

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

(повне найменування назва факультету)

кібербезпеки

(повна назва кафедри)

## Дипломна робота

Проектування систем кібербезпеки в концепції цифрового  
виробництва та Індустрії 4.0

Виконав: студент групи ПМК-42с

спеціальності

125 «Кібербезпеки»

(шифр і назва спеціальності)

*Коханевич*

(підпис)

Коханевич Д.В.

(прізвище та ініціали)

Керівник

*Моркун*

(підпис)

Моркун Н.В.

(прізвище та ініціали)

Рецензент

*Пархоменко*

(підпис)

Пархоменко І.І.

(прізвище та ініціали)



**ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ІВАНА ФРАНКА**

Факультет Прикладної математики та інформатики  
Кафедра Кібербезпеки  
Спеціальність: 125 «Кібербезпека»  
«шифр і назва»

**«ЗАТВЕРДЖУЮ»**  
Завідувач кафедри 

"31 "серпня" 2022 року

Проектування систем кібербезпеки в концепції цифрового виробництва та  
Індустрії 4.0

**ЗАВДАННЯ**  
на кваліфікаційну бакалаврську роботу студента  
**Коханевича Дениса**  
( прізвище, ім'я, по батькові)

1. **Тема роботи:** Проектування систем кібербезпеки в концепції цифрового виробництва та Індустрії 4.0  
Керівник роботи професор, д.т.н. Моркун Н.В.  
затверджені наказом університету від «13» вересня 2021 року № 15
2. **Строк подання студентом роботи** «13» червня 2023 року
3. **Вихідні дані до роботи:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
4. **Зміст пояснювальної записки (перелік питань, які потрібно розробити)**
  1. Основні поняття та принципи концепції цифрового виробництва та Індустрії 4.0
  2. Дослідження ролі кіберзахисту цифрового виробництва
  3. Аналіз кіберзахисту промислового інтернету речей
  4. Розробка та налаштування «Smart Grid» засобами Cisco Packet Tracer
5. **Перелік графічного матеріалу:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## 6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 31 серпня 2022 р.

## КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Точення постановки завдання	21.03.2023	
2	Книз літератури	28.03.2023	
3	Обґрунтування вибору рішення	31.03.2023	
4	Збір даних	07.04.2023	
5	Основні поняття та принципи інфраструктури	18.04.2023	
6	Роль підприємств цифрового виробництва	28.04.2023	
7	Книз підприємств промислового інтернету речей	12.05.2023	
8	Оформлення та функціональної частини	25.05.2023	
9	Оформлення та функціональної частини	08.06.2023	
10	Отримання рецензій	10.06.2023	
11	Надання роботи на оцінку	12.06.2023	
12	Захист в ЕК	16.06.2023	

Студент

  
 (підпис)

 Коханевич Д.  
 (ініціали, прізвище)

Керівник роботи

  
 (підпис)

 Моркун Н.В.  
 (ініціали, прізвище)

## РЕФЕРАТ

Пояснювальна записка дипломного проекту складається зі вступу, чотирьох розділів, що містять 19 рисунків, висновків та списку використаних джерел з 45 найменувань. Загальний обсяг роботи становить 78 сторінки.

**Об'єктом** дослідження є безпека об'єктів у контексті трансформації цифрових виробництв та технології Індустрії 4.0.

**Метою** роботи є дослідження кібербезпеки в концепції цифрового виробництва та Індустрії 4.0, а саме виявлення загроз та вразливостей промислового інтернету речей.

У першому розділі розглядається актуальність питання впровадження та захисту цифрової трансформації виробництва. Аналізуються теоретичні основи концепції цифрового виробництва та Індустрії 4.0, включаючи їх визначення та ключові аспекти. Також розглядаються основні принципи цифрового виробництва та Індустрії 4.0, які визначають напрямки та стратегії розвитку цифрових технологій у виробничому середовищі.

У другому розділі розглядаються основні поняття кібербезпеки в контексті цифрового виробництва та Індустрії 4.0. Аналізуються загрози та вразливості процесу трансформації цифрового виробництва, а також досліджуються ризики трансформації підприємств до цифрових бізнес-моделей у контексті Індустрії 4.0.

У третьому розділі проводиться загальна характеристика промислового Інтернету речей (ІоТ) та його особливості. Розглядається архітектура та компоненти промислового ІоТ, а також питання безпеки технологій промислового Інтернету речей. Крім того, розглядається класифікація загроз промислому інтернету речей та стандарти забезпечення безпеки у промислому Інтернеті речей.

У четвертому розділі розглядається поняття "розумних мереж енергозбереження" і проводиться проектування мережі засобами Cisco Packet Tracer. Аналізуються сервіси конфігурації сервера, маршрутизатори, джерела енергії мережі та підключення моніторингу та програмування ІоТ пристроїв. Також надаються рекомендації щодо захисту розумних мереж енергозбереження. Закінчується розділ висновками, які підсумовують отримані результати розробки та налаштування «Smart Grid»..

**Ключові слова:** ІНДУСТРІЯ 4.0, ЗАГРОЗИ, ЦИФРОВЕ ВИРОБНИЦТВО, ПРОМИСЛОВИЙ ІНТЕРНЕТ РЕЧЕЙ (ІОТ), БЕЗПЕКА, ВРАЗЛИВОСТІ, РОЗУМНІ МЕРЕЖІ.

## ABSTRACT

The explanatory note of the diploma project consists of an introduction, four chapters containing 19 figures, conclusions and a list of 45 references. The total volume of the work is 78 pages.

The **object** of research is the security of facilities in the context of the transformation of digital production and Industry 4.0 technology.

The **purpose** of the study is to investigate cybersecurity in the concept of digital manufacturing and Industry 4.0, namely to identify threats and vulnerabilities of the industrial Internet of Things.

The first section discusses the relevance of the issue of implementing and protecting the digital transformation of production. The theoretical foundations of the concept of digital manufacturing and Industry 4.0 are analyzed, including their definitions and key aspects. The basic principles of digital manufacturing and Industry 4.0, which determine the directions and strategies for the development of digital technologies in the production environment, are also considered.

The second section discusses the basic concepts of cybersecurity in the context of digital manufacturing and Industry 4.0. The threats and vulnerabilities of the digital manufacturing transformation process are analyzed, as well as the risks of transforming enterprises to digital business models in the context of Industry 4.0.

The third section provides a general description of the Industrial Internet of Things (IIoT) and its features. The architecture and components of the industrial IIoT, as well as the security of industrial IoT technologies are considered. In addition, the classification of threats to the industrial Internet of things and standards for ensuring security in the industrial Internet of things are considered.

The fourth chapter discusses the concept of "smart energy networks" and designs the network using Cisco Packet Tracer. It analyzes server configuration services, routers, network energy sources, and IoT device monitoring and programming connections. Recommendations for protecting smart energy networks are also provided. The chapter ends with conclusions summarizing the results of the development and configuration of the Smart Grid.

**Keywords: INDUSTRY 4.0, THREATS, DIGITAL MANUFACTURING, INDUSTRIAL INTERNET OF THINGS (IIoT), SECURITY, VULNERABILITIES, SMART GRIDS.**

## ЗМІСТ

Перелік умовних скорочень.....	8
Вступ.....	9
Розділ 1. Основні поняття та принципи концепції цифрового виробництва та Індустрії 4.0 .....	12
1.1 Актуальність питання впровадження та захисту цифрової трансформації виробництва .....	12
1.2 Теоретичні основи концепції цифрового виробництва та Індустрії 4.0	15
1.3 Основні принципи цифрового виробництва та Індустрії 4.0 .....	20
1.4 Міжнародний досвід розвитку цифрового виробництва та Індустрії 4.0 .....	24
Висновки по розділу 1.....	29
Розділ 2. Дослідження ролі кіберзахисту цифрового виробництва .....	30
2.1 Основні поняття кібербезпеки в контексті цифрового виробництва та Індустрії 4.0 .....	30
2.2 Аналіз загроз та вразливостей процесу трансформації цифрового виробництва .....	33
2.3 Дослідження ризиків трансформації підприємств до цифрових бізнес-моделей у контексті Індустрії 4.0 .....	36
Висновки по розділу 2.....	38
Розділ 3. Аналіз кіберзахисту промислового інтернету речей .....	39
3.1 Загальна характеристика промислового Інтернету речей (ІІоТ) та його особливості .....	39
3.2 Архітектура та компоненти промислового ІІоТ .....	40
3.3 Питання безпеки технологій промислового Інтернету речей .....	43
3.4. Класифікація загроз промислового інтернету речей .....	46
3.5 Стандарти забезпечення безпеки у промисловому Інтернеті речей .....	50

	7
Висновки по розділу 3.....	52
Розділ 4. Розробка та налаштування «Smart Grid» засобами Cisco Packet Tracer .....	53
4.1 Поняття «розумних мереж енергозбереження».....	53
4.2 Проектування мережі .....	58
4.2.1 Сервіси конфігурації сервера .....	58
4.2.2 Маршрутизатор .....	60
4.2.3 Джерела енергії мережі .....	60
4.2.4 Підключення моніторингу та програмування IoT пристроїв ....	62
4.3 Програмне забезпечення мережі .....	64
4.4 Рекомендації щодо захисту розумних мереж енергозбереження .....	69
Висновки по розділу 4.....	71
Висновки.....	72
Список використаних джерел.....	74

**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

IoT	–	Інтернет речей
IIoT	–	промисловий Інтернет речей (Industrial Internet of Things)
ШІ (AI)	–	штучний інтелект (Artificial Intelligence)
Big Data	–	великі дані
Cloud	–	хмарні обчислення
ML	–	машинне навчання (Machine Learning)
ICS	–	промислові системи управління
	–	

## ВСТУП

**Актуальність.** Цифрова революція, що охопила світову економіку, вражає масштабом, темпами та географією. Починаючи з 1960-х років, цифрові інновації поширювалися у світі змінювали одне одного хвилями, що виходили з наукових епіцентрів США, Європи та СРСР. Кожна з цих хвиль була інтенсивнішою за попередню, охоплюючи нові регіони і надаючи все більш відчутний для економіки ефект. Перша хвиля цифрових інновацій зводилася до автоматизації існуючих технологій та бізнес-процесів. Друга хвиля припала на середину 1990-х рр., коли поширення інтернету, мобільного зв'язку, соціальних мереж, поява смартфонів призвели до стрімкого зростання використання технологій кінцевими споживачами. Сьогодні третя хвиля цифрових технологій змінює саму бізнес-модель компаній, підвищує ефективність витрат та виявляє нові можливості на ринку.

Сьогодні цифрові технології змінюють саму операційну модель компаній, особливо в банківському та телекомунікаційному секторах, підвищують ефективність витрат та виявляють нові можливості на ринку. Навіть у традиційних галузях економіки процес перетворення став незворотнім через зростаючий темп диджиталізації усього суспільств.

Сьогодення ставить нові питання щодо модернізації промислових комплексів та побудови цифрової системи їх внутрішнього виробництва та міжсуб'єктної взаємодії. І це є одним з найбільш актуальних напрямків розвитку економіки практично будь-якої країни, як розвиненої так і країни, що розвивається. Технологічний рівень розвитку промислового виробництва має прямий зв'язок із конкурентоспроможністю національної економіки.

Для промислового підприємства диджиталізація насамперед є інформаційним простором у вигляді інфраструктурної надбудови над матеріальним сектором економіки, яка покликана підвищити ефективність взаємодії учасників процесів виробництва та реалізації продукції.

У зв'язку з цим очевидно є необхідність паралельного розвитку digital-процесів, що впроваджуються на виробництві, та інкрементальне вдосконалення матеріально-технічної бази.

Однією з найуспішніших моделей цифрової модернізації промислових підприємств на даний момент можна вважати німецьку стратегічну ініціативу «Індустрія 4.0».

І хоча фактично дана програма далека від кінцевої мети її впровадження, вже на поточному етапі можливе визначення позитивних соціально-економічних факторів для проектування їх на вітчизняну систему промислового виробництва.

Інтенсивне розповсюдження інноваційних інформаційних технологій сприяло появі Інтернет речей (IoT), який активно поширюється світом і знаходиться на порозі сплеску розвитку. Цьому сприяють кілька факторів: мережі 5G, Індустрія 4.0 або Четверта промислова революція, можливості мікропроцесорних обчислень, що зростають. Розумний будинок, бізнес та промисловий сегмент IoT-пристроїв мають схожі проблеми впровадження – відсутність єдиних стандартів, у тому числі стандартів документації, якісних описів протоколів та з'єднань та відповідна дорожня аналіз рівня фактичної захищеності, відсутність стандартів функцій захисту та, як правило, брак ресурсів мікрочіпів на якісне використання цих функцій (шифрування, автентифікація і т.д.).

Основи індустрії 4.0 становили три попередні промислові революції. Як свідчать вчені, основою Четвертої промислової революції є доступність усієї релевантної інформації у режимі реального часу. Тому, проектування ефективної системи захисту є одним із наріжних каменів у структурі цифрової трансформації бізнес-процесів.

**Метою** роботи є дослідження кібербезпеки в концепції цифрового виробництва та Індустрії 4.0, а саме виявлення загроз та вразливостей промислового інтернету речей.

Для вирішення поставленої мети були сформовані наступні завдання:

1. Розглянути основні поняття та принципи цифрового виробництва та Індустрії 4.0

2. Дослідити роль кіберзахисту цифрової трансформації виробництва та визначити їх ризики.
3. Розглянути архітектуру промислового інтернету речей
4. Проаналізувати питання безпеки технологій ПоТ
5. Розробити та налаштувати «розумну» мережу енергозбереження офісу
6. Розробити рекомендації щодо захисту.

**Об'єктом** дослідження є безпека об'єктів у контексті трансформації цифрових виробництв та технології Індустрії 4.0.

## РОЗДІЛ 1.

# ОСНОВНІ ПОНЯТТЯ ТА ПРИНЦИПИ КОНЦЕПЦІЇ ЦИФРОВОГО ВИРОБНИЦТВА ТА ІНДУСТРІЇ 4.0

### 1.1 Актуальність питання впровадження та захисту цифрової трансформації виробництва

Глобалізація і швидкий розвиток технологій приводять до формування нової економічної епохи, відомої як "четверта промислова революція" або Індустрія 4.0. Ця концепція визначає новий етап в розвитку виробництва, який характеризується інтеграцією цифрових технологій у всі сфери господарства.

Характерними рисами Industry 4.0 є повністю автоматизовані виробництва, в яких усі процеси управляються в режимі реального часу та з урахуванням мінливих зовнішніх умов. Кіберфізичні системи створюють віртуальні копії об'єктів фізичного світу, контролюють фізичні процеси, приймають децентралізовані рішення. Вони здатні об'єднуватися в мережі, взаємодіяти в реальному часі, саморегулюватися та навчатися. Важлива роль Інтернет-технологій - спілкування між персоналом і машинами. Підприємства створюють продукцію відповідно до вимог індивідуального замовника, оптимізуючи собівартість продукції.

Ця епоха відкриває широкі можливості для підвищення продуктивності, інновацій та конкурентоспроможності підприємств. Вона змінює спосіб виробництва, забезпечуючи зв'язок між фізичними та цифровими системами, автоматизуючи процеси та створюючи розумні фабрики та мережі. Індустрія 4.0 також має потенціал для збільшення зайнятості, створення нових робочих місць та підтримки сталих економічних зростань.

Однак, разом з перевагами, Індустрія 4.0 ставить перед суспільством нові виклики, такі як зміни в робочій силі та навичках працівників, проблеми кібербезпеки та захисту даних, а також соціальні і етичні питання. Тому важливо враховувати ці виклики і розробляти стратегії, що сприяють сталому розвитку та включають всі сектори суспільства.

Загалом, Індустрія 4.0 відкриває нові можливості для підприємств та суспільства в цілому, але вимагає активної адаптації, інноваційного мислення та співпраці між різними секторами, щоб забезпечити успішний перехід у нову промислову епоху.

Концепція цифрової трансформації виробництва та Індустрія 4.0 є надзвичайно актуальними у сучасному світі. Вони відображають глобальні зміни у сфері виробництва, викликані проникненням інформаційних та комунікаційних технологій у всі аспекти бізнесу та суспільства. Існує ряд факторів, що підтверджують актуальність цих концепцій (рис. 1.1).



Рисунок 1.1 – Базові фактори, що підтверджують актуальність концепцій цифрового виробництва та Індустрії 4.0

Технологічний прогрес є фактором інтенсифікації змін у різних сферах діяльності людини. Швидкий розвиток цифрових технологій, таких як інтернет речей (IoT), штучний інтелект (AI), великі дані (Big Data), хмарні обчислення та автоматизація призводить до появи нових можливостей та переосмислення традиційних методів виробництва. Цифрова трансформація та Індустрія 4.0 є відповіддю на ці виклики і дозволяють компаніям стати більш гнучкими, ефективними та конкурентоспроможними.

Застосування цифрових технологій та концепцій Індустрії 4.0 дозволяє знизити витрати на виробництво, підвищити продуктивність, покращити якість продукції та оптимізувати бізнес-процеси. Автоматизація, використання даних прийняття рішень, управління виробничими активами і цифрова інтеграція ланцюга поставок сприяють підвищенню ефективності виробництва.

Виходячи з цих факторів, можна зробити висновок про те, що концепція цифрової трансформації виробництва та Індустрія 4.0 є актуальними та

важливими для сучасних підприємств. Вони пропонують нові можливості для підвищення конкурентоспроможності, покращення продуктивності, створення інновацій та відповідності вимогам ринку та законодавства.

У сучасному виробничому оточенні, де все більше даних збирається, передається та аналізується, захист конфіденційності, цілісності та доступності цих даних стає особливо важливим. Різні типи даних, такі як інтелектуальна власність, технічні малюнки, конструкторська документація, персональні дані співробітників та клієнтів вимагають надійного захисту від витоку, несанкціонованого доступу та використання.

Кібербезпека цифрового виробництва та Індустрії 4.0 є актуальними темами та привертають значну увагу дослідників, фахівців та організацій. Існує безліч робіт та літератури, присвячених цій темі.

Ціла низка наукових статей присвячена питанням сучасних викликів кібербезпеці у рамках цифрового виробництва та Індустрії 4.0 [5, 6]. Ряд авторів розглядають основні виклики та рішення в галузі безпеки та конфіденційності в Індустрії 4.0 і пропонують різні рішення щодо забезпечення безпеки цифрового виробництва [7].

Основний акцент в роботі [8] зроблено на значущості безпеки та конфіденційності даних у рамках цифрового виробництва, що дозволило докладно описати основні виклики безпеки, які пов'язані з Індустрією 4.0, включаючи загрози кібербезпеки, фізичну безпеку, керування доступом та захист даних. Автори звернули увагу на унікальні аспекти безпеки, що виникають у контексті цифрового виробництва і зробили огляд різних технологій та підходів, які можуть бути застосовані для забезпечення безпеки Індустрії 4.0. Особливістю даної наукової роботи є формування методології забезпечення безпеки для Індустрії 4.0, яка включає кроки з ідентифікації вразливостей, оцінки ризиків, розробки стратегії безпеки, реалізації заходів безпеки та постійного моніторингу [8].

Поява інноваційних технологій і трансформація їх у цифрове виробництво спонукало науковців досліджувати кіберфізичні системи у розрізі розумних фабрик та виробництв [9, 10].

У ряді наукових робіт досліджувалися проблеми безпеки в кіберфізичних системах для розумного виробництва [11]. У статті наведено огляд архітектури кіберфізичних систем для розумного виробництва, включаючи компоненти та їх взаємодію. Особлива увага приділяється аспектам безпеки у цій архітектурі. Автори обговорюють різні виклики та проблеми безпеки, з якими стикаються кіберфізичні системи для розумного виробництва. Це включає загрози кібербезпеки, фізичну безпеку, безпеку даних і конфіденційність [11].

Також у науковій літературі багато робіт присвячено огляду різних методів та заходів безпеки, які можуть бути застосовані для захисту кіберфізичних систем у розумному виробництві, які включають автентифікацію та авторизацію, шифрування даних, контроль доступу та моніторинг загроз [9-11].

Одним з напрямків Індустрії 4.0 є впровадження хмарних технологій (Cloud) та промислового Інтернету речей (Industrial Internet of Things, IIoT). Тому в цьому напрямку працюють і науковці досліджуючи архітектуру безпечного промислового інтернету речей для хмарного виробництва [12, 13].

У ряді робіт проводиться огляд різних заходів безпеки, які можуть бути застосовані в архітектурі безпечного IIoT, різні протоколи та стандарти безпеки, які можуть бути застосовані в архітектурі безпечного IIoT (протоколи шифрування, протоколи автентифікації та стандарти безпеки мереж) [14, 15, 16].

Отже, дослідження в галузі цифрової трансформації виробництва та Індустрії 4.0 мають широкий спектр наукових здобутків, які дозволяють реалізовувати сучасні інновації у ефективному розвитку промисловості.

## **1.2 Теоретичні основи концепції цифрового виробництва та Індустрії 4.0**

Концепція цифрового виробництва, також відома як цифрова промисловість або цифрова трансформація виробництва, є стратегічним підходом до використання цифрових технологій та інновацій для оптимізації та модернізації процесів виробництва.

Метою концепції цифрового виробництва є підвищення ефективності, гнучкості та конкурентоспроможності виробничих підприємств. Вона пропонує

інтеграцію цифрових технологій на всіх етапах життєвого циклу продукту, починаючи з розробки та проектування та закінчуючи виробництвом, управлінням якістю та обслуговуванням.

Термін «Індустрія 4.0» отримав широке розповсюдження на Давоському економічному форумі в 2016 році завдяки монографії його засновника К. Шваба, яка дала поштовх для дискусій та розгортання концепції. Проте важливо зазначити, що поняття "Індустрія 4.0" було вперше введено німецьким урядом ще в 2011 році, в рамках стратегії розвитку ФРН. Ця стратегія спрямовувалась на розбудову інноваційного промислового сектору та забезпечення лідерства Німеччини в галузі промислових інновацій. Метою було досягнення світового лідерства до 2020 року та створення повноцінної системи інтернетизованої промисловості до 2030 року.

Таким чином, Давоський економічний форум у 2016 році використав цей термін для просування концепції та популяризації її ідей на міжнародному рівні.

Подібні розробки представлені в програмних документах, що визначають пріоритети промислового розвитку провідних країн - США, Японії, Великобританії, Франції, Південної Кореї, Китаю. Аналогічні програми запуснені також у Нідерландах, Італії, Бельгії та інших країнах.

Технології «Індустрії 4.0» вже зараз перетворюють промисловість у всьому світі, а їхнє повномасштабне впровадження у світову економіку в майбутньому може вплинути на продуктивність і ринок праці, який можна порівняти з промисловими революціями минулого. McKinsey виділяє вісім основних важелів створення вартості внаслідок впровадження технологій Індустрії 4.0 на виробництві.

Концепція цифрового виробництва та Індустрії 4.0 базується на кількох теоретичних засадах, які формують її основні принципи та цілі (1.2).

Кіберфізичні системи (КФС) є основою цифрового виробництва та Індустрії 4.0. Кіберфізичні системи - це інтеграція фізичних систем, таких як машини та обладнання, з цифровими технологіями, включаючи датчики, виконавчі механізми та обчислювальні системи. CPS дозволяє здійснювати

моніторинг, контроль і координацію фізичних процесів у реальному часі та забезпечує основу для оцифрування й автоматизації виробництва.

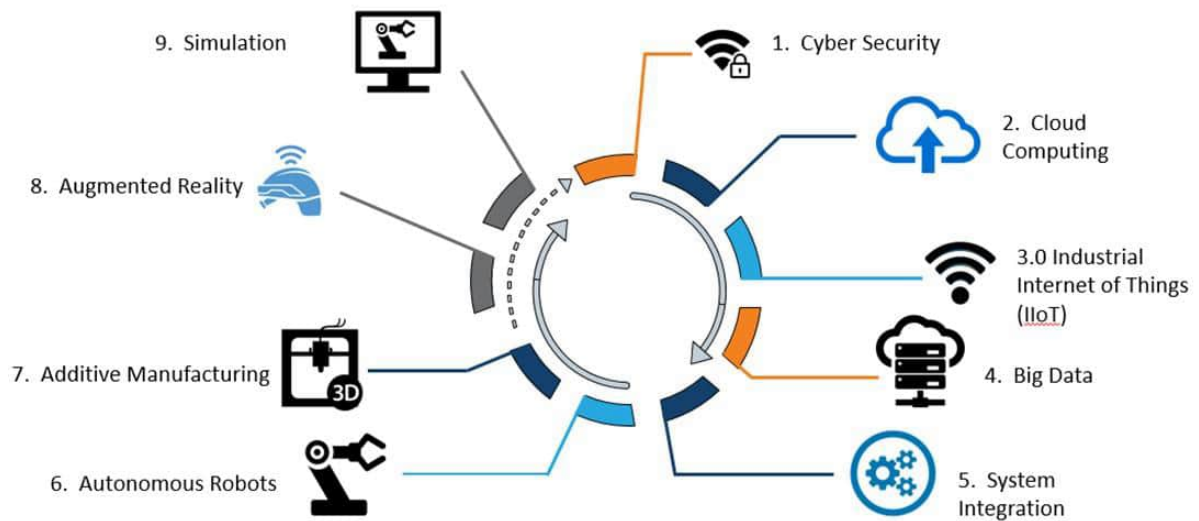


Рисунок 1.2 – Базові засади цифрового виробництва та Індустрії 4.0

Вирішальну роль в Індустрії 4.0 відіграє Інтернет речей (IoT), підключаючи фізичні пристрої та об'єкти до Інтернету, дозволяючи їм збирати та обмінюватися даними. Пристрої та датчики IoT широко використовуються в цифровому виробництві для збору інформації про машини, продукти та процеси в режимі реального часу, що полегшує прийняття рішень та оптимізацію на основі даних.

Великі дані та аналітика: Велика кількість даних, що генеруються пристроями CPS і IoT в цифровому виробництві, вимагає передових методів аналізу для вилучення значущої інформації. Аналітика великих даних допомагає обробляти та аналізувати великі обсяги даних для виявлення закономірностей, кореляцій і тенденцій. Ці знання можна використовувати для оптимізації процесів, прогнозування потреб у технічному обслуговуванні, покращення якості та підвищення загальної операційної ефективності.

Хмарні обчислення забезпечують масштабовану і гнучку інфраструктуру для зберігання, обробки та доступу до даних і додатків через Інтернет. У цифровому виробництві хмарні обчислення забезпечують централізоване зберігання даних, обчислювальні потужності та програмні ресурси, полегшуючи

спільну роботу, віддалений доступ та обмін даними в режимі реального часу між різними зацікавленими сторонами.

Широко застосовуються в Індустрії 4.0 методи штучного інтелекту (AI) та машинного навчання (ML) для забезпечення інтелектуальної автоматизації, предиктивної аналітики та прийняття рішень. Алгоритми AI та моделі ML можуть аналізувати складні моделі даних, прогнозувати результати та автоматизувати завдання, що призводить до підвищення ефективності, якості та швидкості реагування у виробничих процесах.

Зі збільшенням зв'язку та оцифрування в Індустрії 4.0 кібербезпека стає критично важливою проблемою. Захист цифрових активів, даних і систем від кіберзагроз, а також забезпечення приватності та конфіденційності є надзвичайно важливими. Заходи кібербезпеки, включаючи шифрування, автентифікацію, контроль доступу та безпечні протоколи зв'язку, застосовуються для захисту цифрових виробничих систем.

Ці теоретичні основи в сукупності забезпечують основу для концепції цифрового виробництва та Індустрії 4.0. Вони уможливають інтеграцію цифрових технологій, аналізу даних, автоматизації та зв'язку для трансформації традиційних виробничих процесів і стимулювання інновацій, ефективності та продуктивності в промисловому секторі.

Індустрія 4.0 об'єднує набір технологічних досягнень і технічних засобів для оптимізації промислових процесів (рис. 1.3).



Рисунок 1.3 – Набір технологічних досягнень і технічних засобів для оптимізації промислових процесів

Застосування цифрових технологій, зв'язку та підходів на основі даних для перетворення традиційних виробничих процесів на більш ефективні, гнучкі та інтелектуальні операції сприяють появі нових бізнес інструментів, які демонструють принципи Індустрії 4.0 і можуть бути впроваджені для підвищення продуктивності, якості та інновацій у різних галузях промисловості.

Створення «розумних» фабрик та заводів передбачає використання передових технологій, таких як пристрої Інтернету речей, датчики та робототехніка. Ці заводи оснащені взаємопов'язаними машинами, системами і процесами, які дозволяють збирати, аналізувати і приймати рішення в режимі реального часу. Розумні заводи можуть оптимізувати виробничі процеси, скоротити час простою і підвищити загальну ефективність [18].

Це однією технологією стало впровадження адитивного виробництва (3D-друк), яке є ключовим компонентом Індустрії 4.0. Воно передбачає використання технології 3D-друку для створення об'єктів шляхом додавання шарів матеріалу на основі цифрового дизайну. Адитивне виробництво уможлиблює швидке створення прототипів, кастомізацію та виробництво на вимогу, зменшуючи відходи матеріалів та уможливаючи складну геометрію, якої важко досягти традиційними методами виробництва [19].

Розвиток віртуальних технологій сприяв виникненню поняття «цифровий двійник». Цифровий двійник - це віртуальне представлення фізичного продукту, процесу або системи, який інтегрує дані в реальному часі з датчиків і пристроїв Інтернету речей для створення цифрової копії, яку можна використовувати для моделювання, моніторингу та оптимізації. Цифрові двійники допомагають виробникам аналізувати та оптимізувати продуктивність, прогнозувати потреби в технічному обслуговуванні та виявляти потенційні проблеми до того, як вони виникнуть.

Індустрія 4.0 використовує автономних роботів, які можуть виконувати завдання без втручання людини. Ці роботи оснащені сучасними датчиками, алгоритмами штучного інтелекту та можливостями машинного навчання, щоб орієнтуватися в навколишньому середовищі, взаємодіяти з людьми та

виконувати складні виробничі завдання. Вони можуть автоматизувати повторювані та небезпечні завдання, підвищуючи ефективність і продуктивність [20].

Широкого розвитку набув промисловий Інтернет речей (IIoT), який відноситься до мережі взаємопов'язаних пристроїв, машин і систем в промисловому середовищі. IIoT дозволяє здійснювати моніторинг і контроль виробничих процесів в режимі реального часу, полегшує обмін даними між машинами і системами, а також забезпечує прогнозоване технічне обслуговування. Це допомагає оптимізувати виробництво, знизити витрати і підвищити загальну операційну ефективність [21].

Хмарні обчислення відіграють важливу роль у цифровому виробництві. Хмарні виробничі платформи забезпечують централізовану інфраструктуру для зберігання, аналізу та доступу до даних. Вони уможливають співпрацю, віддалений моніторинг та обмін даними в режимі реального часу між різними зацікавленими сторонами. Хмарне виробництво також пропонує масштабованість, економічну ефективність і гнучкість для розподілу ресурсів та оптимізації процесів.

За прогнозами ВЕФ (Всесвітнього економічного форуму), більшість технологій Четвертої революції стануть звичайними у 2027 році. Це означає, що будуть не лише розумні будинки, а й розумні міста, безпілотні автомобілі на вулицях, штучний інтелект, офіси та суперкомп'ютери у кишенях.

### **1.3 Основні принципи цифрового виробництва та Індустрії 4.0**

Основні принципи концепції цифрового виробництва включають:

1. Створення цифрового уявлення фізичного об'єкта, процесу чи системи, що дозволяє у час відстежувати і керувати його станом і характеристиками.
2. Використання цифрових технологій для інтеграції та автоматизації різних виробничих процесів, що збільшує ефективність, точність та швидкість виконання завдань.

3. Збір, аналіз та використання великих обсягів даних для прийняття більш точних рішень, оптимізації процесів та прогнозування майбутніх подій у виробництві.

4. Створення гнучкого виробничого середовища, яке може швидко реагувати на зміни попиту, ринку та технологій.

5. Інтеграція фізичних та цифрових компонентів у єдину систему, де дані та команди передаються між різними пристроями та процесами.

6. Створення мережових зв'язків між різними учасниками виробничого ланцюжка, включаючи постачальників, виробників та споживачів, для покращення координації та комунікації.

Концепція цифрового виробництва дозволяє підприємствам досягти високої ефективності, гнучкості та інноваційності у сучасній промисловості. Вона має потенціал для перетворення традиційних виробничих моделей та створення нових можливостей для зростання та розвитку [23].

Основні принципи Індустрії 4.0 є концепцією та підходами, які визначають цифрову трансформацію та інноваційний розвиток у промисловості. Ось деякі з ключових принципів Індустрії 4.0 [24]:

1. Інтеграція та цифрова зв'язність: Індустрія 4.0 прагне повної інтеграції цифрових технологій і процесів у всьому виробничому ланцюжку, створюючи цифрові платформи та сполучні системи, які дозволяють обмінюватися даними та інформацією між різними пристроями, системами та акторами.

2. Інтелектуалізація та автоматизація: Використання штучного інтелекту (ІІ), машинного навчання та автоматизованих систем стає ключовим аспектом Індустрії 4.0. Це включає в себе розробку самонавчальних та адаптивних систем, здатних приймати автономні рішення та оптимізувати процеси виробництва.

3. Масове налаштування та гнучкість: Індустрія 4.0 прагне масового налаштування та гнучкості виробництва, дозволяючи швидко перемикатися між різними продуктами та варіантами виробництва. Це досягається за рахунок цифрових систем, які можуть налаштовуватися та адаптуватися до різних вимог виробництва.

4. Поділ знань та децентралізоване прийняття рішень: Індустрія 4.0 ставить акцент на поділ знань та інформації між різними учасниками виробничого процесу. Це дозволяє розподілити системам та пристроям приймати локальні рішення на основі доступних даних, підвищуючи ефективність та гнучкість процесів.

5. Кіберфізичні системи та інтернет речей: Індустрія 4.0 поєднує фізичний та цифровий світ, створюючи кіберфізичні системи, які взаємодіють із фізичним оточенням та обмінюються даними через Інтернет речей (IoT). Це дозволяє контролювати та керувати процесами в реальному часі.

Проте слід зазначити, що конкретні принципи Індустрії 4.0 можуть відрізнятися у різних контекстах та інтерпретаціях. Ці принципи зазвичай застосовуються для опису цілей та основних характеристик цифрової трансформації у промисловості.

Для Індустрії 4.0 характерними є риси [25]:

- кастомізація,
- інтероперабельності,
- візуалізації,
- доступність в режимі реального часу,
- децентралізації,
- модульності.

В даний час відбувається розвиток промисловості, який пов'язаний з тенденціями нової економічної епохи. Це можна спостерігати за стадією проектування товару до його доставки та обслуговування.

Можна виділити наступні особливості розвитку Індустрії 4.0 в європейських країнах [26]:

1) країни Європи першими вступили в гонку Індустрії 4.0. В них сконцентровано досвід передової країни, які розробляють стратегію розвитку Індустрії 4.0;

2) Європейські країни очікують, що виробляється підхід дозволить збільшити продуктивність і зменшити витрати;

3) До труднощів, які виникають, можна віднести: зростання витрат на перекваліфікацію співробітників, необхідність у більшій кількості інвестиції, зростання рівня соціального нерівності та міграція із країн, що розвиваються, у розвинені.

Екосистема Industry 4.0 вимагає інтеграції офісного середовища, а також дослідних і виробничих систем. У деяких середовищах під одним дахом співіснують і офісна, і виробничі системи. Екосистема Industry 4.0 є більш помітною — це конвергенція ІТ-компонентів і ОТ. Промислові системи управління (ICS) перестали бути ізольованими, коли включення ІТ-компонентів у домен ICS стало звичайною практикою [27].

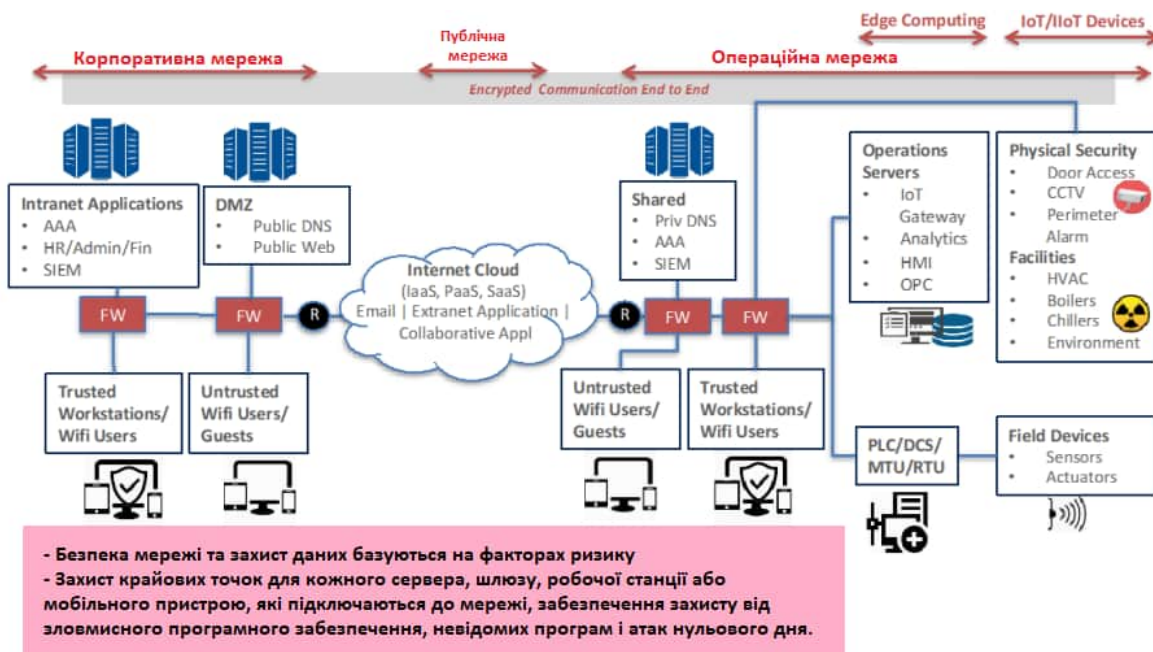


Рисунок 1.4 – Мережева архітектура високого рівня Industry 4.0

На рис. 1.4 зображено мережеву архітектуру високого рівня середовища Industry 4.0, яка складається з корпоративної мережі, загальнодоступної мережі та операційної мережі.

Ця мережева архітектура може бути доречною в середовищі Industry 4.0, наприклад, на виробничих підприємствах, нафтопереробних заводах або Smart City.

## 1.4 Міжнародний досвід розвитку цифрового виробництва та Індустрії

### 4.0

Цифрове виробництво та Індустрія 4.0 є актуальними і важливими концепціями у сучасному світі. Вони сприяють поліпшенню продуктивності, якості та ефективності виробничих процесів.

Країни-лідери, такі як Німеччина, США, Японія та Китай, активно розвивають і впроваджують концепцію цифрового виробництва та Індустрії 4.0. Вони вкладають зусилля у розробку технологій, стандартів та інфраструктури, необхідних для їх успішного впровадження.

На виставці у Ганновері (2011) в Німеччині було вперше представлено поняття "Платформа індустрії 4.0" (Industrie 4.0 Platform). Ця стратегія була запропонована німецьким урядом і промисловими партнерами з метою адаптації німецької промисловості до нової епохи промислових інновацій, яка називається Індустрія 4.0.

Концепція "Платформа індустрії 4.0" передбачає впровадження цифрових технологій, інтернету речей (ІоТ), штучного інтелекту (АІ), аналітики даних та інших інноваційних рішень у виробничі процеси. Це дозволяє створити "розумні" фабрики, де машини, обладнання та системи здатні спілкуватися між собою та з людьми, обмінюватися даними, аналізувати і оптимізувати процеси в реальному часі [28].

Метою "Платформи індустрії 4.0" є забезпечення високої ефективності, гнучкості та індивідуалізації виробництва, зниження витрат та покращення якості продукції. Вона також спрямована на розвиток нових бізнес-моделей та забезпечення конкурентоспроможності німецької промисловості в глобальному ринковому середовищі.

"Платформа індустрії 4.0" стала важливим стратегічним напрямом для розвитку промисловості в Німеччині, а також здобула визнання та інтерес на міжнародному рівні. Її концепція вплинула на розвиток Індустрії 4.0 як глобального руху у сфері промислових інновацій.

Багато країн по всьому світу розробляють власні стратегії та ініціативи, спрямовані на розвиток промисловості в контексті Індустрії 4.0. Ці стратегії можуть мати різні назви, але мають спільну мету - впровадження цифрових технологій та інновацій для покращення ефективності та конкурентоспроможності виробничих процесів.

Наприклад, у Нідерландах існує ініціатива "Smart Industry" або "SmartFactory", спрямована на впровадження цифрових рішень та інновацій у виробничі процеси. У Великій Британії "High Value Manufacturing Catapult" є організацією, яка об'єднує промислові компанії та академічні установи з метою підтримки інновацій та розвитку високотехнологічних виробництв.

Ці стратегії відображають глобальну тенденцію до переходу до цифрового виробництва та використання нових технологій для підвищення продуктивності, якості та конкурентоспроможності промислових секторів. Кожна країна може надавати вагу певним аспектам та розвивати власні підходи, але загальна мета залишається схожою - відповідати вимогам сучасного промислового середовища та забезпечувати стійкий економічний розвиток [28].

У США інтенсифікація розвитку цифрових технологій сприяла створенню Консорціум промислового Інтернету (Industrial Internet Consortium, ІІС) для прискорення впровадження Індустрії 4.0. Це об'єднання підприємств, академічних установ, виробників обладнання та інших зацікавлених сторін з метою спільної роботи над розвитком та стандартизацією промислових інтернет-технологій.

Основна мета Консорціуму промислового Інтернету - створення відкритої платформи та розробка стандартів для побудови надійних, безпечних та ефективних систем промислового Інтернету. Члени консорціуму співпрацюють над розробкою технологічних рішень, випробуванням пілотних проектів, обміном передовим досвідом та співпрацею з академічними та дослідницькими установами.

Участь у Консорціумі промислового Інтернету дозволяє підприємствам США отримати доступ до передових технологій, стандартів та нормативів, що допомагає їм перебудувати виробничі процеси, забезпечити високу якість

продукції та оптимізувати витрати. Консорціум також сприяє обміну знаннями та передовим досвідом між учасниками, що сприяє прискоренню інноваційного розвитку та росту промисловості в США.

Головними цілями Консорціуму виступають [29]:

- стимулювання інновацій;
- визначення та розробка структури;
- сприяння відкритим форумам передачі знань, обмін досвідом, практикою;
- зміцнення довіри до нових інноваційних підходів у сфері безпеки.

Платформи «Індустрія 4.0» та «Інтернет-консорціум» співпрацюють одна з одною на постійній основі. Але слід зазначити, що стратегія розвитку промисловості США більшою мірою орієнтується підвищення рівня продуктивності при зниженні рівня витрат за виробництво.

Основними позитивними результатами, очікуваними США від реалізації виробленої ними політики, можна назвати:

- збільшення прибутку від діяльності підприємств,
- збільшення інвестицій у цифрові технології та зниження їх вартості;
- аналогічно країнам Європейського союзу США змушена збільшити вкладення підвищення рівня цифрової культури населення.

Декілька міжнародних організацій активно працюють із концепцією цифрового виробництва та Індустрії 4.0 та просувають її:

1. Всесвітній економічний форум (WEF, World Economic Forum) є міжнародною організацією, яка залучає політичних, ділових та академічних лідерів до формування глобальних планів. Він має спеціальну ініціативу під назвою «Спільнота передового виробництва та виробництва», яка зосереджена на дослідженні потенціалу цифрових виробничих технологій та їх впливу на галузі та економіку.

2. Міжнародна електротехнічна комісія (IEC, International Electrotechnical Commission) є глобальною організацією, яка розробляє та публікує міжнародні стандарти для електричних та електронних технологій, у тому числі тих, що стосуються цифрового виробництва. Вони відіграють життєво важливу роль у

забезпеченні взаємодії, сумісності та безпеки під час впровадження технологій Індустрії 4.0.

3. Міжнародна організація зі стандартизації (ISO, International Organization for Standardization) є незалежною неурядовою міжнародною організацією, яка розробляє та публікує стандарти для різних галузей. Вони розробили кілька стандартів, пов'язаних із цифровим виробництвом і Індустрією 4.0, наприклад ISO 18451 (Системи промислової автоматизації та інтеграція) та ISO 20282 (Безпека машин).

4. Національний інститут стандартів і технологій (NIST, National Institute of Standards and Technology) є федеральним агентством США, яке сприяє інноваціям і промисловій конкурентоспроможності шляхом розробки та застосування стандартів і технологій вимірювання. Вони мають програми, орієнтовані на передове виробництво та Індустрію 4.0, спрямовані на сприяння прийняттю та інтеграції цифрових технологій у виробничі процеси.

5. Агентство Європейського Союзу з кібербезпеки (ENISA, European Union Agency for Cybersecurity), яке зосереджено на посиленні кібербезпеки в Європі. Вони активно працюють над вирішенням проблем кібербезпеки, пов'язаних із цифровим виробництвом і Індустрією 4.0, надаючи вказівки, передові практики та сприяючи обізнаності щодо кібербезпеки.

6. Організація промислового розвитку ООН (UNIDO, United Nations Industrial Development Organization) є спеціалізованою агенцією ООН, яка сприяє промислового розвитку для зменшення бідності, інклюзивної глобалізації та екологічної стійкості. Вони підтримують прийняття та впровадження цифрових виробничих технологій у країнах, що розвиваються, з метою підвищення їхнього промислового потенціалу.

Ці організації відіграють важливу роль у сприянні впровадження, стандартизації та безпеки цифрового виробництва та технологій Індустрії 4.0 у глобальному масштабі. Вони сприяють розвитку структур, найкращих практик і співпраці між зацікавленими сторонами галузі для забезпечення успішної реалізації цих концепцій у різних секторах по всьому світу.

Концепція цифрового виробництва та Індустрії 4.0 має глобальне значення і отримала визнання в різних країнах світу.

Ключові країни, такі як Німеччина, США, Японія та Китай, активно розвивають та впроваджують концепцію цифрового виробництва та Індустрії 4.0. Вони вкладають значні зусилля у розвиток цифрових технологій, інноваційних платформ та стандартів для підтримки цього процесу.

Країни, які раніше були відстаючими у промисловому розвитку, такі як Корея, Індія, Бразилія та Нідерланди, активно надають пріоритет цифровому виробництву та Індустрії 4.0. Вони впроваджують політики та програми, спрямовані на підтримку цифрової трансформації своїх промислових секторів.

Уряди та промислові асоціації в різних країнах сприяють розвитку та впровадженню цифрового виробництва та Індустрії 4.0 шляхом створення сприятливого середовища для інновацій, фінансової підтримки та співпраці між промисловими секторами.

Одні з найуспішніших прикладів впровадження цифрового виробництва та Індустрії 4.0 спостерігаються у секторах автомобільної промисловості, машинобудування, електроніки та медичного обладнання. Ці галузі демонструють великий потенціал для поліпшення продуктивності, якості та ефективності завдяки використанню цифрових технологій.

Співпраця між університетами, дослідницькими центрами та приватним сектором відіграє важливу роль у розвитку та впровадженні цифрового виробництва та Індустрії 4.0. Це стимулює інновації, обмін знаннями та розробку нових технологій.

Усі ці фактори свідчать про широке визнання і впровадження концепції цифрового виробництва та Індустрії 4.0 в різних країнах. Важливо продовжувати дослідження, сприяти інноваціям та співпраці між країнами, щоб максимально використати потенціал цих технологій у розвитку промисловості та підвищенні її конкурентоспроможності [30].

## Висновки по розділу 1

В розділі обґрунтовано важливість і актуальність питань впровадження та захисту цифрової трансформації виробництва в рамках концепції цифрового виробництва та Індустрії 4.0. Ці дослідження виявили, що цифрова трансформація виробництва може мати значний вплив на підприємства, їхню конкурентоспроможність та ефективність.

Концепція цифрового виробництва та Індустрії 4.0 передбачає використання цифрових технологій, інтернету речей, штучного інтелекту та інших інноваційних рішень для покращення ефективності та конкурентоспроможності виробничих процесів.

Основні принципи концепції цифрового виробництва та Індустрії 4.0 включають цифрову інтеграцію, гнучкість та адаптивність, автоматизацію та автономію, аналітику даних та прийняття рішень на основі даних.

Аналіз міжнародного досвіду показав, що цифрове виробництво та Індустрія 4.0 мають великий потенціал для зміни промислового сектору, які стають основою для підвищення конкурентоспроможності країн, покращення якості продукції та ефективності виробничих процесів. Продовження співпраці, обміну досвідом та розробки нових технологій є ключовими факторами для успішного впровадження цих концепцій у всьому світі.

Однак, разом з потенціалом і перевагами цифрової трансформації, виникають і нові виклики та ризики, пов'язані з безпекою та захистом цифрових систем і даних. У зв'язку зі зростаючим підключенням промислових систем до Інтернету, стає важливим забезпечення кібербезпеки, щоб запобігти несанкціонованому доступу, атакам злочинців та втраті конфіденційності, цілісності та доступності даних.

## РОЗДІЛ 2.

### ДОСЛІДЖЕННЯ РОЛІ КІБЕРЗАХИСТУ ЦИФРОВОГО ВИРОБНИЦТВА

#### 2.1 Основні поняття кібербезпеки в контексті цифрового виробництва та Індустрії 4.0

Для забезпечення кібербезпеки у цифровому виробництві збирається вся інформації від заводу, клієнтів, ланцюгів постачання та якості, щоб переконатися, що справа стосується саме захисту. У 2019 році було зареєстровано 3800 витоків даних. Ці розкриті 4,1 мільярда записів і витоків даних зросли на 54% порівняно з 2018 роком.

За даними IBM та Poneman Institute, кожне порушення даних коштує 3,9 мільйона доларів. Зрозумійте, що ваша компанія повинна захищати широкую мережу комп'ютерів і систем, тоді як хакер повинен знайти лише найслабшу ланку, щоб увійти в мережу.

Це ускладнюється тим, що життєвий цикл обладнання триває приблизно від 26 до 34 років. Деяке з цього обладнання все ще використовує Windows XP, яка не підтримується з 2014 року!

У попередній публікації в блозі я згадував, що багато дій у ланцюзі поставок відбуватимуться за допомогою технології блокчейн. Усі комп'ютери, які складатимуть мережу постачання, будуть називатися DSN або цифровою мережею постачання. Постійний зв'язок через цю широкую мережу DSN означає, що буде багато можливостей для зовнішнього доступу. Кібербезпека буде ключовою для захисту ланцюжка поставок.

Ми всі знайомі з ІТ або інформаційними технологіями. Інфраструктура для збору інформації з цеху буде називатися ОТ або Operational Technology. У Industry 4.0 ці технології повинні будуть взаємодіяти та працювати разом, щоб захистити вашу інтелектуальну власність або інтелектуальну власність. Для більшості виробників це інформація, яку шукає хакер.

Креслення, програми, патенти, комерційні секрети — все це артефакти, які спокушають сторонніх хакерів. Ця інфографіка пояснює, як хакери можуть проникнути в систему.

Зовнішні атаки, зосереджені на ІТ-системах, системі ОТ і виробничих системах, у разі успіху можуть надати доступ до інтелектуальної власності (2.1).

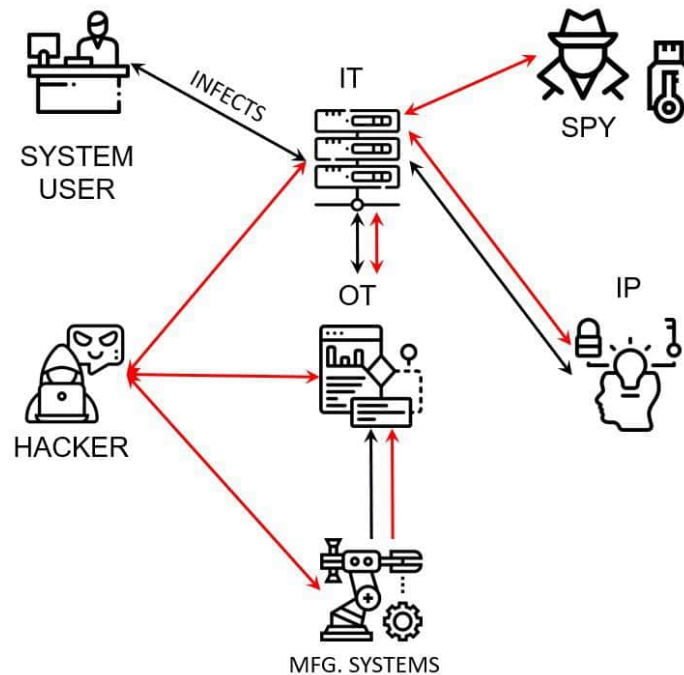


Рисунок 2.1 – Схема атаки

У своєму дослідженні я хочу зазначити, що один із найпростіших способів проникнути у ваші системи — це шкідливі файли CAD. Ці CAD-файли використовують сценарій Visual Basic для послаблення безпеки для майбутніх атак. Вони також використовуються для крадіжки інтелектуальної власності. Вони можуть шукати певні розширення файлів на сервері електронної пошти та направляти ці файли на додаткову адресу електронної пошти. Це призводить до того, що щорічно виробляється підроблена продукція на суму 250 мільярдів доларів.

Ось п'ять основних кроків, які ви можете зробити, щоб захистити свої системи:

1. Обмежте доступ і дозволи користувача.
2. Застосуйте обмеження домену та мережі.
3. Облік активів, підключених до ІТ-систем.
4. Проводити навчання користувачів.

Навчіть співробітників важливості захисту документів, які містять інтелектуальну власність і конфіденційну інформацію.

#### 5. Зробіть безпеку вимогою, пріоритетом.

Апаратно-технічні засоби мають поєднувати вимірювання та керування з виконанням і контролем виробництва. Ці пристрої не тільки будуть об'єднані в мережу, але деякі з них будуть безпосередньо підключені до корпоративної системи, Інтернету та хмарних сервісів, що значно підвищує ризик кібербезпеки в системі.

Саме споживання нових інноваційних продуктів є необхідним для реалізації нижчих переваг Індустрії 4.0. Залежно від того, як хтось прагне скористатися перевагами рішень Industry 4.0, стратегія кібербезпеки буде змінюватися, щоб забезпечити успішне впровадження та масштабування цифрових рішень на виробництві.

Стратегія кібербезпеки також змінюватиметься залежно від того, наскільки поширені цифрові рішення інтегровані на межі промислового циклу управління.

Традиційна архітектура промислової автоматизації дуже розрізнена та покладається на відокремлення керування польовими пристроями від решти інформаційних систем підприємства, послуг і додатків для захисту від загроз кібербезпеці. Фактичні польові пристрої, як правило, є рішеннями «точка-точка» з обмеженим обміном даними та периферійною обробкою, що обмежує ризик кібербезпеки, який будь-який пристрій вносить у систему.

Порушити цю типову архітектуру – непросте завдання, і його необхідно виконувати поетапно. Агресивним прихильникам рішень Industry 4.0 потрібно буде визначити, наскільки глибоко вони хочуть інтегрувати нову технологію на виробництві та керувати стратегією кібербезпеки, яка дозволить реалізувати ці прагнення.

Нова архітектура промислової автоматизації має виглядати значно інакше. Там, де фабрика традиційно сегментується на п'ять різних рівнів за допомогою моделі Перд'ю або подібної, майбутня архітектура фабрики, швидше за все, не буде відповідати тій самій моделі.

## 2.2 Аналіз загроз та вразливостей процесу трансформації цифрового виробництва

Цифрове виробництво, пов'язане з Індустрією 4.0, є сукупністю цифрових технологій, систем і процесів, які можуть бути схильні до різних загроз і атак. Ось огляд деяких типових загроз та атак, пов'язаних із цифровим виробництвом:

**Мальварі та шкідливі програми:** У цифровому виробництві можуть бути використані різні види шкідливих програм, таких як віруси, троянські програми, руткіти та шпигунське програмне забезпечення. Вони можуть бути розгорнуті на пристроях, що контролюють виробничі процеси, і використовуватись для заподіяння шкоди, крадіжки даних або порушення функціональності систем.

**Фішинг та соціальна інженерія:** Атаки фішингу та соціальної інженерії можуть бути спрямовані на працівників та співробітників цифрових виробничих систем. Атакуючі можуть використовувати підроблені листи, веб-сайти або телефонні дзвінки, щоб обдурити користувачів і отримати доступ до їх облікових даних або важливої інформації.

**DDoS-атаки:** Розподілені атаки відмови в обслуговуванні (DDoS) можуть бути спрямовані на цифрові системи виробництва, призводячи до перевантаження мереж чи сервісів та порушення нормальної роботи. Це може призвести до значних простоїв у виробництві та втраті продуктивності.

**Атаки на мережну інфраструктуру:** Цифрове виробництво включає різноманітні мережеві пристрої та комунікаційні мережі. Атаки на інфраструктуру можуть включати сканування портів, перехоплення та заміну даних, а також впровадження зловмисного програмного забезпечення для контролю та вторгнення в системи.

**Фізичні атаки:** Цифрове виробництво також може бути схильне до фізичних атак, таких як фізичне вторгнення в приміщення виробництва або крадіжка обладнання. Атакуючі можуть спробувати перервати процеси виробництва або отримати доступ до конфіденційних даних.

**Атаки на цифровий ланцюжок поставок:** У цифровому виробництві часто використовуються різні постачальники та сторонні системи. Атаки на

цифровий ланцюжок постачання можуть включати компрометацію сторонніх систем або підробку постачальників, що може призвести до надходження шкідливих або неякісних компонентів або матеріалів.

Важливо відзначити, що ці загрози та атаки можуть відрізнятися залежно від конкретних умов та контексту цифрового виробництва. Підприємства повинні застосовувати відповідні заходи безпеки, такі як шифрування даних, багатофакторну автентифікацію, моніторинг та виявлення інцидентів, щоб захистити свої системи та дані від подібних атак.

Цифрова трансформація виробництва приносить значні переваги та можливості, але також створює різноманітні загрози та вразливі місця. Проаналізуємо деякі найпоширеніші загрози і вразливості, пов'язаних із цифровою трансформацією виробництва:

#### 1. Загрози кібербезпеці:

- Зловмисне програмне забезпечення та програми-вимагачі: взаємопов'язана природа цифрових виробничих систем робить їх уразливими до атак зловмисного програмного забезпечення та програм-вимагачів, які можуть порушити роботу, порушити цілісність даних і вимагати фінансову вигоду від організацій.
- Витоки даних: посилене підключення та обмін даними в цифровому виробництві може призвести до витоку даних, коли доступ до конфіденційної інформації, інтелектуальної власності або даних клієнтів здійснюється без авторизації.
- Внутрішні загрози: співробітники або довірені особи з привілейованим доступом до виробничих систем можуть навмисно чи ненавмисно завдати шкоди шляхом зловмисного втручання в системи або випадкового виявлення вразливостей.
- Атаки на ланцюг поставок: цифрове виробництво передбачає складний ланцюг поставок, і атака на постачальника або партнера може мати каскадний вплив на весь виробничий процес.

#### 2. Відсутність безпеки за проектом:

- Застарілі системи: багато існуючих виробничих систем не були розроблені з урахуванням безпеки, що робить їх більш сприйнятливими до атак, оскільки вони інтегровані в цифрове середовище.
- Незахищені конфігурації: неправильна конфігурація цифрових виробничих систем, наприклад слабкі паролі, параметри за замовчуванням або невикористані програмні забезпечення, може зробити їх уразливими для експлуатації.

### 3. Ризики фізичної безпеки:

- Несанкціонований доступ: фізичний доступ до критично важливої виробничої інфраструктури, наприклад виробничих підприємств або диспетчерських, може призвести до підробки, саботажу або викрадення конфіденційної інформації.
- Цілісність ланцюга поставок: цифрова трансформація виробництва передбачає використання різноманітних апаратних і програмних компонентів, що робить вкрай важливим забезпечення автентичності та цілісності цих компонентів, щоб запобігти фізичному втручанню або впровадженню шкідливих елементів.

### 4. Збої в роботі:

- Час простою системи: технічні проблеми, збої програмного забезпечення або кібератаки можуть порушити виробничі процеси, що призведе до значних фінансових втрат і затримок.
- Залежність від технології: надмірна залежність від цифрових систем і автоматизації може створити єдину точку збою, що робить виробництво вразливим до збоїв у разі системних збоїв або зовнішніх факторів.

### 5. Регуляторні ризики та ризики відповідності:

- Невідповідність. Недотримання галузевих норм, законів про захист даних або стандартів кібербезпеки може призвести до юридичних наслідків, репутаційної шкоди та фінансових санкцій.
- Занепокоєння конфіденційністю: цифрова трансформація передбачає збір і обробку величезних обсягів даних, що викликає занепокоєння щодо конфіденційності та безпеки особистої інформації.

Щоб усунути ці загрози та вразливості, організаціям необхідно віддати пріоритет кібербезпеці у своїх ініціативах цифрової трансформації. Це включає впровадження надійних заходів безпеки, таких як сегментація мережі, контроль доступу, шифрування, системи виявлення вторгнень і плани реагування на інциденти.

Регулярні оцінки безпеки, навчання працівників і програми підвищення обізнаності можуть допомогти зменшити ризики, пов'язані з людиною. Співпраця з галузевими партнерами, обмін даними про загрози та постійне оновлення нових технологій і найкращих практик безпеки також мають вирішальне значення для ефективного управління загрозами та вразливими місцями, пов'язаними з цифровою трансформацією виробництва.

### **2.3 Дослідження ризиків трансформації підприємств до цифрових бізнес-моделей у контексті Індустрії 4.0**

Дослідження ризиків, пов'язаних із переходом підприємств на цифрові бізнес-моделі в контексті Індустрії 4.0, є важливою сферою дослідження. Ось кілька ключових аспектів, на які дослідники часто звертають увагу, досліджуючи ризики цифрової трансформації:

1. Ризики кібербезпеки впровадження цифрових технологій і взаємопов'язаний характер систем Індустрії 4.0 створюють нові ризики кібербезпеки. Дослідники аналізують вразливі місця та загрози, з якими можуть зіткнутися організації, зокрема витік даних, несанкціонований доступ, атаки зловмисного програмного забезпечення та потенційний вплив на критичну інфраструктуру. Вони досліджують стратегії пом'якшення цих ризиків, такі як впровадження надійних заходів кібербезпеки, навчання співробітників і постійний моніторинг.

2. Конфіденційність даних і ризики відповідності: цифрова трансформація передбачає збір, зберігання та обробку великих обсягів даних. Дослідники досліджують ризики, пов'язані з конфіденційністю даних і дотриманням нормативних вимог, зокрема щодо таких нормативних актів, як GDPR (Загальний регламент захисту даних) та інших галузевих вимог. Вони

досліджують, як організації можуть забезпечити відповідність, захистити конфіденційні дані та зберегти довіру клієнтів і партнерів.

3. Операційні ризики: цифрова трансформація може порушити існуючі бізнес-процеси та створити нові операційні ризики. Дослідники вивчають такі фактори, як системні збої, проблеми сумісності та залежність від постачальників технологій. Вони оцінюють потенційний вплив на виробничі процеси, управління ланцюгом поставок і загальну безперервність бізнесу. Стратегії пом'якшення можуть включати ретельну оцінку ризиків, планування на випадок непередбачених ситуацій і надійні механізми резервного копіювання та відновлення.

4. Ризики, пов'язані з кваліфікацією та робочою силою: перехід до цифрових бізнес-моделей вимагає нових наборів навичок і можливостей робочої сили. Дослідники досліджують ризики, пов'язані з готовністю робочої сили, і потенційну прогалину в кваліфікації. Вони досліджують стратегії навчання та розвитку, придбання талантів і вплив на робочі ролі та організаційну культуру.

5. Стратегічні ризики. Цифрова трансформація передбачає прийняття стратегічних рішень, які можуть мати довгострокові наслідки для організацій. Дослідники аналізують ризики, пов'язані з вибором технологій, інвестиційними рішеннями, партнерствами та конкурентною динамікою. Вони вивчають стратегії управління ризиками та забезпечення узгодженості цифрових ініціатив із загальними бізнес-цілями.

6. Етичні та суспільні ризики. цифрова трансформація галузей викликає етичні та суспільні занепокоєння. Дослідники вивчають ризики, пов'язані з відповідальним використанням технологій, вплив на зайнятість, цифровий розрив і потенціал соціальної нерівності. Вони досліджують етичні рамки, політичні рекомендації та стратегії сприяння інклюзивності та стійкості в цифрових бізнес-моделях.

Дослідження в цих сферах допомагають організаціям зрозуміти й усунути ризики, пов'язані з цифровою трансформацією в контексті Індустрії 4.0. Отримані результати можуть стати основою для прийняття рішень, стратегій

управління ризиками та розробки найкращих практик для забезпечення успішного впровадження цифрових бізнес-моделей.

## **Висновки по розділу 2**

У розділі було проведено дослідження та оцінка загроз, які впливають на цифрове виробництво, аналіз вразливостей, що можуть бути використані для атак, та оцінку ризиків, пов'язаних з цими аспектами.

Виявлено, що цифрове виробництво піддається різноманітним загрозам, таким як кібератаки, витоки даних, шкідливі програми та інші. Кіберзлочинці можуть навмисно спрямовувати свої атаки на критичні системи, що може призвести до значних втрат для підприємства.

Було виявлено деякі вразливості в інфраструктурі цифрового виробництва, такі як недостатня захищеність мережі, відсутність необхідних заходів безпеки в програмному забезпеченні, використання застарілих технологій тощо. Ці вразливості можуть бути використані зловмисниками для здійснення атак.

## РОЗДІЛ 3.

### АНАЛІЗ КІБЕРЗАХИСТУ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

#### **3.1 Загальна характеристика промислового Інтернету речей (ІоТ) та його особливості**

ІоТ поєднує світ промислових речей (датчики, виконавчі механізми, контролери, роботи тощо) з системами аналітики та зберігання даних. В даний час застосування інтернету речей у промисловості опрацьовується в рамках низки ініціатив, таких як Industry 4.0 та Industrial Internet Consortium. Вони спрямовані на створення нових систем, які виходять за межі можливостей та сфери застосування сучасних систем автоматизації.

На відміну від ІоТ, промисловий інтернет речей призначений для оптимізації виробничих процесів та підвищення ефективності підприємства. Незважаючи на те, що впровадження ІТ-технологій дозволяє зменшити залучення людини у виробництво, говорити про повну роботизацію передчасно. Люди, як і раніше, залишаються ключовим активом підприємства, а поширення ІоТ-технологій дозволить їм працювати не тільки швидше, а й ефективніше.

Цифрові технології допоможуть працівникам підприємства посилити вже наявні навички та виконувати більш складну роботу. Наприклад, оператори бурових установок зможуть керувати обладнанням на відстані у співпраці з інженерами та аналітиками даних, підвищуючи точність та продуктивність бурових робіт.

ІоТ включає взаємопов'язані датчики, прилади та інші пристрої, об'єднані в мережу з комп'ютерами за допомогою промислових застосувань. Такий зв'язок дозволяє збирати, аналізувати дані, обмінюватися ними, що потенційно сприяє підвищенню продуктивності праці та ефективності виробництва, а також забезпечує інші економічні переваги [37].

ІоТ - це еволюція розподіленої системи управління (DCS), яка дозволяє підвищити автоматизацію за рахунок використання хмарних обчислень для уточнення та оптимізації управління процесами.

ПоТ використовує технології кібербезпеки, хмарні обчислення, периферійні обчислення, мобільні технології, міжбусний зв'язок, 3D-друк, передову робототехніку, аналіз великих даних, Інтернет речей, технологію RFID та когнітивні обчислення [38, 39, 40].

ПоТ успішно застосовується як в соціальній сфері (транспорт, охорона здоров'я, житлово-комунальне господарство), так і в різних галузях. За допомогою ПоТ створюються нові бізнес-моделі, підвищується продуктивність праці, трансформується робоча сила [37].

### **3.2 Архітектура та компоненти промислового ПоТ**

Перенесення ідей IoT на промислове підприємство означає їхнє узгодження та інтеграцію з існуючими системами автоматизації. При переході на ПоТ виробничі системи управління працюють так: велика розподільна система управління (PCU) є складною мережею датчиків, виконавчих механізмів, контролерів і обчислювальних ресурсів.

Нижні рівні PCU, як правило, є автономними та відповідають за управління технологічними процесами в реальному часі, працюючи з високим ступенем безпеки та надійності. На більш високих рівнях реалізуються різні функції нагляду, включаючи випереджувальне і диспетчерське управління, людино-машинні інтерфейси, що забезпечують участь в управлінні операторів.

На верхньому рівні розташовуються засоби безперервного збору та аналізу даних про процеси, а також інструменти планування та складання графіків виробничої діяльності, які передаються на нижні рівні для виконання.

Системи ПоТ часто сприймаються як багаторівнева модульна архітектура цифрових технологій [41]. Рівень пристрою визначається фізичною складовою: CPS, датчик або машина. Мережевий рівень включає фізичні мережеві шини, хмарні обчислення та протоколи зв'язку, які агрегують та транспортують дані на сервісний рівень. Сервісний рівень складається з додатків, які маніпулюють даними і об'єднують їх в інформацію, що відображається на сервісному рівні. приладова панель драйвера [42, 43].

Платформи IoT допомагають підтримувати сумісність між речами та створювати більш складні структури, такі як розподілені обчислення та розподілені програми. Розвиток цифрових технологій в цьому напрямку може привести до створення середовищ розробки програмного забезпечення, розроблених спеціально для IoT. Компанії розробляють технологічні платформи для забезпечення такого типу функціональності для IoT. Розробляються нові платформи, які більш широко використовують штучний інтелект.

Німецька ініціатива Industrie 4.0 передбачає застосування комплексного підходу до імплементації бізнес цілей. Однією з основних особливостей такої парадигми є злиття двох світів, світу інформаційно-комунікаційних технологій (ICT) та світу операційних технологій (OT), тобто технологій автоматизації промислових процесів та виробництв. Останні означаються стандартами, що застосовуються в машинобудуванні, електроніці, електротехніці, автоматизації в цілому. Крім Німеччини інші країни також долучилися до здійснення четвертої промислової революції у себе. Проте, саме концепція Industrie 4.0, яка представлена моделлю Reference Architecture Model Industrie 4.0 (RAMI 4.0), сформована на основі майстерного об'єднання кращих світових практик. З метою формування швидкої відповіді на потреби ринку модель RAMI 4.0 описана німецьким інститутом стандартизації DIN та затверджена шляхом спеціальної нової процедури стандартизації, як DIN SPEC 91345:2016-04. Ця модель сформована з міцних цеглин світового досвіду – найбільш важливих стандартів для виробництва.

Автоматизоване виробництво в концепції Industrie 4.0 бачиться, як взаємодія кіберфізичних компонентів I4.0, який включає в себе актив (Asset) та його віртуальну сутність (цифровий двійник). Поняття фізичного активу присутнє як в стандарті IEC-62264 так і в RAMI 4.0, що робить можливим супроводжувати усі сутності, задіяні у виробництві по їх життєвому циклу. У RAMI4.0 поняття активу значно розширене (включає персонал, стандарти, софт, поширюється і на продукт), тим не менше в загальному розумінні вони з IEC-62264 мають одну основу.

Згідно моделі RAMI 4.0 компонент I4.0 представляється тривимірною моделлю (рис.3.1), яка відображає основні аспекти його діяльності протягом усього життєвого циклу. Перевагою використання такого підходу є чітке та наочне розуміння функції кожного рівня. Визначальною особливістю німецької концепції є організація виробничої діяльності за рахунок об'єднання всіх активів підприємства в єдину I4.0-сумісну мережу, яка не має конкретних меж та може мати урегульований доступ для встановлення з'єднання та здійснення автоматичного обміну інформацією з іншими активами, навіть за межами підприємства.

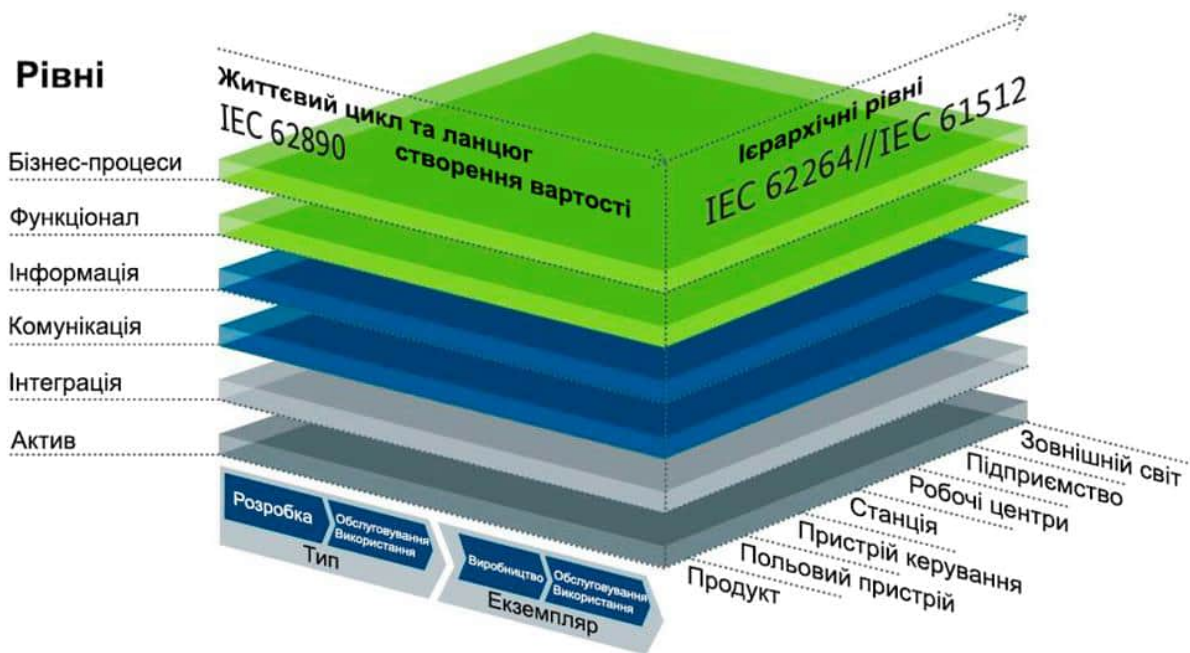


Рисунок 3.1 – Еталонна модель архітектури Industrie 4.0

Промисловий інтернет речей є елементом цифрового виробництва та Індустрії 4.0 і його технологічна архітектура представлена на рис. 3.2.

Промисловий Інтернет речей - це підгрупа технології IoT, яка в основному застосовується в промислових районах, такі як виробничі зручності ПоТ. ПоТ є важливою технологією в Індустрії 4.0, і це прогнозована глава промислової революції. Деякі технології та можливості, що є у Індустрії 4.0 включають штучний інтелект, розумна технологія, взаємозв'язок, та автоматизація даних. Ці технології змінюють повсякденну діяльність промисловості та фабрики.

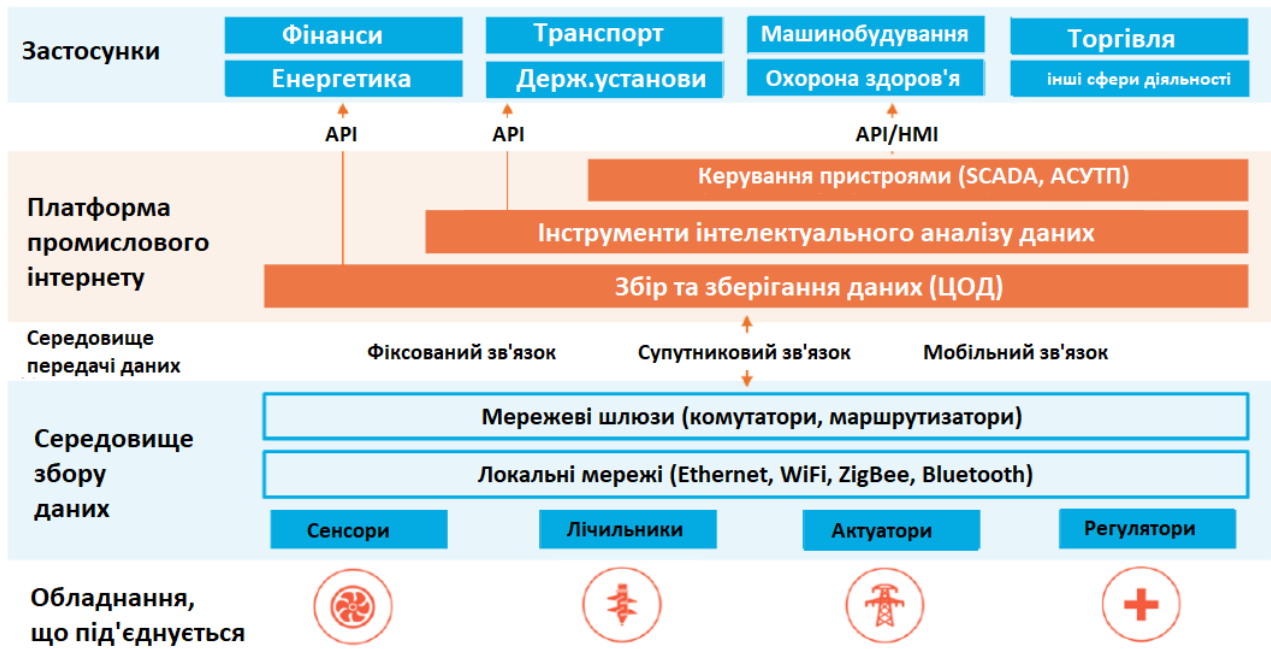


Рисунок 3.2 – Технологічна архітектура IIoT

Як і IoT, IIoT також має значне використання та переваги. Розумні датчики інтегровані з енергетичними системами, виробничі машини, та інфраструктури, такі як проводка та трубопроводи. Ці датчики збирають дані, що підвищують продуктивність, компетентність, та безпеки працівників у промислових умовах.

IIoT покращує передачу даних між двома або більше машинами та пропонує дані керівникам підприємств, що дозволяє їм знати, як працює їхня установка. Коли галузі постійно збирають детальні дані, вони можуть уважно стежити за енергією-водою та іншими необхідними ресурсами. Також, вони можуть визначати, скільки вони виробляють і коли їх машини працюють. Це допомагає операторам вносити корективи вручну або автоматично налаштовувати своє обладнання для покращення своєї роботи.

### 3.3 Питання безпеки технологій промислового Інтернету речей

Оскільки компоненти розумних заводів взаємодіють на базі традиційної IT-інфраструктури, що складається з маршрутизаторів, комутаторів, серверів та пристроїв промислового Інтернету речей (IIoT), для забезпечення її безпеки доцільно застосовувати відпрацьовані за багато років класичні рішення у вигляді

поділу критичних ділянок мережі та інших технічних заходів . Розробляти ці заходи та стежити за їх реалізацією – загальне завдання ІТ- та ОТ-команд.

Перш ніж з'ясувати поточні загрози ПоТ , необхідно визначити технології, які використовуються в цій галузі. У таблиці 3.1 наведені технології ПоТ.

Таблиця 3.1

## Технології промислового Інтернету речей

Технології	Опис
Кінцеві точки ІоТ	Пристрої, оснащені вбудованими технологіями збору, обробки, зберігання, передачі інформації, інтелектуального прийняття рішень
Зв'язок машина-машина (М2М)	Технологія , що полегшує прямий зв'язок між пристрої в мережі без участі людини
Аналіз великих даних	Процес вивчення величезної кількості різних типів наборів даних, відео та аудіо, що генеруються в режимі реального часу розумними датчиками, пристроями, журналами
Робототехніка	Передові промислові роботи, Призначений для вирішення складних завдань інтелектуальні можливості, такі як вміння вчитися на своїх помилках і підвищувати свою продуктивність.
Штучний інтелект	Алгоритми , що дозволяють комп'ютерам і комп'ютери для виконання завдань, які зазвичай виконуються людьми.
Машинне навчання	Алгоритми , що дозволяють комп'ютерам Дійте та покращуйте здатність прогнозувати без явного програмування.
Профілактичне обслуговування	Рішення, які контролюють стан обладнання, прогнозують, коли може статися збій, для ефективного обслуговування з мінімально можливою частотою.
Моніторинг в режимі реального часу	Технології, що дозволяють збирати і об'єднувати дані безпеки з компонентів системи, а також контролювати і аналізувати події, що відбуваються в мережі.
Розширена аналітика збитків	Методи аналізу різних видів втрат, які можуть виникнути в навколишньому середовищі з метою їх усунення або зменшення.
Комп'ютерні обчислення	Рішення, які надають доступ до спільних наборів ресурсів, таких як мережі, сервери та програми, з мінімальними вимогами до керування та взаємодія з постачальником послуг.
Доповнена реальність	Технології, що змінюють сприйняття реального середовища , інструмент підвищення оперативність виконання завдань (наприклад, ручна збірка).

Проблеми ІоТ та ПоТ багато в чому повторюють одна одну. На основі вищевказаних технологій можна виділити ряд проблем безпеки ПоТ.

**Уразливість пристроїв і систем.** З кожним днем кількість нових пристроїв стрімко збільшується. Питання безпеки ПоТ не може бути вирішено ізольовано без забезпечення інших видів безпеки, таких як інформаційна безпека, безпека операційних технологій та фізична безпека. У промислових умовах це може стати істотною проблемою, оскільки більшість систем такого типу проектувалися без урахування вимог безпеки, а тому уразливості в такому обладнанні зустрічаються все частіше.

**Складність управління процесами.** На додаток до великої зони атаки, враховуючи величезну кількість підключених пристроїв, слід розглянути багато складних процесів, пов'язаних з розумним виробництвом. У системах ПоТ контроль процесу представляє проблему безпеки, оскільки функціональність та ефективність пристроїв, як правило, вважаються вищим пріоритетом, ніж безпека.

**Конвергенція інформаційних та операційних технологій (ІТ/ОТ).** Промислові системи управління перестали бути ізольованими після того, як впровадження ІТ-компонентів в промисловість стало звичайною практикою. Конвергенція ІТ-організацій спростила управління складними середовищами, а також внесла нові загрози безпеці. До супутніх факторів можна віднести незахищені мережеві з'єднання (внутрішні і зовнішні), використання технологій з уразливістю, які вносять в середовище ОТ раніше невідомі ризики, і нерозуміння вимог до середовищ АСУ ТП.

**Складність ланцюжка поставок.** Компанії, які виробляють продукцію або рішення, рідко здатні виготовити весь продукт самостійно і зазвичай звертаються до третіх осіб за допомогою у виробництві окремих компонентів. Розробка технологічно складних продуктів призводить до надзвичайно складного ланцюжка поставок за участю великої кількості людей і організацій, що робить його надзвичайно складним з точки зору управління. Неможливість простежити кожен компонент до його джерела означає, що продукт не може бути захищений. Збереження всього продукту оцінюється по його найслабшому (з точки зору безпеки) ланці.

**Мають застарілі промислові системи управління.** Застаріле обладнання є суттєвою перешкодою для впровадження систем безпеки. Виробники встановлюють нові системи поверх застарілих, і це може привести до неефективності попередніх заходів захисту, а також до прояву невідомих вразливостей, які були неактивні протягом багатьох років. Додавання нових пристроїв IoT до застарілого обладнання викликає законні побоювання, оскільки це може дозволити зловмисникам знайти новий спосіб злому систем.

**Незахищені протоколи.** Виробничі компоненти з'єднуються по приватних промислових мережах за певними протоколами. У сучасних мережевих середовищах ці протоколи часто не забезпечують належного захисту від загроз.

**Людський фактор.** Впровадження нових технологій означає, що працівники заводу та інженери повинні застосовувати нові способи роботи з новими типами даних, мереж і систем. Якщо вони не знають про ризики, пов'язані зі збором, обробкою та аналізом даних, вони можуть стати легкою мішенню для зловмисників.

**Невикористовувані функції.** Промислове обладнання призначене для надання великої кількості функцій і послуг, деякі з яких можуть не бути затребувані на окремому виробництві. У промислових умовах машини або їх окремі компоненти часто використовують не весь доступний функціонал, а невикористовувані функції можуть значно розширити сферу потенційної атаки і стати шлюзом для зловмисників.

**Забезпечення збереження виробу після його реалізації.** Безпека пристрою повинна враховуватися протягом усього життєвого циклу виробу, навіть у разі закінчення терміну служби пристрою.

### **3.4. Класифікація загроз промисловому інтернету речей**

Активи промислового Інтернету речей (IIoT) являють собою фізичні та віртуальні компоненти, які входять до складу системи IIoT і є об'єктами, що можуть бути захищені від кібератак. Основними активами IIoT можуть бути:

1. промислові пристрої
2. промислові мережі

3. хмарні сервіси та інфраструктура
4. програмне забезпечення
5. дані та інформація
6. корпоративна інформація:

Промисловими пристроями є фізичні пристрої, такі як датчики, реле, контролери, актуатори, промислові роботи тощо, які забезпечують збір, передачу та обробку даних у промисловій мережі.

Промислові мережі представлені у вигляді фізичної інфраструктури, яка забезпечує зв'язок між промисловими пристроями, включаючи проводові та бездротові мережі, протоколи зв'язку, комутатори, маршрутизатори та інші мережеві компоненти.

ПоТ може використовувати хмарні платформи для зберігання, обробки та аналізу великого обсягу даних, а також для надання додаткових сервісів, таких як машинне навчання та аналітика.

Програмні компоненти в промисловому Інтернеті речей (ПоТ) включають операційні системи, програмні драйвери, програмні бібліотеки та додатки, які керують промисловими пристроями і забезпечують їх функціональні можливості. Ці програмні компоненти взаємодіють між собою, забезпечуючи роботу та функціональність промислових пристроїв в ПоТ. Важливо забезпечити безпеку цих програмних компонентів, оновлювати їх регулярно та впроваджувати механізми захисту, щоб запобігти кіберзагрозам і забезпечити надійну роботу системи ПоТ.

Дані та інформація, що збирається у велику кількість даних, які генеруються та обробляються в системі ПоТ. Ці дані можуть включати вимірювання з датчиків, стан промислових процесів, журнали подій тощо. Інформація, яка отримується з цих даних, може бути використана для прийняття рішень та виконання дій.

Інтеграція промислового Інтернету речей (ПоТ) з корпоративними системами, такими як системи управління виробництвом (MES), системи планування ресурсів підприємства (ERP) та інші, є поширеним сценарієм. Ці системи містять важливу конфіденційну корпоративну інформацію, таку як дані

про виробництво, складський облік, фінансову інформацію, дані про клієнтів тощо.

Захист цієї конфіденційної інформації є важливим аспектом системи ІоТ. Деякі засоби захисту, які можуть бути використані для інтеграції та захисту ІоТ та корпоративних систем

Отже, захист активів ІоТ є критично важливим для забезпечення безпеки та надійності промислових процесів, а також для запобігання витоку конфіденційної інформації та зниження можливостей кіберзлочинців завдати шкоди системі.

На основі виявлених активів була складена класифікація загроз ІоТ, представлена на рис. 3.3.



Рисунок 3.3 - Класифікація загроз ІоТ

Пристрої інтернету речей – це всі пристрої, які мають будь-яку операційну систему, нехай навіть найпростішу, і можуть якимось чином отримувати, обробляти та передавати різноманітні відомості. На побутовому рівні йдеться про системи «розумного будинку» чи камери відеоспостереження, проте інтернет речей поступово поширюється і в міському господарстві, дозволяючи

віддалено знімати свідчення лічильників або, наприклад, керувати мережею світлофорів.

На окрему розмову заслуговує застосування інтернету речей у промисловості. Саме IoT став одним із головних драйверів процесу цифровізації виробництв, яке ще називають переходом до Індустрії 4.0. Новий технологічний стрибок здатний вирішити низку найважливіших завдань: підвищення продуктивності обладнання, зниження матеріальних та енергетичних витрат, підвищення якості, рентабельності виробництва та конкурентоспроможності. Однак на шляху цифровізації є одна неприємна перешкода — вразливість інтернету до кібератак.

Будь-який пристрій, підключений до інтернету, може зазнати хакерських атак. Справа лише у масштабі наслідків.

Зловмисники можуть підключатися до погано захищених мережевих камер — постраждає приватність. Як мінімум. А витік конфіденційних даних може призвести до фінансових втрат. Відомий випадок, коли з локальної мережі казино було викрадено цінну базу даних. Злочинці проникли в неї, використавши як точку входу бездротовий термостат в акваріумі, що стояв у гральному закладі.

Наслідки атак на промисловий інтернет речей можуть бути набагато серйознішими. Інформаційні системи підприємств стають кіберфізичними, тобто мають вихід реальний світ. Зловмисник може отримати контроль над системами, що управляють реальними об'єктами – насосами, реле, двигунами тощо. У найкращому разі наслідком стане зниження продуктивності, а в найгіршому — аварія на виробництві.

Втрати від простою ключової технологічної установки типового нафтопереробного заводу можуть становити мільйон доларів на добу.

Проблема полягає ще й у тому, що промисловий IoT – приваблива мета. Зламавши корпоративну мережу через уразливість в інтернеті речей, у великих компаній можна вимагати серйозних грошей. У всіх, напевно, на слуху торішній випадок з атакою на американського оператора трубопроводу Colonial Pipeline. Через зрив постачання палива в кількох штатах навіть було оголошено режим

надзвичайної ситуації. За чутки, за розблокування обладнання Colonial Pipeline виплатила шантажистам \$5 млн.

І за всіх можливих наслідків IoT залишається «дірявим», тобто вразливим до кібератаків. Більше того, його, в принципі, не завжди можна убезпечити від мережесих загроз.

### **3.5 Стандарти забезпечення безпеки у промисловому Інтернеті речей**

Промисловий Інтернет речей (IIoT) включає в себе використання різноманітних міжнародних та національних стандартів для забезпечення безпеки його структури. Ось деякі з них:

1. ISO/IEC 27001: Це міжнародний стандарт для систем управління інформаційною безпекою. Він надає рекомендації та вимоги для встановлення, впровадження, підтримки та постійного вдосконалення систем управління безпекою інформації в організації.

2. NIST SP 800-53: Цей стандарт розроблений Національним Інститутом Стандартів і Технологій (NIST) у США і визначає набір контролів безпеки інформації для федеральних інформаційних систем. Він може бути використаний для розробки безпекових політик і процедур для структури IIoT.

3. IEC 62443: Цей стандарт розроблений Міжнародною Комісією з Електротехніки (IEC) і має на меті забезпечити безпеку систем автоматизації та управління. Він включає ряд вимог та рекомендацій для захисту мереж, пристроїв та даних в контексті IIoT.

4. GDPR (Загальний регламент з захисту даних): Це регуляторний стандарт Європейського Союзу, який регулює захист персональних даних громадян ЄС. IIoT-структури повинні дотримуватися вимог GDPR, включаючи збір, обробку та зберігання персональних даних.

5. ISA-95: Цей стандарт розроблений Міжнародною Асоціацією Інструментального й Автоматизаційного Контролю (ISA) і визначає модель інтеграції систем керування виробництвом. Він має на меті забезпечити безпеку та надійність обміну даними між системами IIoT.

Ці стандарти представляють лише деякі приклади міжнародних та національних стандартів, які забезпечують безпеку структури промислового Інтернету речей. Реалізація цих стандартів допомагає забезпечити конфіденційність, цілісність та доступність даних, а також захист від шкідливих атак та загроз.

Використання промислового Інтернету речей (IIoT) та безпеки елементів IIoT базується на кількох основних стандартах. Ось деякі з них:

1. MQTT (Message Queuing Telemetry Transport): MQTT є протоколом комунікації, який широко використовується в IIoT для передачі даних між пристроями. Цей протокол має низьку пропускну здатність та малу споживану енергію, що робить його ефективним для використання в обміні даними між обмеженими ресурсами пристроями.

2. CoAP (Constrained Application Protocol): CoAP є іншим легковаговим протоколом для обміну даними в обмеженому середовищі IIoT, де ресурси, такі як пропускну здатність і енергія, обмежені. Цей протокол підтримує безпечний обмін даними і забезпечує надійну комунікацію.

3. OPC UA (Open Platform Communications Unified Architecture): OPC UA є стандартом відкритої платформи комунікаційної архітектури, який використовується в IIoT для побудови забезпечених та надійних зв'язків між пристроями. Він забезпечує стандартизований протокол комунікації та можливість використання різних мережових технологій.

4. TLS (Transport Layer Security): TLS є шифрувальним протоколом, який забезпечує безпечну комунікацію та захист від атак для передачі даних в IIoT. Використання TLS допомагає забезпечити конфіденційність, цілісність та аутентифікацію даних, що передаються між пристроями.

5. IEEE 802.11 (Wi-Fi): Wi-Fi є стандартом бездротового зв'язку, який широко використовується в IIoT для забезпечення безпроводового підключення до мережі. Він забезпечує швидку передачу даних і можливість підключення багатьох пристроїв до однієї мережі.

Ці стандарти допомагають забезпечити ефективну комунікацію між пристроями IIoT, забезпечуючи безпеку, надійність та стандартизований обмін

даними. Проте, варто зазначити, що безпека IoT є комплексним завданням, і вона також включає в себе застосування криптографії, автентифікації, контролю доступу та інших методів захисту даних.

### **Висновки по розділу 3**

У розділі було досліджено архітектуру промислового Інтернету речей (IIoT) і встановлено, що вона складається з мережі фізичних та віртуальних пристроїв, які зв'язані між собою та з центральними системами керування. Ця архітектура забезпечує збір, обробку та передачу даних для підтримки промислових процесів.

Було ідентифіковано різноманітні загрози для промислового Інтернету речей. Ці загрози включають кібератаки на системи IIoT, витоки даних, фізичні атаки на пристрої IIoT, шпигунство та маніпулювання даними, а також використання брешей в безпеці мережі для несанкціонованого доступу.

Аналіз кібербезпеки промислового Інтернету речей (IIoT) показує, що ця технологія стикається з різними загрозами та вразливостями, які можуть бути використані зловмисниками для здійснення кібератак. Для ефективного захисту IIoT необхідно вживати заходів з кібербезпеки, таких як вдосконалення автентифікації та авторизації, захист даних, моніторинг мережі та пристроїв, а також своєчасне виявлення та реагування на потенційні загрози.

## РОЗДІЛ 4.

### РОЗРОБКА ТА НАЛАШТУВАННЯ «SMART GRID» ЗАСОБАМИ CISCO PACKET TRACER

#### 4.1 Поняття «розумних мереж енергозбереження»

«Розумні мережі» або «Smart Grid» - дуже масштабний напрямок у сучасній енергетиці. "Розумна мережа" або "Smart Grid" представляє собою концепцію сучасної енергетики, яка ставить перед собою мету зробити електричні мережі більш ефективними, надійними та стійкими до змінних умов.

Головна ідея полягає в застосуванні передових технологій та інновацій для управління електроенергетичною системою з метою забезпечення оптимального споживання, енергоефективності та інтеграції відновлювальних джерел енергії.

Основні компоненти "розумної мережі" представлені на рис. 4.1.

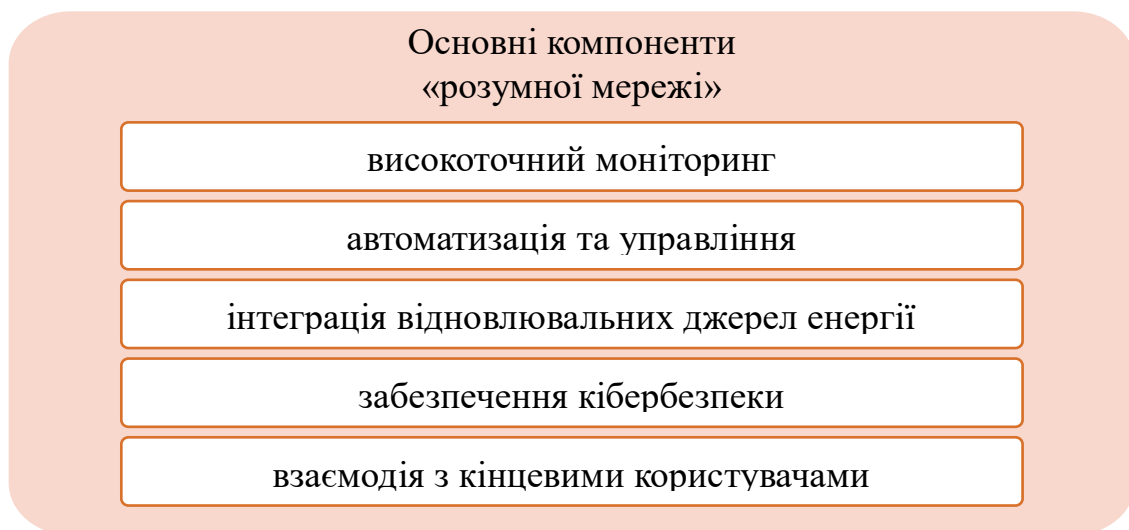


Рисунок 4.1 – Перелік структурних елементів «розумної мережі»

Встановлення сучасних засобів вимірювання та моніторингу, таких як смарт-лічильники, сенсори стану мережі, системи збору даних тощо. Це дозволяє збирати точну інформацію про виробництво, передачу та споживання електроенергії.

Використання розумних алгоритмів та систем управління для оптимізації розподілу енергії, прогнозування навантаження та керування роботою

електричних мереж. Це дозволяє підтримувати стабільність, знижувати втрати енергії та забезпечувати попередження аварійних ситуацій.

"Розумна мережа" сприяє інтеграції відновлювальних джерел енергії, таких як сонячна та вітрова енергія, в електроенергетичну систему. Це дозволяє збільшити енергетичну ефективність та знизити викиди шкідливих речовин.

Враховуючи збільшену кількість з'єднань та цифрових систем у "розумній мережі", забезпечення кібербезпеки стає критично важливим. Необхідно застосовувати заходи безпеки, щоб захистити мережу від зловмисних атак та зберегти надійність та конфіденційність даних.

"Розумна мережа" надає можливості взаємодії між операторами систем енергопостачання та кінцевими користувачами. Це включає можливість моніторингу та керування споживанням електроенергії, тарифними ставками, використанням енергоефективних пристроїв тощо.

Ризики безпеки в "розумній мережі" включають можливість зламу систем, збій у роботі мережі, несанкціонований доступ до конфіденційної інформації, атаки на інфраструктуру мережі, втрату даних та порушення приватності користувачів.

З метою забезпечення безпеки "розумної мережі" необхідно використовувати шифрування даних, мережеві заходи безпеки, аутентифікацію та авторизацію, моніторинг та виявлення вторгнень, планування бізнес-контенту та резервне копіювання даних.

Головна ідея «Smart Grid» полягає у тому, щоб зробити «інтелектуальними» генерацію, передачу та розподіл електричної енергії, наситити електричні мережі сучасними засобами діагностики, електронними системами управління, алгоритмами, технічними пристроями типу обмежувачів струмів короткого замикання надпровідних ліній та багатьом-багатьом сьогодні з'явилося у науці та техніці. Грубо кажучи, це поєднання можливостей інформаційних технологій, вже звичних для нас в Інтернеті, із силовою електротехнікою. І це дає кратне в рази зменшення втрат під час передачі електричної енергії від генератора до споживача, кратне збільшення надійності енергопостачання, дає можливість оптимально перерозподіляти енергетичні

потоки і тим самим зменшити пікові навантаження (а всі електротехнічні системи конструюються саме з розрахунку на пікові навантаження). Це нарешті дає можливість споживачеві працювати на ринку електроенергії. Адже якщо раніше споживач брав електричну енергію від одного продавця, то тепер він перебуває в умовах ринку: може обирати серед компаній, що генерують. У цьому й був сенс реформ в енергетиці – створити конкурентне середовище.

Щоб споживач міг проаналізувати де дешевше купити і взяти енергію, він повинен точно знати, де і за якими цінами вона продається, де сьогодні її надлишок, а де недолік. Відповідно, якщо у компанії-виробника її надлишок, вона повинна знижувати ціни в цьому проявляється економіко-соціальний мотив, якого раніше не було.

Ще одна потреба в Smart Grid пов'язана з так званими відновлюваними джерелами енергії. І в нас, і в Європі багато говорять, що потрібно уникати вуглецевої енергетики, пов'язаної зі спалюванням органічного палива, і переходити на альтернативну енергетику: сонячну, вітрову, водневу тощо. Зокрема це пов'язано також і з розвитком електротранспорту, де необхідно мати розосереджені джерела живлення, зарядки. Але щоб підключати відновлювані джерела енергії у велику мережу і робити їх такими ж об'єктами ринку, як і інші джерела, потрібні ці «розумні мережі» – «Smart Grid».

Є ще стара проблема, пов'язана із споживачами електричної енергії. Наприклад, ви підводите електричну мережу до будинку, де 200 квартир, з яких 20 не платять за електроенергію, інші платять справно. Щоб примусити ці двадцять, ви повинні їх відключити, але для цього ви повинні знати точно, хто не платить і відключити саме «неплатників», при цьому сусідів не відключати.

Сьогодні, на жаль, такої можливості немає, якщо відключають, то весь будинок. Або інше питання: як сьогодні платять за теплову енергію, воду? Обчислюються деякі середні дані, скажімо, по Львову і вам видається рахунок за витрату теплової енергії або води відповідно до цього усередненого показника.

Зрозуміло, правильніше було б поставити лічильник і в реальному масштабі часу дивитися, скільки конкретно ви споживали тепла або води і виставляти вам рахунок на оплату тільки за це. Але щоб так зробити, потрібно

наситити всю систему від генерації до споживача, до розетки в квартирі або на підприємстві розумною електронікою, яка дасть точну інформацію: скільки вам сьогодні електроенергії можуть поставити, за якою ціною.

І ви через керуючу компанію чи самі, якщо здатні це зробити, вибираєте оптимального виробника, а завтра не цього, а іншого. Таким чином, необхідно поєднати засоби діагностики, з одного боку, із сучасними засобами управління з іншого боку, та із засобами прийняття рішень з третьої.

У масштабах країни нам потрібні магістральні чи розподільні мережі, які самостійно можуть контролювати свій стан та режим роботи споживачів, генераторів, електричних ліній та підстанцій та автоматично реалізувати рішення, які дозволяють здійснювати електропостачання безперебійно та з максимальною економічною ефективністю.

Скажімо, «розумна мережа» сама повинна сформувати керуючу дію з досягненням оптимального рівня втрат електроенергії при наростанні перетоків по ЛЕП через зростання споживання якогось великого споживача або цілого енергооб'єднання. Повинні спрацьовувати самодіагностика і самовідновлення, при цьому автоматично повинні виявлятися найслабші ділянки або аварійно-небезпечні елементи мережі і автоматично схема мережі повинна перебудовуватися, щоб уникнути аварії.

Важливим елементом розумної мережі є цифрова підстанція: роботи над подібними проектами ведуться в Європі, США, Японії, Індії, Китаї, в тому числі і в нашій національній мережевій компанії. У такій підстанції вся інформація систем контролю, захисту та управління народжується, переробляється та керується у цифровому форматі за допомогою спеціальних оптичних цифрових вимірювальних трансформаторів та комплексів цифрової апаратури нового покоління.

Якщо підсумовувати, то в найближчому майбутньому електричні мережі повинні бути:

а) гнучкими, щоб прогнозувати можливі зміни, проблеми та реагувати на них;

б) доступними, щоб до них могли підключитися всі користувачі мережі (генератори та споживачі) з пріоритетом відновлюваних джерел енергії, а також таких, що найефективніше використовують вуглеводневі ресурси;

в) надійними, тобто. що забезпечують безпеку та якість електропостачання;

г) економічними – за рахунок нових технологій та ефективного управління мережами;

д) централізоване та місцеве управління в нормальних та в аварійних режимах має бути охоплене адаптивною системою, при цьому оцінка стану та управління в режимі online та offline повинна проводитись із застосуванням швидкодіючих програм.

Існують різницю між російським і західним поглядами в розвитку інтелектуальних мереж. Фахівці на Заході прагнуть упорядкованої взаємопов'язаності функціонування та взаємодії компактно розташованих генеруючих об'єктів, електромереж та споживачів за рахунок інтелектуальних можливостей, відмовостійкості та двостороннього обміну даними на територіально-організаційному рівні муніципальних утворень.

Їх насамперед цікавить можливість підключення невеликих генеруючих джерел електроенергії, адаптація до динаміки споживання та забезпечення економії енергії зі зниженням викиду парникових газів. Вони ринку диктують попит на локальні «розумні мережі»; управлінські завдання на міжрегіональному, національному та міжнародному рівні функціонування енергетичних систем їх турбують поки що менше.

А в Україні енергозабезпечення споживачів відбувається в складних умовах економічного, технічного, природно-кліматичного характеру, ми орієнтуємося на великі об'єкти, що генерують, у нас інший рівень інтегрованості великих систем зі значно вищим рівнем складності системних взаємозв'язків. Відповідно, нам потрібна перебудова всієї глобальної електроенергетичної мережі на принципах багатофункціональної автоматизації.

## 4.2 Проектування мережі

Розумна мережа енергопостачання складається з 1 комп'ютера, смартфона та ноутбука, 1 сервера, 1 комутатора та маршрутизатора, 6 пристроїв енергосистеми, а також інших пристроїв таких як вікно, двері та світлодіоди.

Усі розумні пристрої підключені через комутатор до сервера. Загалом задіяно 11 входів комутатора. На рис. 4.2 представлено серверну стійку з пристроями мережі.

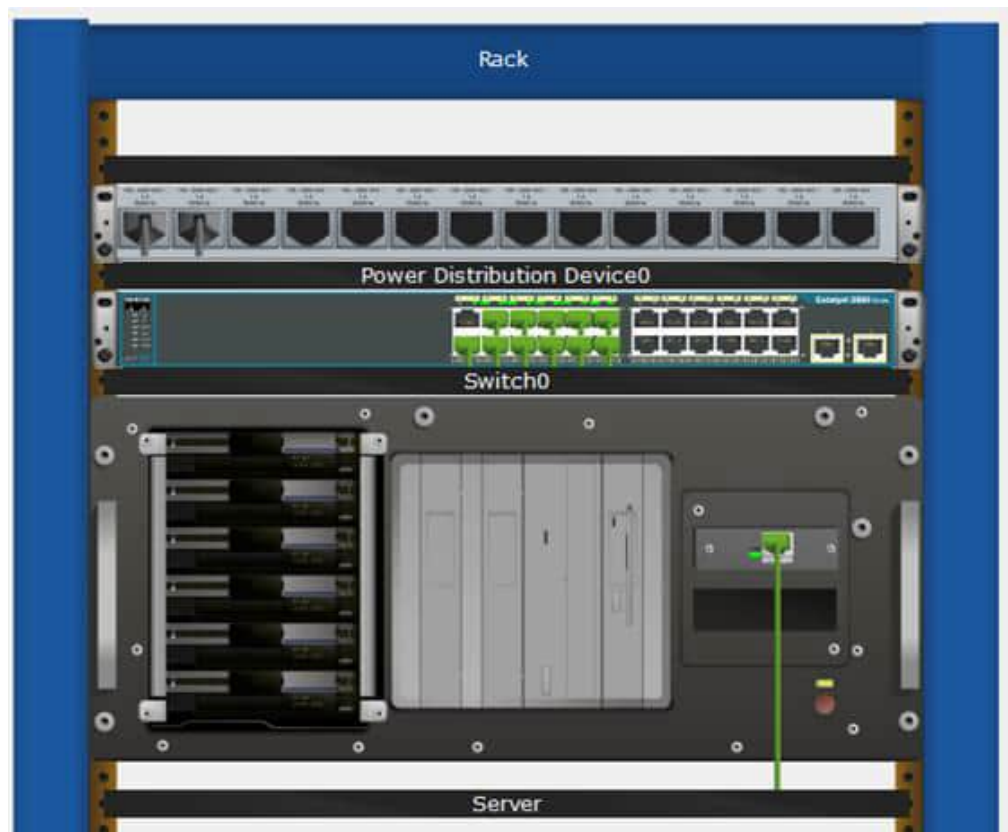


Рисунок 4.2 – Серверна стійка із пристроями мережі

### 4.2.1 Сервіси конфігурації сервера

Зважаючи на вузьку специфіку професійної спрямованості, передбачається мінімум наявність DHCP сервера. Розглянемо й інші можливі варіанти серверів:

1. Файл-сервер. Виділений сервер, призначений для виконання файлових операцій введення-виводу та зберігає файли будь-якого типу.

2. Сервер баз даних. Сервер БД виконує обслуговування та управління базою даних та відповідає за цілісність та збереження даних, а також забезпечує операції введення-виведення при доступі клієнта до інформації.

3. Сервер DNS. Комп'ютерна розподілена система для отримання інформації про домени. Найчастіше використовується для отримання IP-адреси на ім'я хоста (комп'ютера або пристрою), отримання інформації про маршрутизацію пошти, обслуговуючих вузлах для протоколів в домені (SRV-запис).

4. Сервер DHCP. Автоматично видає клієнтам мережі мережеві реквізити у межах заданого діапазону.

В рамках даної роботи було використано мережу з адресами з пулу 10.0.0.0 з максимальним числом користувачів 512. На рис. 4.3 представлена конфігурація мережевих реквізитів DHCP сервера.

5. Web-сервер. Сервер, який приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, і видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потокком або іншими даними.

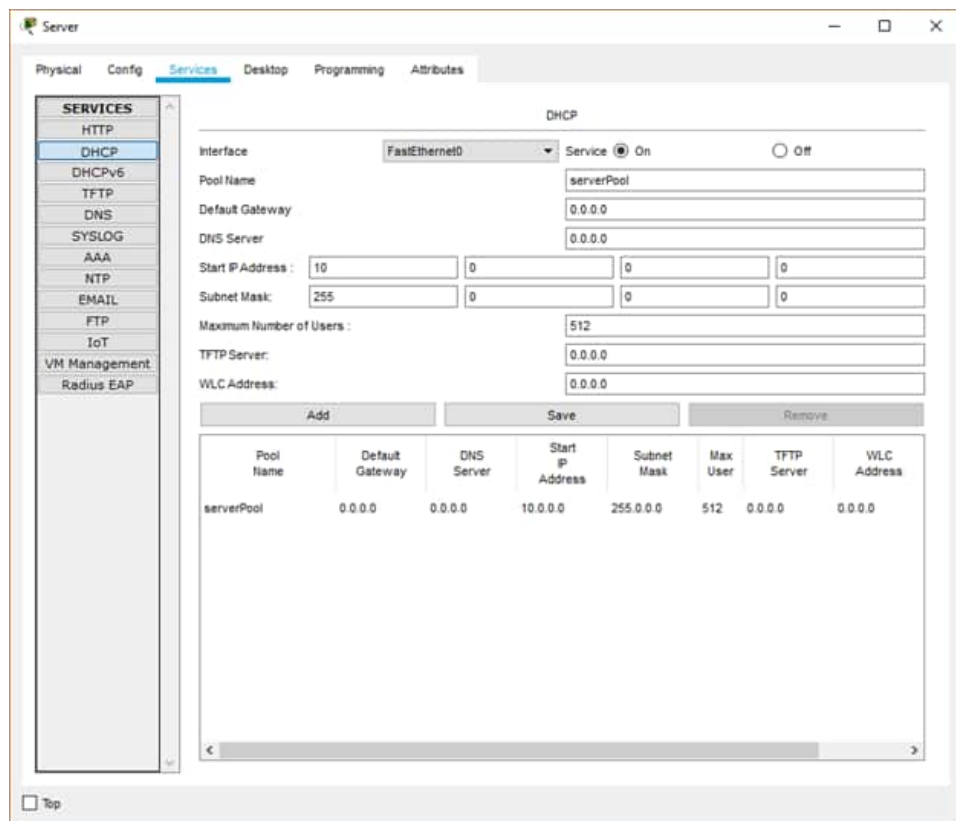


Рисунок 4.3 – Конфігурація мережевих реквізитів сервера DHCP

### 4.2.2 Маршрутизатор

Для управління та моніторингу IoT пристроїв за допомогою сучасних пристроїв таких як смартфони та ноутбуки використовується маршрутизатор.

Маршрутизатор – пристрій, який пересилає пакети між різними сегментами мережі з урахуванням правил і таблиць маршрутизації. Маршрутизатор може пов'язувати різноманітні мережі різних архітектур. Для прийняття рішень про пересилання пакетів використовується інформація про топологію мережі та певні правила, задані адміністратором.

Зазвичай маршрутизатор використовує адресу одержувача, вказану в заголовку пакета, і визначає за таблицею маршрутизації шлях, яким слід передати дані. Якщо в таблиці маршрутизації адреси немає описаного маршруту, пакет відкидається.

Існують інші способи визначення маршруту пересилання пакетів, коли, наприклад, використовується адреса відправника, використовувані протоколи верхніх рівнів та інша інформація, що міститься в заголовках пакетів мережного рівня.

Нерідко маршрутизатори можуть здійснювати трансляцію адрес відправника та одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/дешифрування даних і т.д. Конфігурація мережевих реквізитів маршрутизатора представлена рис. 4.4.

### 4.2.3 Джерела енергії мережі

Джерелами, від яких мережа може отримувати електроенергію, зазвичай є великі підстанції енергосистеми або місцеві електростанції, що входять в енергосистему. В обох випадках у години найбільших навантажень джерело повинне мати необхідний резерв по активній потужності, достатній для підключення додаткових споживачів мережі, що знову проектується.

У розумній мережі енергопостачання цими джерелами є два перетворювачі енергії, а саме сонячна панель і вітряна турбіна які перетворюють сонячну енергію і енергію вітру в постійний електричний струм.

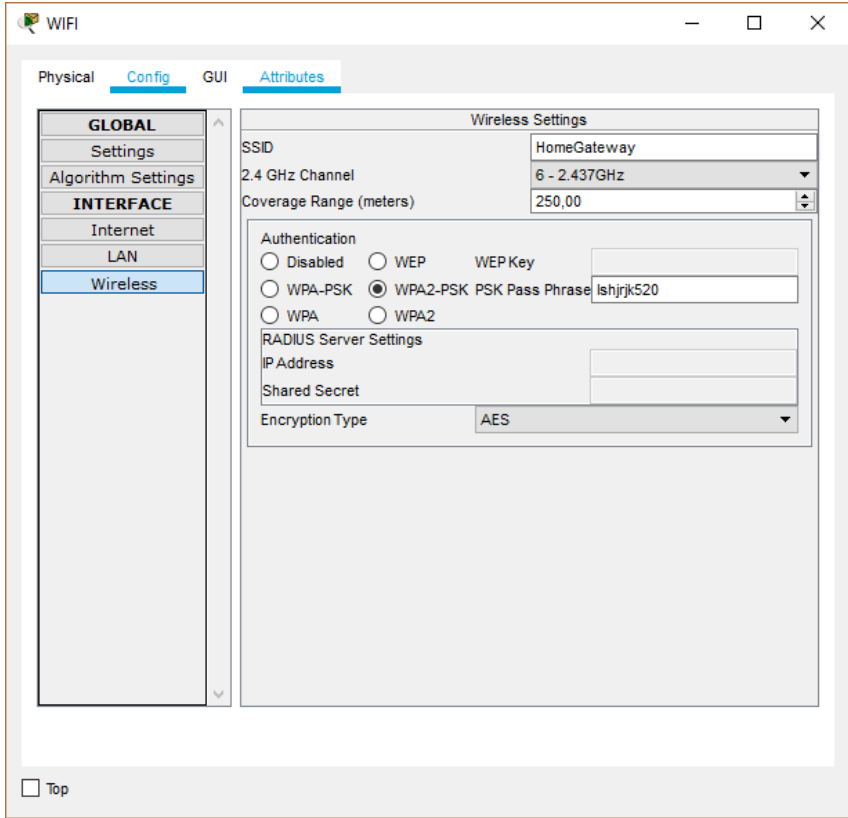


Рисунок 4.4 – Конфігурація мережесих реквізитів маршрутизатора

Запропонована розумна мережа енергопостачання розробляється для невеликого офісу для постійного використання. Спрощена схема мережі представлена рис. 4.5.

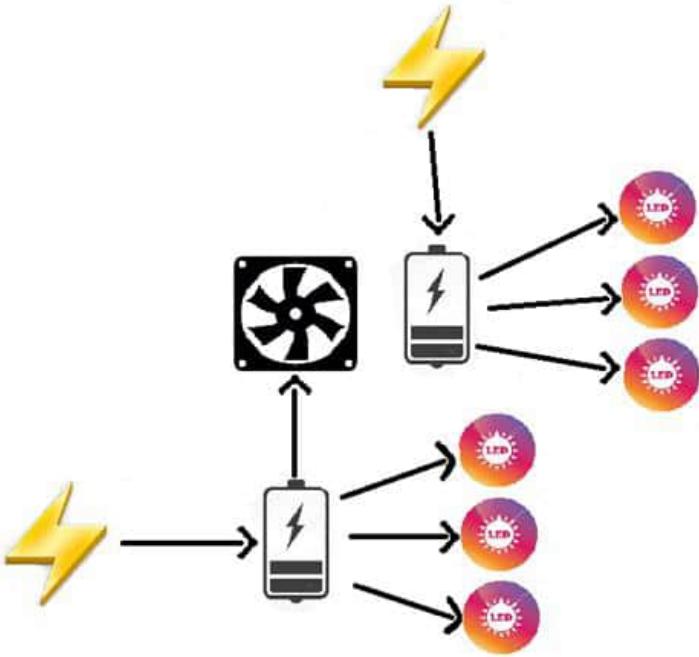


Рисунок 4.5 – Схема мережі енергозбереження

#### 4.2.4 Підключення моніторингу та програмування IoT пристроїв

Для програмування та моніторингу IoT пристроїв необхідно провести їх налаштування, а саме отримати IP-адресу за допомогою DHCP сервера і відповідно підключитися до IoT серверу. Отримання ір має на увазі лише вибір ір configuration між DHCP і Static, а параметри підключення до серверу представлені рис. 4.6.

Оскільки в курсовому проєкті застосовуються IoT пристрої, дуже важливо відстежувати підключені пристрої, мати можливість здійснювати моніторинг та керувати ними. Необхідно гарантувати правильну та безпечну роботу пристроїв IoT після розгортання. Крім того, необхідно забезпечити безпечний доступ до своїх пристроїв, відстежувати їх стан, виявляти та віддалено усувати проблеми, а також керувати оновленнями програмного та мікропрограмного забезпечення.

The screenshot displays the configuration page for a device named "Датчик вєтра" (Wind Sensor). The interface is divided into several sections:

- GLOBAL Settings:** Includes "Settings", "Algorithm Settings", and "Files".
- INTERFACE:** Shows "FastEthernet0" selected.
- Global Settings:**
  - Display Name:** Датчик вєтра
  - Serial Number:** PTT00104VH4-
  - Gateway/DNS IPv4:**
    - DHCP
    - Static
    - Gateway: 0.0.0.0
    - DNS Server: 0.0.0.0
  - Gateway/DNS IPv6:**
    - DHCP
    - Auto Config
    - Static
    - IPv6 Gateway: [empty field]
    - IPv6 DNS Server: [empty field]
  - IoT Server:**
    - None
    - Home Gateway
    - Remote Server
    - Server Address: 10.0.0.1
    - User Name: admin
    - Password: admin
    - Refresh button

At the bottom, there are "Top" and "Advanced" buttons.

Рисунок 4.6 – Загальні налаштування підключення IoT пристроїв

IoT Monitor спрощує безпечне підключення, організацію, моніторинг підключених пристроїв IoT та віддалене керування ними. За допомогою IoT Monitor можна зареєструвати підключені пристрої по одному або пакетному режимі і легко керувати дозволами, щоб пристрої залишалися під надійним захистом. Крім того, ви можете організувати свої пристрої, відстежувати функціональність пристроїв, усувати проблеми, пов'язані з функціональністю, запитувати інформацію про стан будь-якого пристрою IoT [33]. Інтерфейс IoT Monitor представлений малюнку 4.7.

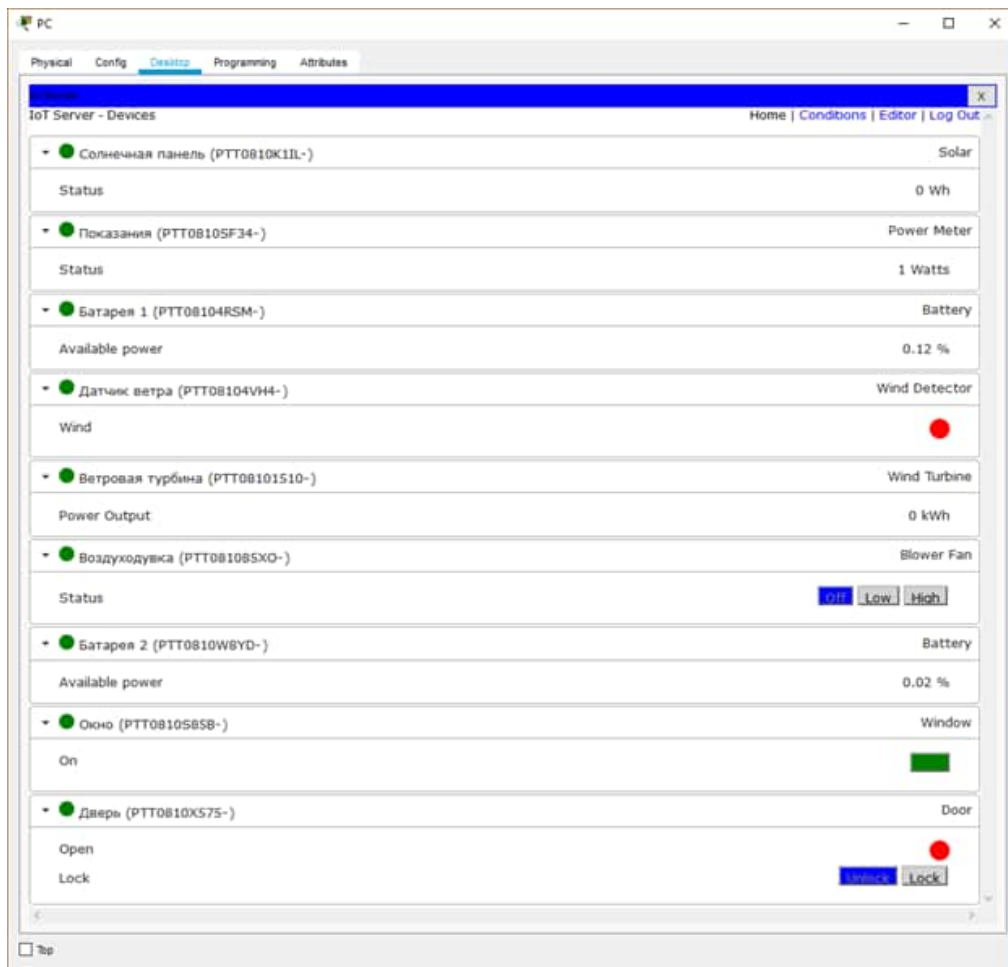


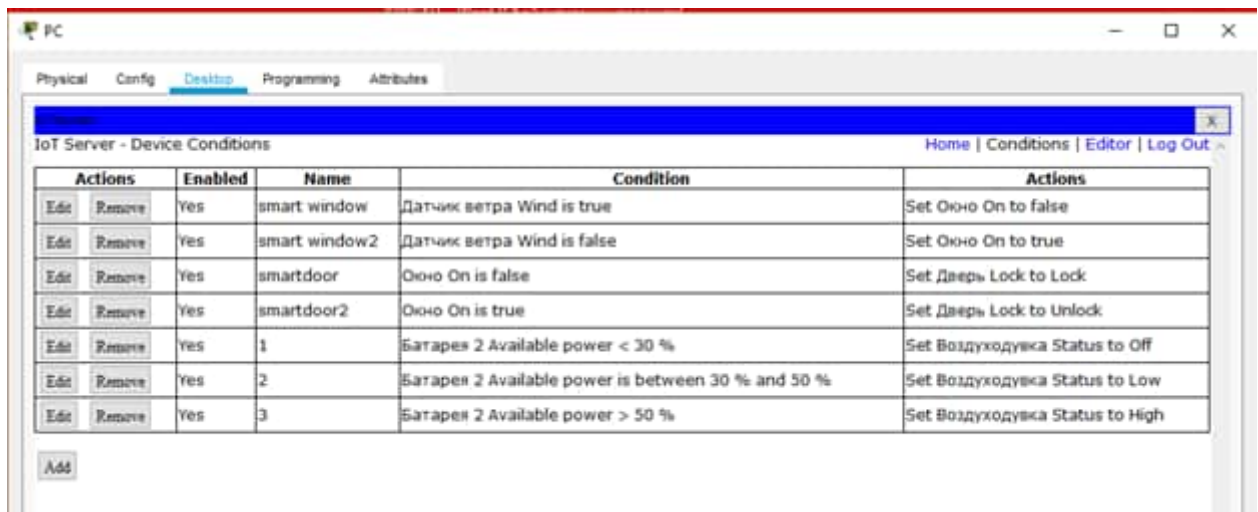
Рисунок 4.7 – IoT Monitor

Технології «розумного будинку» підвищують якість життя споживача, розширюючи можливості звичних пристроїв та предметів - кавоварок, штор, вентиляторів, камер відеоспостереження. IoT conditions надає технології «розумного дому», наділяючи інтелектуальні пристрої новими можливостями, дозволяючи їх програмувати, тим самим задаючи правила роботи в симбіозі. Всі

ці можливості знаходять особливе застосування у ключових прикладах використання «розумного будинку»: автоматизація, безпека, моніторинг і створення домашньої мережі.

Всі ці вимоги прямо або опосередковано можна віднести і до розумної мережі енергопостачання, виходячи із загального становища і спираючись на сукупність усіх вищезазначених і вищезгаданих фактів, було вирішено запрограмувати деякі пристрої [34].

На рис. 4.8 представлено таблицю умов роботи IoT пристроїв.



Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	smart window	Датчик ветра Wind is true	Set Окно On to false
Edit	Remove	Yes	smart window2	Датчик ветра Wind is false	Set Окно On to true
Edit	Remove	Yes	smartdoor	Окно On is false	Set Дверь Lock to Lock
Edit	Remove	Yes	smartdoor2	Окно On is true	Set Дверь Lock to Unlock
Edit	Remove	Yes	1	Батарея 2 Available power < 30 %	Set Воздуходувка Status to Off
Edit	Remove	Yes	2	Батарея 2 Available power is between 30 % and 50 %	Set Воздуходувка Status to Low
Edit	Remove	Yes	3	Батарея 2 Available power > 50 %	Set Воздуходувка Status to High

Рисунок 4.8 – Таблица умов функціонування IoT пристроїв

Загальна схема всього розробленого та реалізованого проекту наведена на рис. 4.9.

### 4.3 Програмне забезпечення мережі

У програмне забезпечення сервера входять:

- операційна система Windows Server 2012;
- антивірусна програма NOD 32 Anti Virus System;
- пакет програм Microsoft Office 2010;
- пакет програм ABBY FineReader Corporate Edition v8.0 (серверна ліцензія);
- програма для адміністрування мережі Symantecpc Anywhere 12 (сервер).

У програмне забезпечення робочої станції входять:

- ОС Windows 10;

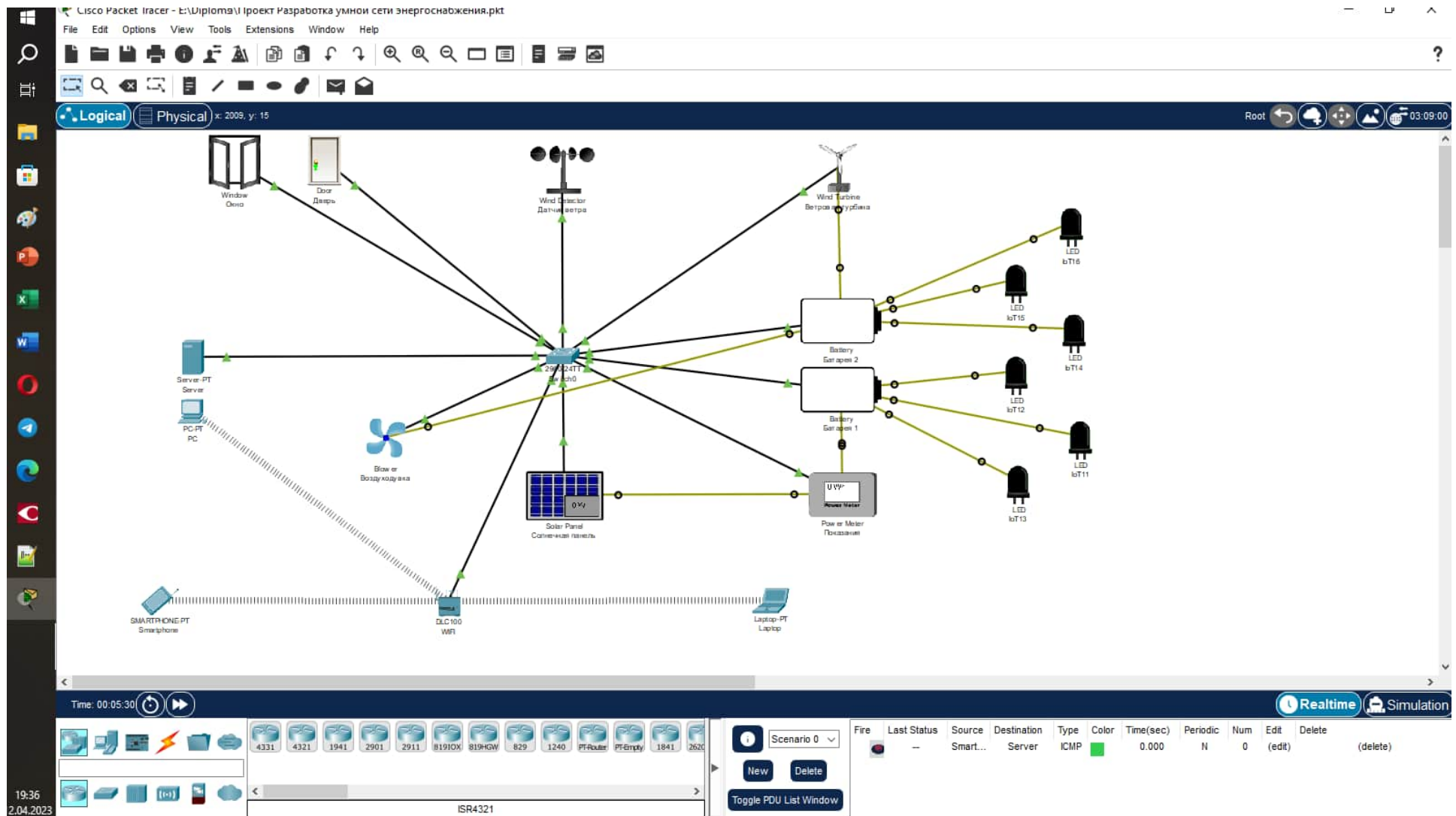


Рисунок 4.9 – Загальна схема проекту «розумна мережа енергоживлення», розроблена у Cisco Packet Tracer

- антивірусна програма AVAST;
- пакет програм Microsoft Office 2010;
- пакет програм ABBY FineReaderCorporateEdition v8.0 (клієнтська ліцензія);
- програма для адміністрування мережі Symantecsc Anywhere 12 (клієнт) довідково-правової системи «Консультант Плюс»;
- програми користувача.

Для моніторингу та захисту від вірусів на сервері встановлено антивірусну програму NOD 32 Anti Virus System. Маючи антивірусну програму на сервері, її необхідно налаштувати так, щоб антивірусна база на клієнтських машинах оновлювалася автоматично і по локальній мережі.

На початку необхідно налаштувати оновлення сервера через інтернет. На сервері відкриваємо вікно програми - NOD 32. Заходимо в розділ: Налаштування>Оновлення, відкриється діалогове вікно "Налаштування автоматичного оновлення", на вкладці "Розташування" натискаємо кнопку "Сервери" і вводимо свій сервер оновлення, який додається до антивірусної системи.

Потім вводимо наше ім'я та пароль, який також йде у поставці до програмного продукту. Другим етапом нам потрібно налаштувати "Дзеркало". Дзеркало це така папка, що знаходиться на сервері, до якої будуть звертатися клієнтські комп'ютери по локальній мережі, для оновлення антивірусних програм. Для цього: на вкладки дзеркало, заходимо до налаштувань. У вікні, ставимо галочку «створити дзеркало оновлення», натискаємо на кнопку «Папка», створюємо папку на диску C:\, прописуємо їй ім'я, наприклад, «NOD obnov», натискаємо Ок. Необхідно зайти в розділ «Додатково» та визначити, який порт використовується для надання файлів через НТТР (2221), натискаємо Ок. На клієнтській машині відкриваємо вікно антивірусної програми > оновлення > Розташування > Сервери > Додати > ://192.168.1.250:2221, тобто прописуємо IP адресу нашого сервера та порт НТТР сервера, натискаємо Ок. Потім зі списку вибираємо наш сервер і натискаємо Ок.

На рис. 4.10 представлені параметри антивірусної програми NOD 32 Anti Virus System.

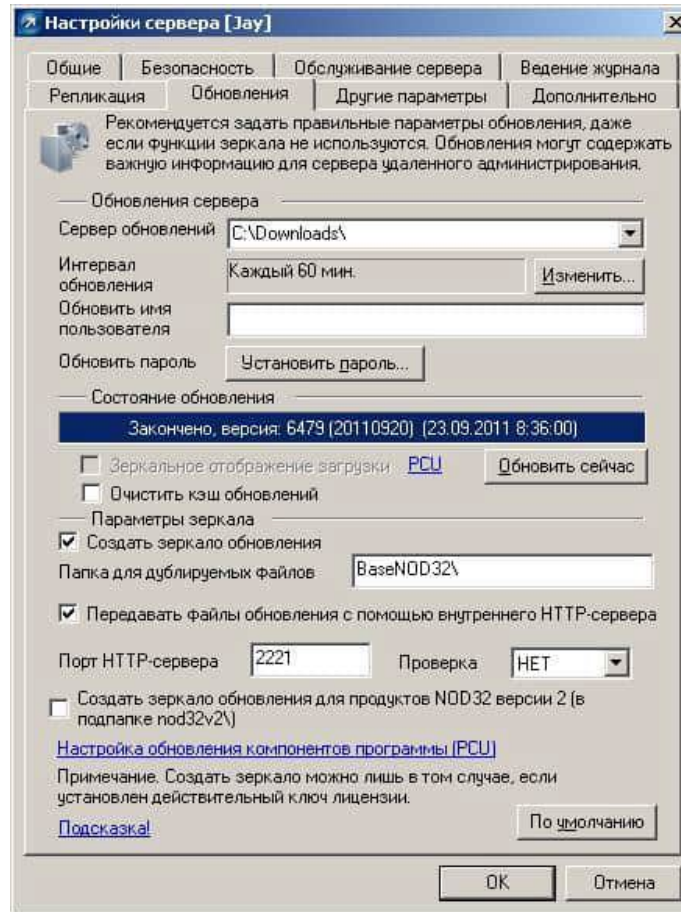


Рисунок 4.10 – Налаштування антивірусної програми

Після встановлення антивірусної програми необхідно налаштувати мережеві параметри.

Наступним кроком є налаштування програми адміністрування мережі Symantecsc Anywhere. Ця програма є найпопулярнішим у світі програмним продуктом для віддаленого керування. Дозволяє ефективно керувати комп'ютерами, швидко усувати неполадки на комп'ютерах користувача, а також просто і безпечно підключатися до віддалених пристроїв.

До нових можливостей продукту відносяться підтримка вбудованої довідкової дошки та ідентифікації за допомогою смарт-карток, при цьому віддалені користувачі можуть знаходити потрібні сервери, підключатися до них та керувати ними. На рис. 4.11 представлено інтерфейс Symantecsc Anywhere 12.

Основні функції ПЗ Symantecsc Anywhere 12:

- Швидке та безпечне підключення до віддалених пристроїв для роботи з користувачами незалежно від розташування.

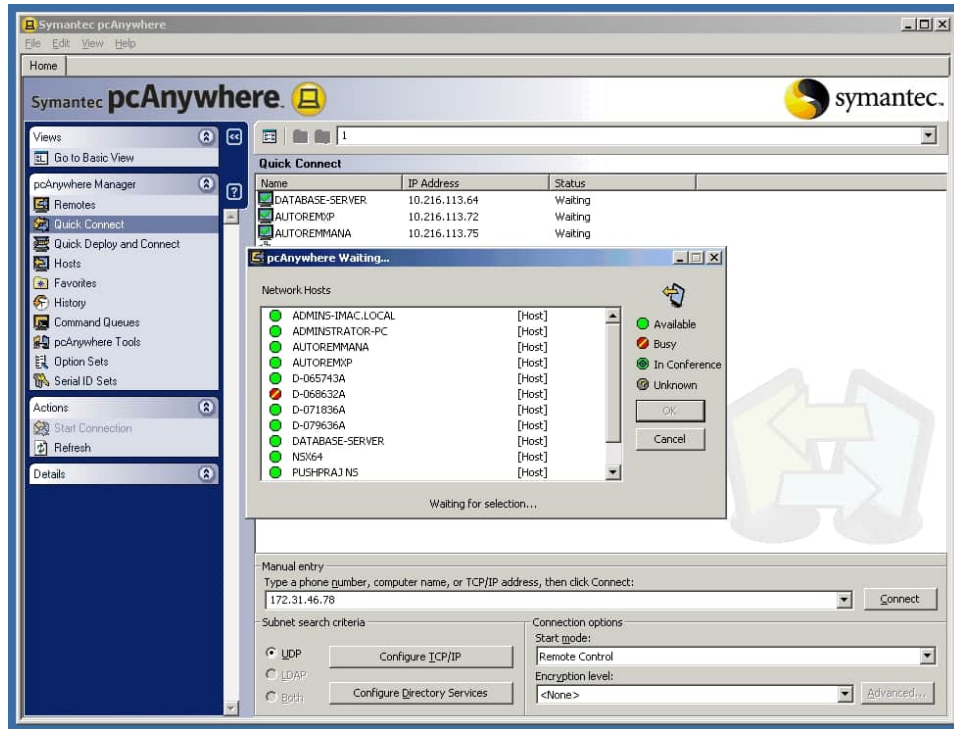


Рисунок 4.11 – Приклад інтерфейсу Symantecpc Anywhere 12

- Керування комп'ютерами з операційними системами Microsoft Windows, Linux, Mac OS X Universal та Microsoft Pocket PC
- Керування комп'ютерами та швидке усунення несправностей на комп'ютерах користувача.
- Дозволяє віддаленим користувачам швидко знаходити сервери за брандмауерами та маршрутизаторами
- Простота у використанні та безпека віддалених з'єднань забезпечується за рахунок застосування нового інтерфейсу Basic View та вбудованого 256-розрядного шифрування AES.
- Функція запрошення сервера (Host Invitation) дозволяє користувачам встановлювати зворотні з'єднання зі службою підтримки, не знаючи її IP-адресу
- Компонент Single Session Manager об'єднує адміністратор pcAnywhere Manager та всі активні сеанси в одне вікно з вкладками
- Дозволяє віддаленим системам Microsoft Windows, Linux, MacOS X Universal та Microsoft Pocket PC підключатися до серверів Windows, Linux та MacOS X Universal

- Майстер підключень допомагає новим користувачам під час встановлення початкового з'єднання "клієнт-сервер"
- Обов'язковий захист за допомогою паролів та шифрування даних при вході гарантують лише санкціонований доступ
- У режимі віддаленого доступу можна використовувати засоби операційної системи хоста.

#### **4.4 Рекомендації щодо захисту розумних мереж енергозбереження**

Для забезпечення кращого розуміння потенційних ризиків і розробки ефективних заходів забезпечення безпеки, розглянемо загрози безпеці розумних мереж енергозбереження.

«Розумні» технології є інноваційними і тому постійно зазнають кібератак з боку зловмисників. Розумні мережі енергозбереження можуть бути піддані різноманітним кібератакам, таким як DDoS-атаки, фішинг, впровадження шкідливих програм або несанкціонований доступ до системи. Ці атаки можуть призвести до перебоїв у роботі мережі, витоку даних або навіть контролю над системою.

Розумні пристрої енергозбереження можуть мати вразливості в програмному забезпеченні або конфігурації, які можуть бути використані зловмисниками для несанкціонованого доступу або маніпуляції з системою. Недостатня аутентифікація, слабкі паролі, відсутність оновлень програмного забезпечення - це лише деякі приклади таких вразливостей.

Недостатні заходи контролю доступу можуть призвести до несанкціонованого доступу до розумної мережі енергозбереження. Якщо зловмисники отримують несанкціонований доступ до системи, вони можуть контролювати роботу пристроїв, змінювати налаштування або навіть впливати на споживання енергії.

Недостатні заходи забезпечення конфіденційності можуть призвести до витоку важливої інформації про розумну мережу енергозбереження. Це може включати дані про споживання енергії, графіки роботи, інформацію про користувачів тощо.

Розумні пристрої енергозбереження можуть бути піддані фізичним атакам, якщо їх не захищено відповідним чином. Фізичний доступ до пристроїв може призвести до їх пошкодження або маніпуляції, що може вплинути на роботу всієї мережі.

Дослідження цих загроз може включати аналіз вразливостей пристроїв, побудову моделей загроз, проведення тестів на проникнення, виявлення аномалій та інші методи. Це допоможе розуміти, які загрози можуть бути актуальними для конкретної розумної мережі енергозбереження і які заходи забезпечення безпеки слід прийняти для їх запобігання або зменшення ризику.

Враховуючи загрози та ризики впровадження та функціонування «розумних» технологій та мереж, можна сформулювати ряд рекомендацій.

1. Забезпечити безпеку мережевого з'єднання. Важливо захистити мережеве з'єднання, яке використовується для зв'язку з розумними пристроями енергозбереження. Використовуйте захищені протоколи комунікації, такі як SSL/TLS, для шифрування передачі даних і запобігання несанкціонованому доступу.

2. Змінити фабричні паролі. Багато розумних пристроїв енергозбереження мають фабричні паролі за замовчуванням, які можуть бути легко вгадані або зламані. Змініть паролі на сильні і унікальні для кожного пристрою, щоб запобігти несанкціонованому доступу до системи.

3. Оновлювати програмне забезпечення. Регулярно оновлюйте програмне забезпечення на розумних пристроях енергозбереження. Виробники часто випускають патчі безпеки, які виправляють виявлені вразливості. Впевніться, що ви встановлюєте всі необхідні оновлення, щоб забезпечити максимальний рівень безпеки.

4. Використовуйте захист від DDoS-атак. Розумні мережі енергозбереження можуть стати ціллю DDoS-атак, які призводять до перебоїв у роботі системи. Встановіть захист від DDoS-атак, який може розпізнавати та фільтрувати надмірний трафік, що надходить до мережі.

5. Моніторинг та виявлення загроз. Встановіть систему моніторингу та виявлення загроз, яка буде надсилати сповіщення про підозрілу або аномальну

активність. Це дозволить вам швидко реагувати на потенційні кіберзагрози та забезпечити безпеку мережі.

6. Навчання персоналу. Забезпечте навчання персоналу з питань кібербезпеки. Всі користувачі та адміністратори повинні бути свідомі загроз, які можуть впливати на розумні мережі енергозбереження, і знати, як правильно поводитись та реагувати на них.

Ці рекомендації допоможуть забезпечити максимальний рівень кібербезпеки для розумних мереж енергозбереження та захистити їх від потенційних загроз. Важливо пам'ятати, що безпека є постійним процесом, і системи мають бути оновлювані та підтримуватись у безпечному стані на протязі всього їх життєвого циклу.

#### **Висновки по розділу 4**

У розділі було проведено роботу з розробки та налаштування проекту "розумної мережі енергозбереження" у середовищі Cisco Packet Tracer. Проект був спроектований з метою впровадження інноваційних технологій та підходів у сучасну енергетичну систему.

У процесі розробки проекту були враховані ключові складові "розумної мережі", такі як високоточний моніторинг, автоматизація та управління, інтеграція відновлювальних джерел енергії, а також забезпечення кібербезпеки.

Було виконано налаштування мережевих пристроїв, встановлено смарт-лічильники та сенсори стану мережі для збору даних про споживання та передачу електроенергії. Також були використані розумні алгоритми та системи управління для оптимізації розподілу енергії та прогнозування навантаження.

Результатом роботи був розроблений та налаштований проект "розумної мережі живлення" у середовищі Cisco Packet Tracer, який демонструє принципи та можливості "розумної мережі" в сучасній енергетиці.

## ВИСНОВКИ

Концепція цифрового виробництва та Індустрії 4.0 передбачає використання цифрових технологій, інтернету речей, штучного інтелекту та інших інноваційних рішень для покращення ефективності та конкурентоспроможності виробничих процесів.

Основні принципи концепції цифрового виробництва та Індустрії 4.0 включають цифрову інтеграцію, гнучкість та адаптивність, автоматизацію та автономію, аналітику даних та прийняття рішень на основі даних.

Аналіз міжнародного досвіду показав, що цифрове виробництво та Індустрія 4.0 мають великий потенціал для зміни промислового сектору, які стають основою для підвищення конкурентоспроможності країн, покращення якості продукції та ефективності виробничих процесів. Продовження співпраці, обміну досвідом та розробки нових технологій є ключовими факторами для успішного впровадження цих концепцій у всьому світі.

Однак, разом з потенціалом і перевагами цифрової трансформації, виникають і нові виклики та ризики, пов'язані з безпекою та захистом цифрових систем і даних. У зв'язку зі зростаючим підключенням промислових систем до Інтернету, стає важливим забезпечення кібербезпеки, щоб запобігти несанкціонованому доступу, атакам злочинців та втраті конфіденційності, цілісності та доступності даних.

Виявлено, що цифрове виробництво піддається різноманітним загрозам, таким як кібератаки, витоки даних, шкідливі програми та інші. Кіберзлочинці можуть навмисно спрямовувати свої атаки на критичні системи, що може призвести до значних втрат для підприємства.

Було виявлено деякі вразливості в інфраструктурі цифрового виробництва, такі як недостатня захищеність мережі, відсутність необхідних заходів безпеки в програмному забезпеченні, використання застарілих технологій тощо. Ці вразливості можуть бути використані зловмисниками для здійснення атак.

У роботі було досліджено архітектуру промислового Інтернету речей (ІІоТ) і встановлено, що вона складається з мережі фізичних та віртуальних

пристроїв, які зв'язані між собою та з центральними системами керування. Ця архітектура забезпечує збір, обробку та передачу даних для підтримки промислових процесів.

Було ідентифіковано різноманітні загрози для промислового Інтернету речей. Ці загрози включають кібератаки на системи ПоТ, витоки даних, фізичні атаки на пристрої ПоТ, шпигунство та маніпулювання даними, а також використання брешей в безпеці мережі для несанкціонованого доступу.

Аналіз кібербезпеки промислового Інтернету речей (ПоТ) показує, що ця технологія стикається з різними загрозами та вразливостями, які можуть бути використані зловмисниками для здійснення кібератак. Для ефективного захисту ПоТ необхідно вживати заходів з кібербезпеки, таких як вдосконалення аутентифікації та авторизації, захист даних, моніторинг мережі та пристроїв, а також своєчасне виявлення та реагування на потенційні загрози.

У роботі було проведено роботу з розробки та налаштування проекту "розумної мережі енергозбереження" у середовищі Cisco Packet Tracer. Проект був спроектований з метою впровадження інноваційних технологій та підходів у сучасну енергетичну систему.

У процесі розробки проекту були враховані ключові складові "розумної мережі", такі як високоточний моніторинг, автоматизація та управління, інтеграція відновлювальних джерел енергії, а також забезпечення кібербезпеки.

Було виконано налаштування мережевих пристроїв, встановлено смарт-лічильники та сенсори стану мережі для збору даних про споживання та передачу електроенергії. Також були використані розумні алгоритми та системи управління для оптимізації розподілу енергії та прогнозування навантаження.

Результатом роботи був розроблений та налаштований проект "розумної мережі живлення" у середовищі Cisco Packet Tracer, який демонструє принципи та можливості "розумної мережі" в сучасній енергетиці.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гірченко, Т.Д., Чмерук, Г.Г., Семенюк, І.М. (2020). Шляхи модернізації цифрової економіки. Інфраструктура ринку, Вип. 41, С. 25–30.
2. Краус, Н.М., Краус, К.М. (2018). Цифровізація в умовах інституційної трансформації економіки: базові складові та інструменти цифрових технологій. Інтелект ХХІ століття, 1, С. 211–214.
3. Краус, Н.М., Краус, К.М. (2018). Сучасні цифрові інформаційно-інноваційні технології в сфері фінансів, управління і адміністрування. Економічна стратегія та політика реалізації європейського вектору розвитку України: концептуальні засади, виклики та протиріччя: монографія. К. : Київський національний університет ім. Т. Шевченка; НДС “Центр економічних досліджень”; ТОВ “СІК ГРУП УКРАЇНА”. С. 469–487.
4. Марченко, О.В., Краус, Н.М., Краус, К.М. (2020). Інноваційне підприємництво і цифровий бізнес: науково-економічна фіча розвитку та зміни в управлінні. Ефективна економіка, 4. Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=7779>.
5. Cybersecurity Challenges in Industry 4.0 //MJP Lopes et al., 2020.
6. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing //J.N. da Silva et al., 2019.
7. Cybersecurity Challenges and Solutions in Digital Manufacturing Era: Industry 4.0 //A. Gökteş et al., 2019.
8. Security and Privacy of Industry 4.0: Challenges and Solutions //Т. К. Das, А. Garza, D. K. P. Levy, M. Wang. IEEE Security & Privacy, vol. 16, no. 4, pp. 8-11, 2018.
9. A Survey of Cybersecurity in Cyber-Physical Systems //M. Saad et al., 2019.
10. D.C. Tien Design and Implementation of Cyber-Physical Systems for Industry 4.0// International Journal of Distributed Sensor Networks, vol. 13, no. 10, 2017.
11. Security Challenges in Cyber-Physical Systems for Smart Manufacturing //S. Biswas, N. Kumar, R. N. Uma, R. Buyya, " Future Generation Computer Systems, vol. 97, pp. 653-668, 2019.

12. Secure Industrial Internet of Things Architecture for Cloud Manufacturing, //J. Shen, H. Chen, G. Wang, J. Li, W. Zou, Future Generation Computer Systems, vol. 87, pp. 389-398, 2018.
13. Secure Industrial Internet of Things for Industry 4.0: A Survey //M.C. Zhou, S.A. Pirbhulal, X.L. Wang, J.G. Zhang. IEEE Access, vol. 6, pp. 78244-78260, 2018.
14. Cyber Security in the Era of Cloud Computing and IoT: Challenges and Opportunities //M.J. Hassan, K. Salah, F. Al-Turjman, Future Generation Computer Systems, vol. 78, pp. 849-861, 2018.
15. Data Security and Privacy Preservation for Cloud-based Industrial Internet of Things //C. Zhang, L. Ren, T. Xie. Journal of Network and Computer Applications, vol. 88, pp. 12-20, 2017.
16. Towards a Secure and Reliable Industrial Internet of Things: A Survey //H.A. Abbasi, M. Younas, M.M. Hassan. Journal of Network and Computer Applications, vol. 135, pp. 62-82, 2019.
17. Industry 4.0 The background to Plattform Industry 4.0. – Режим доступу: <http://www.plattformi40.de/I40/Navigation/EN/ThePlattform/PlattformIndustrie40/plattform-industrie40.html>.
18. When China's 'Made in China 2025' meets Germany's 'Industry 4.0'. – Режим доступу: <http://chinaplus.cri.cn/news/china/9/20170502/3933.html>.
19. Odnorog, M., Kraus, N., Kraus, K. (2019). The features of entrepreneurial interactions in the interactions in the agricultural sector in terms of institutional transformation. Baltic Journal of Economic Studies, 4. pp. 171–181. Режим доступу: <http://www.baltijapublishing.lv/index.php/issue/article/download/720/pdf>
20. Цифрова адженда України – 2020 (“Цифровий порядок денний” – 2020). Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти “цифровізації” України до 2020 року. НІТЕСН office. груд. 2016. 90 с. Режим доступу: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf>
21. Білоус, М. Ю.; Медова, К. Г. Огляд сучасних технологій на прикладі Індустрії 4.0. 2021.
22. Gerrikagoitia, Jon Kepa, et al. Digital manufacturing platforms in the industry 4.0 from private and public perspectives. Applied Sciences, 2019, 9.14: 2934.

23. Chong, Li; Ramakrishna, Seeram; Singh, Sunpreet. A review of digital manufacturing-based hybrid additive manufacturing processes. *The International Journal of Advanced Manufacturing Technology*, 2018, 95: 2281-2300.
24. A. Jacobsson, M. Boldt, and B. Carlsson, "On the risk exposure of smart home automation systems," in *Future Internet of Things and Cloud (FiCloud)*, 2014 International Conference on. IEEE, 2014, pp. 183–190..
25. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015
26. J. Qin, Y. Liu, R. Grosvenor, *A Categorical Framework of Manufacturing for Industry 4.0 and Beyond, Changeable, Agile, Reconfigurable & Virtual Production*, *Procedia CIRP* 52 (2016) 173 – 178.
27. R. Neugebauer, S. Hippmann, M. Leis, M. Landherr, *Industrie 4.0- Form the perspective of applied research*, 49th CIRP conference on Manufacturing systems (CIRP-CMS 2016), 2-7.
28. Четверта промислова революція: зміна напрямів міжнародних інвестиційних потоків: моногр. / за наук. ред. д.е.н., проф. А.І. Крисоватого та д.е.н., проф. О.М. Сохацької. – Тернопіль: Осадца Ю.В., 2018. – 478 с.
29. K.D. Thoben, S. Wiesner, T. Wuest , *Industrie 4.0 and Smart Manufacturing- A Review of Research Issues and Application Examples*, *International Journal of Automation and Technology* Vol.11 No.1, 2017 4-16.
30. *Seizing Industry 4.0 opportunities in Japan*. – Режим доступу: [https://www.businesssweden.se/contentassets/4f2db52dbae148a78e626486d64e7c2b/seizing\\_industry\\_4\\_0\\_in\\_japan.pdf](https://www.businesssweden.se/contentassets/4f2db52dbae148a78e626486d64e7c2b/seizing_industry_4_0_in_japan.pdf)
31. МЕК 61508-1. Функційна безпека електричних / електронних / програмовних електронних систем, пов'язаних із безпекою – Частина 1: Загальні вимоги. Режим доступу: <https://tk185.appau.org.ua/61508/standard-iec-61508/iec-61508-1-ukrainian/>
32. ISO 26262 – *Automotive Functional Safety Training*. Режим доступу: <https://www.sgsgroup.com.ua/en/training-services/industry-based->

- training/automotive-training/automotive-functional-safety-training/iso-26262-automotive-functional-safety-training
33. The digital transformation of industry (A European study commissioned by the Federation of German Industries (BDI) and conducted by Roland Berger Strategy Consultants). URL: [http://bdi.eu/media/user\\_upload/Digital\\_Transformation.pdf](http://bdi.eu/media/user_upload/Digital_Transformation.pdf)
  34. Practical Industrial Programming using IEC 61131-3 for PLCs. IDC Technologies, 2007. 120 p.
  35. Karl Heinz John, Michael Tiegelkamp IEC 61131-3: Programming Industrial Automation Systems: Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids. Springer-Verlag Berl in Heidelberg, 2010. 390 p.
  36. Пупена О. М., Ельперін І. В., Луцька Н. М., Ладанюк А. П. Промислові мережі та інтеграційні технології в автоматизованих системах. Навчальний посібник. — К.: Ліра-К, 2011. — 500с. ISBN 978-966-2174-13-7
  37. The industrial internet of things (IIoT): An analysis framework / Н. Boyes [et al.] // Computers in Industry. 2018. Vol. 101. P. 1–12. <https://doi.org/10.1016/j.compind.2018.04.015>.
  38. Proposal of an automation solutions architecture for Industry 4.0 / М. Saturno [et al.] // 24th International Conference on Production Research (ICPR 2017) : proceedings. Lancaster, U.S.A. : DEStech Publications, Inc., 2017. 7 p. doi:10.12783/dtetr/icpr2017/17675.
  39. Why Edge Computing Is an IIoT Requirement : How edge computing is poised to jumpstart the next industrial revolution // IOT World Today : [site]. 2017. 18th May. Режим доступу: <https://www.iotworldtoday.com/2017/05/18/why-edge-computing-iiot-requirement/>
  40. Erguler I. A potential weakness in RFID-based Internet-of-things systems // Pervasive and Mobile Computing. 2015. Vol. 20. P. 115–126. <https://doi.org/10.1016/j.pmcj.2014.11.001>.
  41. Yoo Y., Henfridsson O., Lyytinen K. Research Commentary – The New Organizing Logic of Digital Innovation: An Agenda for Information Systems

Research // Information Systems Research. 2010. Vol. 21, issue. 4. P. 724–735.  
<https://doi.org/10.1287/isre.1100.0322>

42. Hylving L., Schultze U. Evolving The Modular Layered Architecture in Digital Innovation: The Case of the Car's Instrument Cluster // International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design : proceedings. Milan, 2013. 17 p. Режим доступу: [https://www.researchgate.net/publication/270782497\\_Evolving\\_The\\_Modular\\_Layered\\_Architecture\\_in\\_Digital\\_Innovation\\_The\\_Case\\_of\\_the\\_Car%27s\\_Instrument\\_Cluster](https://www.researchgate.net/publication/270782497_Evolving_The_Modular_Layered_Architecture_in_Digital_Innovation_The_Case_of_the_Car%27s_Instrument_Cluster)
43. Industrial internet of things // 2021. Режим доступу: [https://en.wikipedia.org/wiki/Industrial\\_internet\\_of\\_things](https://en.wikipedia.org/wiki/Industrial_internet_of_things)
44. Smart Grid. Режим доступу: <https://aws.amazon.com/iot-device-management/>
45. Report: Smart Grid Market Could Double in Four Years. Zpryme Smart Grid Market. Архів оригіналу за 6 вересня 2014. Процитовано 6 березня 2016.