тому методи протидії та захисту потребують удосконалення на постійній основі. Великі обсяги даних зібраних сенсорами, а також захист самих сенсорів є дуже актуальним. З огляду на зростання автоматизації виробництва за допомогою робототехніки та автоматичних систем, важливо забезпечити безпеку працівників та виробничих приміщень, використовуючи безпечні та надійні системи. Встановлення міжнародних стандартів у сфері безпеки є ключовим для забезпечення відповідності та захисту систем у всіх країнах та галузях промисловості.

Успішна реалізація концепції Індустрії 5.0 вимагає співпраці між державними органами, промисловими лідерами та науково-дослідними установами для створення сприятливого середовища для інновацій та розвитку нових технологій.

Література

1. What is Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en – Назва з екрану. – Дата звернення: 24.11.2023.