МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
_____
(повне найменування факультету)
Кафедра інформаційної безпеки та наноелектроніки
_____
(повне найменування кафедри)

Пояснювальна записка

до дипломної роботи
магістра
(ступінь вищої освіти)

на тему Дослідження та розроблення рекомендацій щодо застосування методів з кібербезпеки в кіберфізичних енергетичних системах
(назва теми)

Виконав: студент 2 курсу, групи БК-813м

Спеціальності 125 - Кібербезпека та захист інформації
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
ПАВЛЕНКО В.М.
(ПРІЗВИЩЕ та ініціали)

Керівник КАРПУКОВ Л.М.
(ПРІЗВИЩЕ та ініціали)
Рецензент МОРОЗ Г. В.
(ПРІЗВИЩЕ та ініціали)

2024

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

Факультет Інформаційної безпеки та електронних комунікацій
Кафедра Інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 - Кібербезпека та захист інформації
(код і найменування)
Освітня програма Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН
Андрій КОРОТУН

«_____» _____20___року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТА
ПАВЛЕНКА Володимира Миколайовича

1. Тема роботи: Дослідження та розроблення рекомендацій щодо застосування методів з кібербезпеки в кіберфізичних енергетичних системах, Research and development of recommendations for the application of cybersecurity methods in cyber-physical energy systems
керівник роботи: д.т.н., професор, КАРПУКОВ Леонід Матвійович,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «05» грудня 2024 року №507
2. Строк подання студентом роботи «10» грудня 2024 року
3. Вихідні дані до роботи: Технічна документація та стандарти кібербезпеки, наукові статті, нормативна база, дані про реальні випадки кібератак, результати моделювання кіберфізичних систем, експериментальні дані з тестування механізмів безпеки

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз стану кібербезпеки в кіберфізичних енергетичних системах, Застосування та методологія кібербезпеки кіберфізичних систем, Розроблення рекомендацій та практичні аспекти застосування методів кібербезпеки в кіберфізичних енергетичних системах

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) 32 рисунки (аналіз стану кібербезпеки кіберфізичних енергетичних систем, методологія забезпечення кібербезпеки, рекомендації забезпечення кібербезпеки). Презентація доповіді (підготовлена в Microsoft Power Point)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	КАРПУКОВ Л.М., професор кафедри ІБтаН	04.09.24	10.12.24
Нормоконтроль	КОРОЛЬКОВ Р.Ю., доцент кафедри ІБтаН		10.12.24

7. Дата видачі завдання «04» вересня_2024_року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз літературних джерел за тематикою дослідження	04.09.24 – 21.09.24	Виконано
2.	Аналіз стану кібербезпеки в кіберфізичних енергетичних системах,	22.09.24 – 07.10.24	Виконано
3.	Застосування та методологія кібербезпеки кіберфізичних систем	08.10.24 – 20.10.24	Виконано
4.	Розроблення рекомендацій щодо кібербезпеки в кіберфізичних енергетичних системах	21.10.24 – 17.11.24	Виконано
5.	Практичні аспекти застосування методів кібербезпеки в кіберфізичних енергетичних системах	18.11.24 – 25.11.24	Виконано
6.	Виконання графічної пояснювальної записки	26.11.24 – 03.12.24	Виконано
7.	Оформлення матеріалів магістерської роботи	04.12.24 – 10.12.24	Виконано

Студент _____ Володимир ПАВЛЕНКО
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ Леонід КАРПУКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 104 с., 12 табл., 8 рис., 1 дод. 79 джерел.

АДАПТИВНІ АЛГОРИТМИ, БЛОКЧЕЙН, ВИЯВЛЕННЯ АНОМАЛІЙ, ЕНЕРГЕТИЧНИЙ СЕКТОР, ЗАХИСТ ДАНИХ, ІНТЕЛЕКТУАЛЬНА МЕРЕЖА, КІБЕРФІЗИЧНІ СИСТЕМИ, ШТУЧНИЙ ІНТЕЛЕКТ

Об'єктом дослідження є процес забезпечення кібербезпеки кіберфізичних енергетичних систем.

Предметом дослідження є методи забезпечення кібербезпеки кіберфізичних енергетичних систем, включаючи адаптивні алгоритми та інтегровані системи моніторингу.

Метою дослідження є розроблення та обґрунтування рекомендацій для впровадження в сучасні методи кібербезпеки за умови підвищення стійкості кіберфізичних енергетичних систем.

Робота присвячена дослідженню актуальних проблем кібербезпеки кіберфізичних систем енергетичного сектора. Проаналізовано загрози та вразливості, запропоновано інноваційні методи виявлення аномалій, використання штучного інтелекту, технологій блокчейну та адаптивних стратегій для підвищення захисту даних і стійкості системи. Результати включають практичні рекомендації та алгоритми для вдосконалення моніторингу кіберфізичних систем енергетичного сектора.

ABSTRACT

Explanatory note to the master's thesis: 104 p., 12 tab., 8 fig., 79 s.

ANOMALY DETECTION, ADAPTIVE ALGORITHMS, ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, CYBER-PHYSICAL SYSTEMS, DATA PROTECTION, ENERGY SECTOR, SMART GRID.

The object of research is the process of ensuring cybersecurity of cyber-physical power systems.

The subject of the study is the methods of ensuring cybersecurity of cyber-physical energy systems, including adaptive algorithms and integrated monitoring systems.

The purpose of the study is to develop and substantiate recommendations for implementation in modern cybersecurity methods to increase the resilience of cyber-physical energy systems.

The paper is devoted to the study of current issues of cybersecurity of cyber-physical systems in the energy sector. Threats and vulnerabilities are analysed, and innovative methods of anomaly detection, artificial intelligence, blockchain technologies, and adaptive strategies are proposed to improve data protection and system resilience. The results include practical recommendations and algorithms for improving the monitoring of cyber-physical systems in the energy sector.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КФС - Кіберфізична система

КФЕС - Кіберфізична енергетична система

ПЗ - програмне забезпечення;

ПКС - Промислові кіберфізичні системи

ПЛК - Програмований логічний контролер

ADP - Adaptive Dynamic Programming - Адаптивне динамічне програмування

AI, ШІ - Artificial Intelligence - Штучний інтелект

AMI - Advanced Metering Infrastructure - Вдосконалена інфраструктура обліку

AMI-SER - Advanced Metering Infrastructure Security Requirements - Вимоги до системи безпеки вдосконаленої інфраструктури обліку

CIP - Critical Infrastructure Охорона - Захист критичної інфраструктури

COVID-19 - Coronavirus Disease 2019 - Пандемія пошкодженої хвороби

CPPS - Cyber-Physical Power System - Кібер-фізична енергосистема

CPS - Cyber-Physical Systems - Кіберфізичні системи

DDoS - Distributed Denial of Service - Розподілена відмова в обслуговування

DoS - Denial of Service - Відмова в обслуговуванні

FDIA - False Data Injection Attack - Атака на основі введення хибних даних

HMI - Human-Machine Interface - Людино-машинний інтерфейс

HTTP - Hypertext Transfer Protocol - Протокол передачі гіпертексту

ICMP - Internet Control Message Protocol - Протокол управління інтернет-повідомленнями

ICPS - Industrial Cyber-Physical Systems - Індустріальні кіберфізичні системи

IEC - International Electrotechnical Commission - Міжнародна електротехнічна комісія

IEEE - Institute of Electrical and Electronics Engineers - Інститут інженерів з електротехніки та електроніки

IIoT - Industrial Internet of Things - Промисловий інтернет речей

IoT - Internet of Things - Інтернет речей

IP - Internet Protocol - Інтернет-протокол

LCDR - Line Current Differential Relay - Диференціальні реле струму лінії

LOF - Local Outlier Factor - Локальний коефіцієнт відхилення

LSTM - Long Short-Term Memory - Довга короткочасна пам'ять

MADDL - Multi-Agent Distributed Deep Learning - Багатоагентне розподілене глибоке навчання

NERC - North American Electric Reliability Corporation -

Північноамериканська корпорація електричної надійності

NERC-CIP - North American Electric Reliability Corporation Critical Infrastructure Protection - Захист критичної інфраструктури Північноамериканської корпорації

NIST - National Institute of Standards and Technology -

Національний інститут стандартів і технологій

NIST SP - National Institute of Standards and Technology Special Publication - Спеціальна публікація Національного інституту стандартів

FDI - False Data Injection - Введення неправдивих даних

SCADA - Supervisory Control and Data Acquisition - Диспетчерське управління та збір даних

SG - Smart Grid - Інтелектуальна мережа

SMC - Sliding Mode Controller - Регулятор ковзного режиму

TCN - Temporal Convolutional Network - Тимчасова згортка нейронна мережа

TCP - Transmission Control Protocol - Протокол управління передачею

ВСТУП

Сучасний енергетичний сектор активно трансформується під впливом цифровізації та впровадження кіберфізичних систем (КФС). Інтеграція цифрових технологій у традиційні енергетичні мережі забезпечує ефективне управління та моніторинг, проте, водночас створює нові проблеми у сфері кібербезпеки. Значна кількість кібератак, спрямованих на критичну інфраструктуру, підкреслює використання комплексних рішень для забезпечення кіберстійкості. Атаки, такі як BlackEnergy чи Stuxnet, демонструють загрозу для енергетичних систем, а також спонукають до розроблення ефективних механізмів протидії. Це дослідження мотивоване прагненням знайти інноваційні рішення для забезпечення безпеки кіберфізичних енергетичних систем (КФЕС), особливо в контексті збільшення викликів.

Забезпечення безперебійної роботи КФЕС в умовах зростаючих кібератак залишається проблемою, яка потребує оперативного рішення. Більшість існуючих механізмів кіберзахисту мають обмежену ефективність проти складних атак, таких як атаки на цільність даних (FDIA) чи атаки на відмову в обслуговуванні (DoS). Також бракує універсальних рішень, що забезпечили адаптивність системи до нових типів загроз.

Метою дослідження є розроблення та обґрунтування рекомендацій задля впровадження в сучасні методи кібербезпеки за умови підвищення стійкості КФЕС.

Для досягнення цієї мети потрібно вирішити наступні задачі:

- провести аналіз архітектури та компонентів КФС з визначенням основних вразливостей;
- вивчити типологію кібератак на енергетичні системи та їхні наслідки;

- розробити рекомендації щодо впровадження інтелектуальних алгоритмів для виявлення аномалій у реальному часі;
- запропонувати стратегії пом'якшення наслідків атак та відновлення системи після інцидентів.

Об'єктом дослідження є процес забезпечення кібербезпеки кіберфізичних енергетичних систем, а саме кіберфізичні енергетичні системи, що інтегрують інформаційні та енергетичні технології.

Предметом дослідження є методи забезпечення кібербезпеки КФЕС, включаючи адаптивні алгоритми та інтегровані системи моніторингу.

Наукова новизна роботи полягає в розробленні та обґрунтуванні рекомендацій щодо пом’якшення наслідків кібератак на кіберфізичні енергетичні системи. Запропоновані підходи спрямовані на підвищення кіберстійкості систем шляхом інтеграції адаптивних алгоритмів та інтелектуальних технологій, які дозволяють виявляти загрози в режимі реального часу й оперативно реагувати на них.

Практична цінність дослідження полягає в можливості впровадження розроблених механізмів захисту в реальні енергетичні системи, що забезпечить підвищення їхньої стійкості до кібератак. Зокрема, результати роботи можуть бути використані для модернізації SCADA-систем та підвищення їхньої надійності в умовах складних загроз.

Результати дослідження були представлені на міжнародній науковій конференції [1, 2]:

Карпуков Л.М., Павленко В.М. Інтеграція відновлюваних джерел і кіберзахист у сучасних енергетичних системах. Матеріали VIII Міжнародної науково-технічної конференції "Енергоефективність та енергетична безпека електроенергетичних систем", НТУ "Харківський політехнічний інститут", Харків, 2024.

1 АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ В КІБЕРФІЗИЧНИХ ЕНЕРГЕТИЧНИХ СИСТЕМАХ

1.1 Дослідження типології та історії кібератак на енергетичну інфраструктуру

Кібератаки - це віртуальні дії, спрямовані на проникнення в комп'ютерні мережі окремих осіб або організацій, які зазвичай мають на меті завдати шкоди або порушити роботу сервісів. Ці атаки можуть мати різну спрямованість - від порушення цілісності даних до викрадення конфіденційної інформації [3]. Тому розроблення адекватних рівнів захисту від кіберзагроз є необхідною для забезпечення безпеки та надійної роботи енергетичних та енергетичних систем. Проте, протягом останніх років енергетична галузь зазнає все більшої кількості спроб кібератак. Починаючи з 1980-х років, в енергетичному секторі було зафіксовано близько 800 кібератак [4]

Взаємозв’язок «інтелектуальної мережі» з Інтернетом наражає мережу на нові типи ризиків, включаючи розширені постійні загрози, розподілене-заборонене обслуговування (DDoS), ботнети та нульові дні, Stuxnet, Duqu, Red October або Black Energy – це лише кілька прикладів сучасних загроз, які з’явилися з 2010 року [5].

Протягом останніх десятиліть енергетична інфраструктура неодноразово ставала об’єктом кібератак. Деякі з них мали значний вплив на безпеку та стабільність систем:

- **S**tuxnet (2010 рік) - перший документований випадок використання шкідливого програмного забезпечення для фізичного руйнування інфраструктури;
- атака на енергосистему України (2015 рік) - спричинила масове знеструмлення, вплинувши на 225 000 користувачів;

– NotPetya (2017 рік) - масована атака з використанням вірусу-шифрувальника, спрямована на критичну інфраструктуру.

Історичний аналіз атак демонструє зростаючу складність і руйнівний потенціал загроз для енергетичних систем

За останні роки відбулося кілька кібератак на системи управління електроенергетикою по всьому світу [6]. У червні 2007 року відключення електроенергії тривалістю близько 46 хвилин в районі Темпе, штат Арізона, торкнулося близько 100 000 споживачів, що призвело до втрати 400 МВт навантаження. Причиною відключення стала випадкова активація програми зниження навантаження [7]. Аналогічно, у лютому 2008 року системні збої у Південній Флориді, спричинені відмовою системи передачі, призвели до втрати 2300 МВт навантаження [8]. Ці два інциденти не розглядалися як навмисні та зловмисні атаки, однак вони свідчать про кібернетичні вразливості енергосистеми. У цьому контексті в роботі [7] представлено детальний огляд та аналіз для розуміння мотивації основних кібератак, що відбулися між 2001 та 2013 роками. Крім того, в цьому дослідженні наводиться інформація про цілі атак та описуються методи, які використовувалися зловмисниками [7]. Основними цілями кібератак були визначені країни, що мають ризики для національної безпеки; стратегічна інфраструктура, галузі та компанії країни; глобальне шпигунство; заохочення хакерської діяльності [7]. Історичний аналіз основних кіберінцидентів, що сталися у світі, перший з яких датується 1903 роком, можна знайти в [8].

З цих списків можна зробити висновок про те, як відбувалися ці атаки, виявити можливі вразливості, а також спостерігати зростання кількості атак в останні роки і більшу складність і витонченість кібервторгнень. У 2010 році засоби управління атомної електростанції в Ірані були атаковані комп'ютерним хробаком під назвою Stuxnet [9]. Це шкідливе програмне забезпечення небезпечне тим, що воно самовідтворюється, поширюється по всій системі і використовує незаплановані вразливості в операційній системі технологічних

комп'ютерів [10]. Stuxnet вважається однією з основних кібератак, описаних в літературі, оскільки вона спричинила зміни в стратегіях і політиці кібербезпеки країн [11]. Нещодавній приклад руйнівних наслідків кібератак стався в грудні 2015 року в Україні, де 225 000 споживачів на кілька годин залишилися без енергопостачання через вимушене відключення електроенергії [12]. Ця подія стала відомою як найгірше відключення енергосистеми, спричинене кібератакою, коли- небудь зафіксоване в літературі [12].

Сектор охорони здоров'я, університети, дослідницькі центри, лікарні та лабораторії під час пандемії коронавірусної хвороби (COVID-19) зазнали скоординованих кібератак на свої інформаційно-комунікаційні системи. Ці атаки мали на меті отримати несанкціоновану інформацію про розробку вакцин та ліків для боротьби з COVID-19. У березні 2020 року університетська лікарня в Чеській Республіці зазнала кібератаки, яка вивела з ладу її інтернет-мережу і спричинила затримки та перенесення операцій і надання невідкладної допомоги. Дев'ять інших кібератак і порушень у секторі охорони здоров'я під час пандемії COVID-19 більш детально представлені в [13].

На додаток до кібератак, енергосистеми також піддаються акціям кібертероризму, спрямованим на поширення страху серед населення, яке обслуговується [14]. У цій новій формі тероризму Пакистан виділяється найбільшою кількістю атак (439), за ним йдуть Ємен (170), Колумбія (161) та Ірак (146). На рис. 1.1. показано кількість терористичних атак, яких зазнав електроенергетичний сектор окремих країн у період з 2010 по 2014 роки [14]

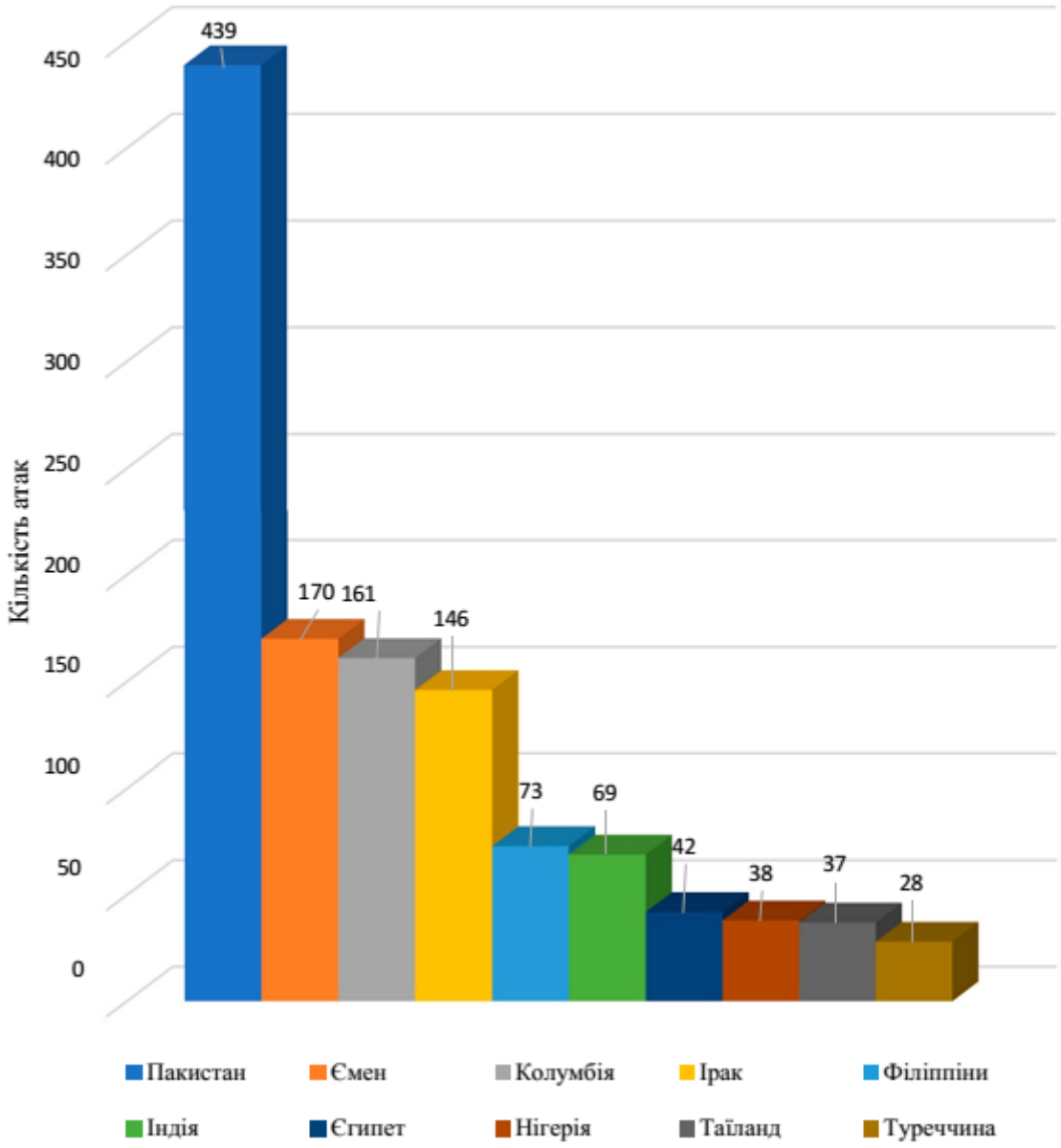


Рисунок 1.1 - Кількість терористичних кібератак в електроенергетичному секторі окремих країн [15]

Хронологія та приклади кібератак у системах управління промисловістю та енергетичному секторі, а також їхні наслідки продемонстровано в табл. 1.1.

Таблиця 1.1 - Кібератаки в промислових системах управління та енергетичному секторі [16-18]

Рік	Залучені країни	Тип кібератаки	Кібератака
1	2	3	4
1982 рік	СРСР	Маніпуляція кодом	Знищення трубопроводу в Сибіру через маніпуляцію кодом програмного забезпечення управління, що викликало несправність клапанів.
1999 рік	Беллінгем, США	Маніпуляція кодом	Маніпуляція кодом, що призвела до уповільнення роботи трубопровідної SCADA-системи.
2000 рік	Квінсленд, Австралія	Атака	Кібератака на Maroochy Water Services: бездротова атака, яка віддалено контролювала 150 насосних станцій і випустила мільйони літрів необроблених стоків.
2003 рік	Огайо, США	Шкідливе ПЗ	Атака на атомну електростанцію в Огайо шляхом впровадження шкідливого програмного забезпечення (Slammer Worm) в систему управління.
2007 рік	Національна лабораторія Айдахо, США	Атака	Хакер впровадив хібні дані та контролює генераторний вімікач. Ця кібератака отримала назву «Атака Аврора».
2008 рік	Туреччина	Атака	Вибух нафтопроводів у Туреччині через атаку на ін'єкцію помилкових даних, яка маніпулювала системою управління трубопроводом.
2010 рік	Іран	Шкідливе ПЗ	Ядерні об'єкти Ірану були атаковані шкідливим програмним забезпеченням Stuxnet.
2010 рік	Китай, США, Нідерланди	Шкідливе ПЗ	Шкідливе ПЗ Night Dragon, яке було спрямоване на великі компанії в енергетичному секторі та секторі нафти і газу.
2011 рік	Глобально	Шкідливе ПЗ	Шкідливе ПЗ Duqu/Flame/Gauss було виявлено угорськими дослідниками у 2011 році та мало на меті викрадання інформації із систем управління компаніями та їхніх постачальників.
2012 рік	Глобально	Кампанія (серія атак)	Серія кібератак, спрямованих на нафтову та газову промисловість, повідомляє як "Кіберкампанія щодо вторгнення в газопроводи".
2012 рік	Саудівська Аравія та Катар	Шкідливе ПЗ	Енергетичні компанії створили від шкідливого ПЗ Shamoon, яке вплинуло на генерацію та постачання електроенергії.

Продовження таблиці 1.1

1	2	3	4
2013 рік	США та Росія	Атака	Кібератака на компанію з обслуговування систем опалення, вентиляції та кондиціювання повітря. Витяг фінансових даних великих магазинів, відомий як "Атака на магазини Target".
2013 рік	США та Іран	Атака	Кібератака на дамбу Bowman у Нью-Йорку через кіберінцидент, організований іранськими хакерами, відомо як "Атака на дамбу Нью-Йорка".
2013 рік	США та Росія	Шкідливе ПЗ	Троянська програма Havex, яка дозволяла віддалено отримувати доступ і викрадати інформацію з промислових контрольних систем.
2014 рік	Німеччина	Атака	Кібератака на сталеварному заводі в Німеччині, яка спричинила порушення в роботі обладнання та операційні збої через використання соціальної інженерії.
2014 рік	Глобально	Шкідливе ПЗ	Шкідливе ПЗ BlackEnergy, спрямоване на витяг інформації від постачальників Людино-машинних інтерфейсів.
2014 рік	США, Туреччина, Швейцарія, Росія	Кампанія (серія атак)	Компанія Dragonfly/Energetic Bear спрямована на шпигунство та витяг конфіденційної інформації з енергетичного сектору.
2015 рік	Україна	Атака	Масштабне відключення електроенергії внаслідок ін'єкцій помилкових даних в енергосистемі, що стало першим успішним прикладом кібератаки на енергосистеми країни.
2016 рік	Сирія та США	Атака	Кібератака на компанію з обробки води, що змінила дозування хімікатів, використаних у процесі, повідомляє як "Ataka Kemuri Water Company".
2016 рік	Саудівська Аравія та інші країни Близького Сходу	Шкідливе ПЗ	Використання шкідливого ПЗ Shamoon через чотири роки після першої атаки, спрямованої на цивільну авіацію Саудівської Аравії та інших країн Близького Сходу.
2016 рік	Україна	Атака	Чергова кібератака на українську енергосистему, що спричинила відключення електроенергії. Використано шкідливі ПЗ CRASHOVERRIDE.
2017 рік	США, Україна	Шкідливе ПЗ	CRASHOVERRIDE, шкідливе ПЗ, яке відповідає для відключення електроенергії в енергосистемах.
2017 рік	Іран, США, Саудівська Аравія, Південна Корея	Група (набір шкідливих програм)	APT33 — набір шкідливих програм, спрямованих на шпигунство у сферах авіації, енергетики та нафтопереробки. Також здатний видаляти дані та розповсюджувати конфіденційну інформацію.

Кінець таблиці 1.1

1	2	3	4
2017 рік	Україна, Росія, США, Велика Британія, Австралія	Атака	Шкідливе ПЗ NotPetya, яке використовується для атаки на критичну інфраструктуру країни.
2017 рік	США	Кампанія (серія атак)	Компанія Dragonfly/Energetic Bear No. 2, спрямована на стратегічну інфраструктуру, зокрема електромережі та системи водопостачання.
2017 рік	Країни Близького Сходу	Шкідливе ПЗ	Шкідливе ПЗ TRITON/Trisis/HatMan здатне отримувати доступ до конфіденційної інформації та змінювати алгоритми роботи промислових систем.
2019 рік	США	Атака	Кібератака на енергосистему США 5 березня 2019 року. Тип атаки — відмова в обслуговуванні. Перша атака в секторі вітрової та сонячної енергетики.
2019 рік	Індія	Шкідливе ПЗ	Кібератака на ядерну електростанцію Kudankulam в Індії.
2019 рік	Венесуела	Атака	Атака на енергосистему Венесуелі, яка призвела до відключення електроенергії понад п'ять днів у кількох країнах, включаючи столицю.
2020 рік	Португалія	Вимагач (шкідливе ПЗ)	Кібератака на енергетичну компанію Energias de Portugal із викраденням 10 ТБ конфіденційних даних.
2020 рік	Бразилія	Атака	Кібератака на компанію Light SA із використанням шкідливого ПЗ Sodinokibi, що тимчасово припинила її діяльність.
2020 рік	Венесуела	Атака	Кібератака на енергосистему Венесуелі, яка призвела до відключення електроенергії в кількох штатах, окрім столиці.
2021 рік	США	Вимагач (шкідливе ПЗ)	Хакери використали програму-вимагач для кібератаки на Colonial Pipeline, що призвело до зупинки операції трубопроводу на кілька днів.

1.2 Класифікація кібератак в енергетичному секторі

Інтелектуальні мікромережі є основною мішенню кібератак, які зазвичай можна об'єднати в три різні типи класифікації атак [19-21]: доступність, чесність, конфіденційність.

Огляд та опис основних типів кібератак, які наразі визначені в відкритих джерелах зведений в табл. 1.2.

Дані про роботу електромереж у реальному часі повинні бути доступними для операторів систем з автоматизованими системами управління, а також для консультацій з ними. Забезпечення безпеки цих даних є необхідним, оскільки їх підробка та/або відсутність можуть призвести до катастрофічних наслідків, таких як аварійні відключення та знеструмлення. У цьому сенсі кібератаки, спрямовані на доступність даних, відбуваються, коли надсилається шкідлива інформація, що спричиняє перевантаження мережі або сервера. Як наслідок, відбувається переривання або затримка передачі даних. Ця подія називається атакою на доступність даних [22].

Таблиця 1.2 - Класифікація кібератак в енергетичному секторі [22,23]

Категорія	Тип атаки	Опис атаки
1	2	3
Доступність (Availability)	DoS/DDoS	Атака на відмову в обслуговуванні (DoS) або розподілена атака (DDoS), яка перевантажує мережу та призводить до збоїв у роботі.
	ICMP	Атака через ICMP-пакети, яка перевантажує мережу, зазвичай відома як Ping Flood.
	HTTP	Атака, спрямована на перевантаження веб-сервера через великий обсяг HTTP-запитів.
	TCP SYN	Атака, яка використовує незавершені запити TCP для встановлення ресурсів сервера.
	UDP	Атака на мережу через великий обсяг UDP-пакетів, що причиною перевантаження.
Доброчесність (Integrity)	Міжсайтовий скриптинг	Ін'єкція шкідливого коду на веб-сторінці для атаки користувачів браузера.
	Обробка даних	Незаконна модифікація даних перед їх використанням або обробкою.
	Салямі	Викрадання невеликих сум грошей або даних через багатократні мікрозміни, що залишаються непомітними.
	Викрадення сесії	Викрадання сеансу користувача для отримання доступу до його облікових записів.
	SQL ін'єкція	Ін'єкція SQL-коду в запитах бази даних для отримання несанкціонованого доступу до даних.

Кінець таблиці 1.2

1	2	3
	Повтор	Повторення перехоплених повідомлень для обману системи або виклику несанкціонованих дій.
Конфіденційність (Privacy)	Підслуховування	Пасивне перехоплення даних під час їх передачі через мережу.
	Кейлоггер	Використання програм або пристроїв для запису натискання клавіш на клавіатурі.
	Пароль	Викрадання паролів користувачів різними методами, включаючи фішинг або соціальну інженерію.
	Підглядання	Шпигування користувачами або пристроями для отримання конфіденційних даних.
	Соціальна інженерія	Використання обману для отримання доступу до системи або конфіденційних даних через людський фактор.
	Аналіз трафіку	Аналіз мережевого трафіку для передачі даних або конфіденційної інформації.

Атаки на відмову в обслуговуванні (DoS) мають на меті перевантажити мережу і заблокувати системну комунікацію, щоб перервати запит користувача на обслуговування.

Розподілена атака на відмову в обслуговуванні (DDoS) є різновидом DoS-атак, що базується на одночасному координованому впливі численних ботів, контрольованих зловмисником. Ці боти, також відомі як "зомбі", заражають шкідливими програмами, які зловмисник встановлює на вразливих комп’ютерах, створюючи мережу для атак. DDoS-атаки призводять до перевантаження мережевих ресурсів, що робить їх недоступними для авторизованих користувачів. Такі атаки вважаються одними з найбільш руйнівних у сучасному мережевому середовищі. Підготовка до атаки включає кілька етапів: вивчення вразливостей системи, створення бот-мережі, запуск атак і витяг інформації з подальшим знищенням слідів. Основними наслідками цих атак є значне уповільнення комунікаційної мережі та блокування доступу до системних ресурсів.

Окремі типи DoS/DDoS-атак мають свої унікальні характеристики:

– ICMP-атака використовує протокол керуючих повідомлень Інтернету, що відповідає за оброблення помилок у доставці IP-пакетів. Зловмисник створює численні ICMP-запити, перевантажуючи пропускну здатність мережі жертви. Існують два основні способи реалізації таких атак: "Ping of Death", коли величезні пакети перевантажують систему, та "Smurf Attack", яка зловживає широкомовними запитами для атак.

– HTTP-атака використовує протокол передачі гіпертексту, надсилаючи численні GET- і POST-запити. Метою є створення хаосу в обробці запитів і порушення роботи веб-застосунків. На відміну від ICMP, цей тип атаки не споживає значну пропускну здатність, але ефективно порушує роботу цільового сервера.

– TCP SYN-атака зловживає недосконалістю триетапного процесу "рукостискання" протоколу TCP. Зловмисник надсилає численні запити SYN без завершення процесу авторизації (ACK), що перевантажує системну пам'ять та блокує доступ до сервісів.

– UDP-атака використовує протокол користувацьких дейтаграм, який не потребує встановлення з’єднання. Зловмисник створює численні фальшиві UDP-пакети з випадковими адресами, викликаючи перевантаження системи та збої у роботі сервера, що робить сервіси недоступними для легітимних користувачів.

Кожен із цих типів атак спрямований на підрив доступності мережевих ресурсів і є серйозною загрозою для сучасних інформаційних систем

Для ефективного управління електромережами та їх стабільного функціонування дані мають бути точними, узгодженими та достовірними. Атаки, спрямовані на порушення доброчесності, відбуваються шляхом зміни командних сигналів або періодичних вимірювань, що руйнує цілісність даних. Прикладом таких атак є введення неправдивих даних (FDI), яке порушує узгодженість інформації. Існує кілька ключових стратегій, які використовуються зловмисниками для компрометації доброчесності даних.

Однією з найпоширеніших атак є міжсайтовий скриптинг (XSS). Це форма атак на впровадження коду, що використовує вразливості в безпековій системі для виконання шкідливого коду через веб-браузери. Шкідливий код може бути поширений через заражені веб-сторінки, надаючи зловмиснику доступ до конфіденційної інформації. Цей тип атак буває постійним, непостійним або пов'язаним із "об'єктною моделлю документа" (DOM). Інший тип атак, відомий як маніпуляція даними, полягає у незаконній зміні інформації в базах даних, наприклад, зміна статусу файлів чи конфіденційності.

Салямі-атаки відрізняються поступовим і майже непомітним збором невеликих обсягів конфіденційної інформації, що в сукупності завдає значної шкоди. Викрадення сесії полягає у перехопленні сеансів, де зловмисник інтегрується в мережеву взаємодію, отримуючи несанкціонований доступ до даних. У таких випадках зловмисники часто використовують незашифровані протоколи чи мережеві вразливості.

Ще одним розповсюдженим методом є ін’єкція SQL-коду, де зловмисники використовують вразливості в операторах SQL для доступу до бази даних. Такі атаки можуть надавати доступ до всієї інформації, що зберігається у базі даних, дозволяючи зловмисникам змінювати, завантажувати або видаляти дані. Окрім цього, атаки з відтворенням (Replay Attack) спрямовані на моніторинг і запис вимірювань із датчиків, після чого ці дані відтворюються для імітації нормальної роботи системи. Такий метод зазвичай використовується для компрометації компонентів кіберфізичних систем, зокрема датчиків, виконавчих механізмів та контролерів.

Ці типи атак на доброчесність не тільки порушують цілісність даних, але й створюють загрозу для безперебійної роботи електромереж, критично впливаючи на їхнє управління та контроль

Для забезпечення конфіденційності доступу даних до важливої системної інформації має бути обмежено лише для неавторизованих осіб. У випадку, коли неавторизовані особи отримують доступ до інформації про планування, контроль

та операційні стратегії, конфіденційність порушується, і дані залишаються вразливими для шпигунства та зловживань. Це може вплинути на функціонування системи та призвести до серйозних фінансових і технічних наслідків. Розглянемо основні типи атак, які загрожують конфіденційності даних.

Підслуховування є одним із методів, за допомогою якого зловмисник таємно отримує доступ до конфіденційної інформації в мережі. Ця атака дозволяє несанкціоновано читати, змінювати або видаляти дані, що порушує конфіденційність комунікації. Іншим способом є використання клавіатурних шпигунів або кейлоггерів, які без відомості користувача встановлюються в системі для запису натискання клавіш. Такі дані, як паролі або інша конфіденційна інформація, можуть бути викрадені для подальшого використання.

Атаки на паролі є ще однією поширеною загрозою конфіденційності. Зловмисники використовують різні методи, такі як атаки на основі словника, підбираючи комбінації за допомогою спеціального програмного забезпечення або використання персональних даних жертви для введення пароля. Це може призвести до витоку важливої інформації, фінансових втрат та вторгнення в особисте життя. Періодичні зміни паролів та створення складних комбінацій символів можуть значно підвищити рівень захисту.

Шпигунство, або снупінг, може відбуватися як фізично, коли зловмисник спостерігає за введенням конфіденційної інформації, так і в цифровому форматі, коли хакери підтримують доступ до даних через мережеве обладнання або зламані камери. Соціальна інженерія спрямована на маніпулювання людьми для отримання конфіденційної інформації. Використовуючи методи переконання або створення довірливих відносин через соціальні мережі, електронні листи або телефонні дзвінки, зловмисники підтримують доступ до особистих даних.

Аналіз трафіку є пасивною атакою, що забезпечує моніторинг комунікацій між відправником і отримувачем для виявлення вразливостей у мережі. Цей метод дозволяє зловмисникам отримувати інформацію про структуру мережі та

планувати подальші атаки. Усі ці типи залишають під загрозу конфіденційності даних та особисту інформацію, що створює їх серйозну проблему для безпеки інформаційних систем

1.3 Дослідження архітектури та компонентів кіберфізичних систем

Кіберфізичні енергетичні системи (КФС) є складними інтегрованими структурами, які поєднують фізичні енергетичні компоненти із сучасними інформаційними технологіями. Основними складовими КФС є системи моніторингу, управління та передачі даних, що забезпечуються через SCADA-системи (Supervisory Control and Data Acquisition), інтелектуальні лічильники та мережеві протоколи.

Технологічний прогрес у промисловості сприяє появі кіберфізичних систем КФС. На рис. 1.2. зображено систему КФС у вигляді блок-схеми.

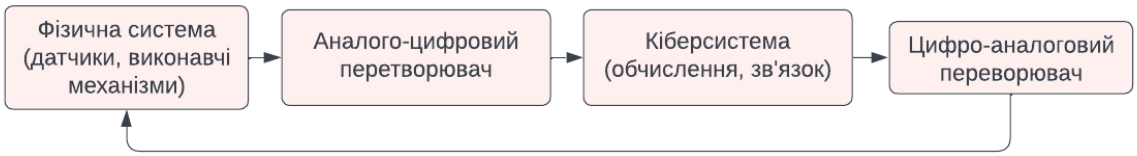


Рисунок 1.2 - Блок-схема кіберфізичної системи [24]

Архітектура КФС (табл. 1.4.) поділяється на три основні типові рівні: фізичний рівень, комунікаційний рівень та рівень управління. Рис. 1.3 ілюструє архітектуру КФС [25].

Таблиця 1.4 - Рівні та компоненти КФС

Рівень / Компонент	Опис
Фізичний рівень	Основні енергетичні об'єкти, такі як генератори, трансформатори та мережеві вузли.
Комунікаційний рівень	Мережі передачі даних, які виконують протоколи DNP3, Modbus, TCP/IP для стабільного та безпечного обміну інформацією.
Рівень управління	Системи управління, аналізу даних та оптимізації, побудовані на основі IoT-технологій і алгоритмів машинного навчання.
SCADA-системи	Забезпечують віддалений моніторинг та управління енергетичними об'єктами.
Інтелектуальні сенсори	Використовуються для збору даних про стан системи.
Програмовані логічні контролери (PLC)	Відповідають за локальні процеси управління.
Людино-машинний інтерфейс (HMI)	Забезпечує інтерактивну взаємодію оператора з системою через інтуїтивно зрозумілі інструменти.

Ключовими компонентами, які формують архітектуру КФС, є SCADA-системи, що забезпечують віддалений моніторинг та управління енергетичними об’єктами, інтелектуальні сенсори для збору даних про стан системи, програмовані логічні контролери (PLC), які реалізують локальні процеси управління, а також людино- машинний інтерфейс (HMI), що дає можливість операторам взаємодіяти з системою через інтерактивні інструменти. Ці компоненти забезпечують інтеграцію фізичних і цифрових елементів, що є основою ефективного функціонування КФС.

Перший рівень архітектури КФС називається фізичним рівнем. На цьому рівні знаходиться все обладнання, яке буде інтерпретувати фізичні явища та перетворювати їх на електричні сигнали, а згодом - на інформацію. До обладнання цього першого рівня належать агрегатори, актуатори, датчики, перетворювачі, глобальна система позиціонування (GPS), камери, мітки радіочастотної ідентифікації (RFID), лазери та будь-яке інше інтелектуальне обладнання так званого "заводського цеху". Цей рівень спрямований на збір інформації про процеси в реальному часі для планування, моніторингу та управління фізичною системою.

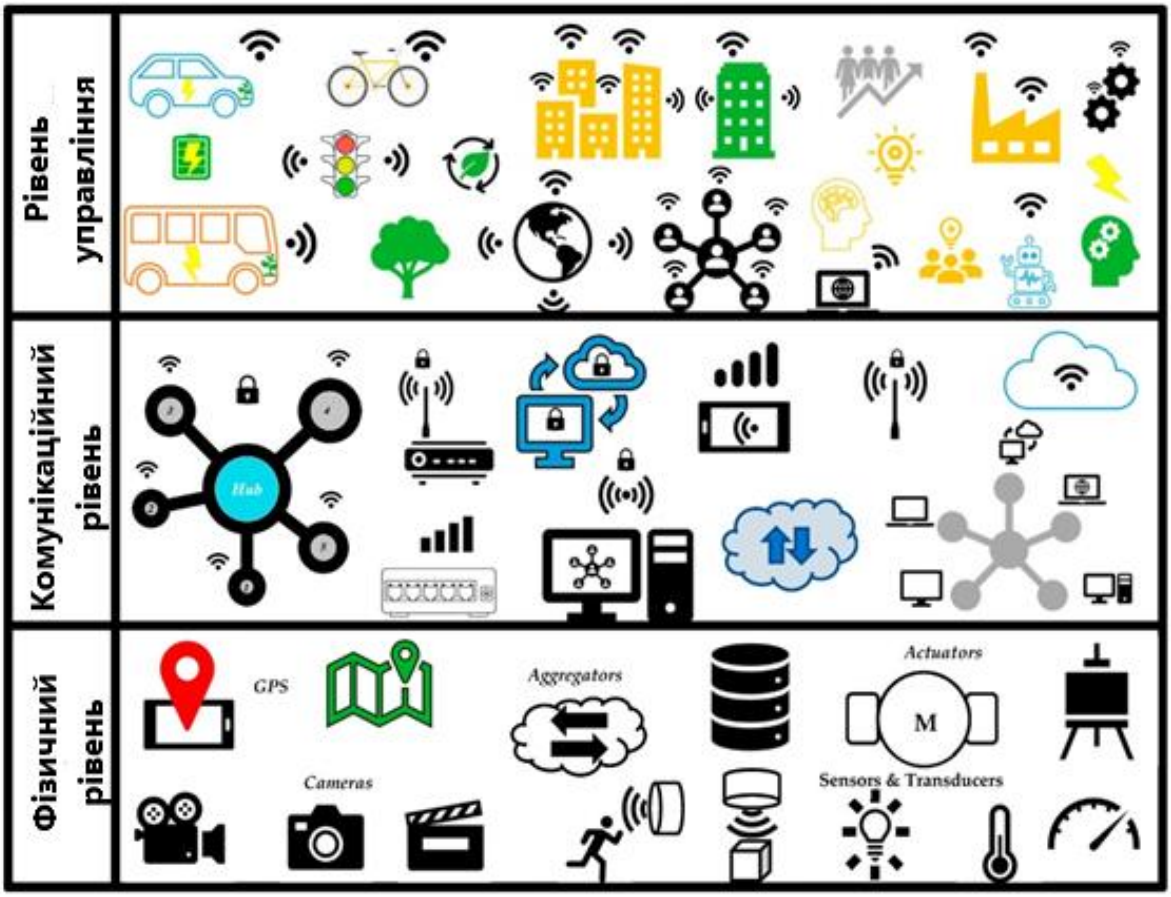


Рисунок 1.3 - Архітектура кіберфізичної системи [26]

Другий рівень архітектури КФС називається комунікаційним. Це проміжний рівень між фізичним рівнем і рівнем управління, який відповідає за передачу даних між рівнями. Його основна функція забезпечити безперебійний зв'язок з використанням дротових або Wi-Fi інтернет-мереж, технології Bluetooth, інфрачервоного зв'язку, 4G і 5G, Zigbee та інтернет-протоколів, а також інших технологій, що сприяють зв'язку. Крім того, цей рівень відповідає за маршрутизацію і транспортування даних через маршрутизатори, комутатори, концентратори, шлюзи і хмари.

Останній і найбільш інтерактивний рівень архітектури КФС називається рівнем управління. Роль цього рівня полягає в отриманні інформації від комунікаційного рівня, її аналізі та надсиланні відповідних командних сигналів пристроям, розташованим на фізичному рівні, для виконання дій у фізичному

процесі. Рівень управління генерує інтелектуальні алгоритми прийняття рішень для аналізу отриманої інформації і, відповідно, прийняття найбільш доцільного управлінського рішення для належного функціонування фізичної системи. Крім того, на цьому рівні виконується системний моніторинг, який намагається відобразити поведінку фізичної системи, щоб допомогти в процесі прийняття рішень. Також, рівень управління може враховувати попередні рішення при застосуванні операційних покращень та результатів реакції системи через зворотній зв'язок.

Одною із ключових проблем динамічної системи постачання електроенергії є те, що стабільний стан повинен підтримуватися в реальному часі. Такі системи характеризуються високою складністю через численні компоненти, що використовуються у їх роботі. Це призводить до невизначеності щодо нових типів загроз, які виникають в результаті взаємодії цих компонентів. Тому пропонується розглядати кіберфізичні системи, що складаються із трьох аспектів: кібернетичного, кіберфізичного та фізичного [27]. Перший з них здійснює обчислення даних, допускаються зв’язки та взаємодії, що не впливають на фізичний світ, тоді як кіберфізичний аспект розглядає всі взаємодії цих двох «світів». Третій аспект містить будь-які фізичні компоненти, властивості яких можуть впливати на безпеку.

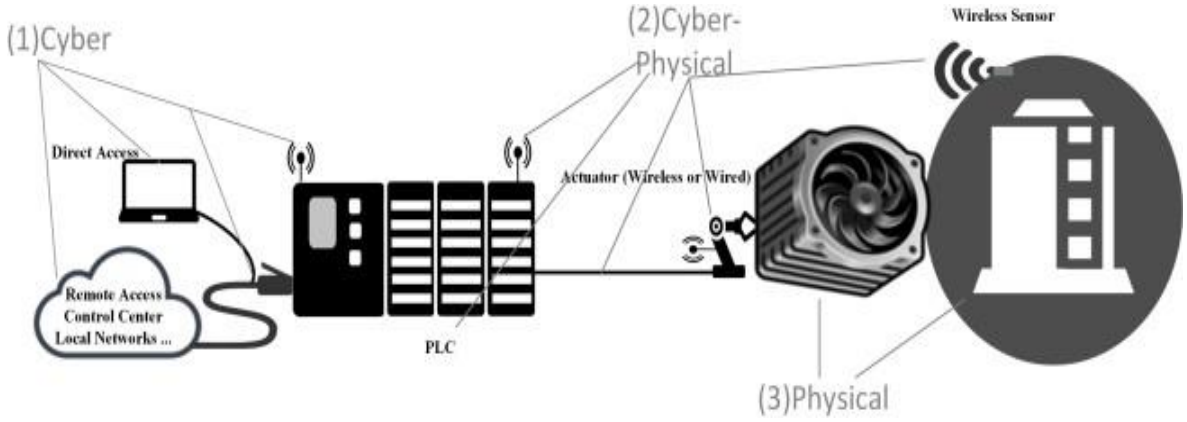


Рисунок 1.4 - Кібернетичний, кіберфізичний та фізичний аспекти системи [27]

Кібераспект (1) на рис. 1.4 не має прямого впливу на фізичні компоненти, а пов’язаний із ними через PLC (Програмований логічний контролер), який відповідає за зв’язок із середовищем вищого рівня.

Кіберфізичний аспект (2) містить в собі PLC, виконавчий механізм та датчики, що напряму взаємодіють із фізичним аспектом системи, який у свою чергу містить фізичні об’єкти, які треба контролювати та здійснювати моніторинг.

1.4 Аналіз вразливостей енергетичних систем до кібератак

Інтелектуальні мережі надають можливість активно контролювати енергоспоживання, користуючись гнучкими планами енергоресурсів і навіть стаючи дрібними постачальниками електроенергії. Що стосується постачальників енергоносіїв, то це дає змогу встановити ціни, що базуються на часі доби, покращити планування потужностей та використання енергії та більш гнучко пристосовуватися до потреб ринку. Мережа покращує управління передачею енергії та підвищує стійкість до відмов системи управління [28]. Сучасна конфігурація Smart Grid системи представлена на рис.1.5.

Водночас інтенсивне використання інформаційно-комунікаційних технологій викликає багато нових проблем.

«Інтелектуальні мережі» - це сукупність різних застарілих систем, оточених новими технологіями та архітектурними підходами, що відповідають різним стандартам і нормам, які всі повинні поєднувати в одну мережу зв'язку. Системи зв'язку «інтелектуальної мережі» мають багато вразливих місць, що відрізняються між мережами.

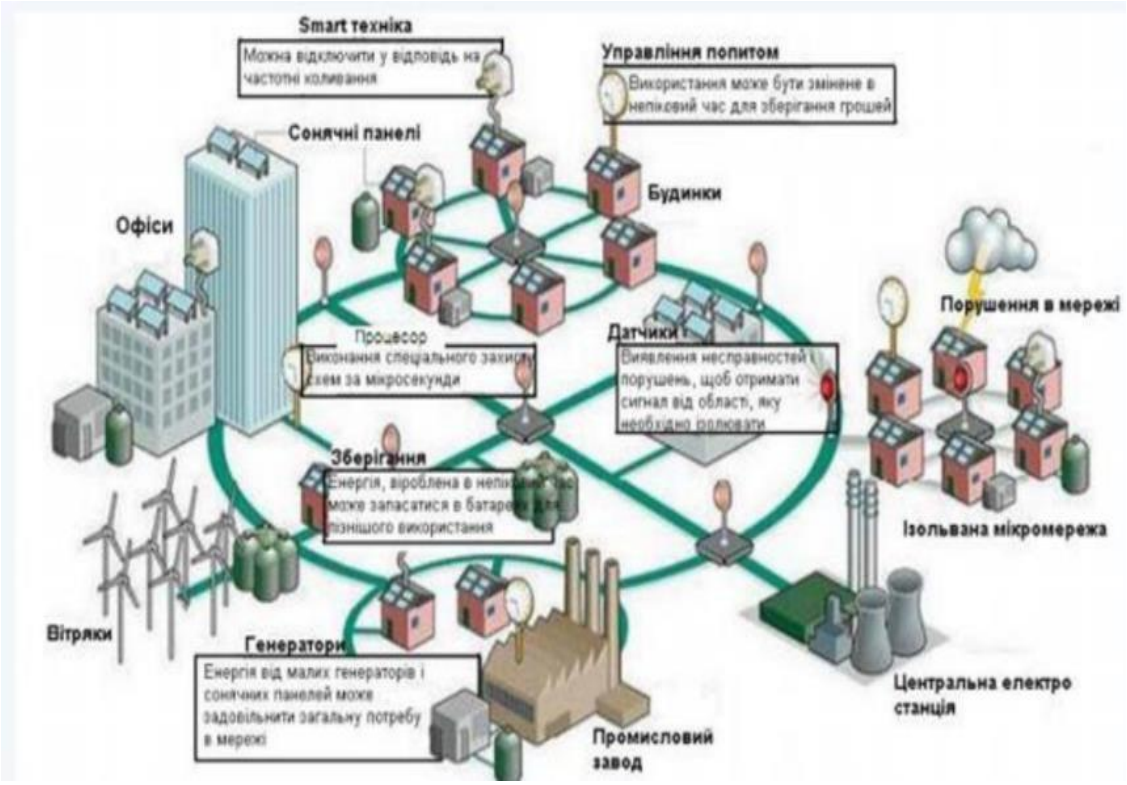


Рисунок 1.5 - Сучасна конфігурація Smart Grid системи

Впровадження «інтелектуальних мереж» вимагає мультидисциплінарного підходу, який поєднує різні технології та включає в себе управлінські, політичні, юридичні аспекти тощо. Вирішальну частину цього процесу формує оцінка безпеки, тобто оцінка рівня безпеки та виявлення потенційних вразливих місць, якими можуть скористатися зловмисники.

Енергетичні системи характеризуються кількома критичними вразливостями, пов'язаними з архітектурою та використанням комунікаційних технологій. Основними типами вразливостей кіберфізичних систем є протокольні, програмні та фізичні слабкі місця. Протоколи зв'язку, такі як Modbus і DNP3, зазвичай не мають вбудованої автентифікації та шифрування, що створює умови для маніпуляцій переданими даними з боку зловмисників. Уразливості програмного забезпечення часто зумовлені дефектами у написаному коді або залишеними бекдорами в пристроях, наприклад, в інтелектуальних лічильниках,

які можуть стати точками входу, виключно, для кіберзагрози, ці фізичні уразливості можливі через наявність прямого доступу до обладнання, яке не забезпечено належним рівнем захисту. Усі ці фактори разом створюють значні ризики для надійного функціонування кіберфізичних систем.

Сучасна інтеграція між людьми і машинами, керованими віддалено в режимі реального часу за допомогою інтернет-мереж, обробки даних і нових комп'ютерних та інформаційних технологій забезпечують переваги щодо ефективності та продуктивності системи управління в промисловості та автоматизації процесів. З іншого боку, ця система створює нові загрози для кібербезпеки інформації на фізичних пристроях, комунікації, моніторингу, експлуатації та управління кіберфізичною системою (табл. 1.5.).

Таблиця 1.5 - Вразливості кіберфізичних енергетичних систем від несанкціонованого доступу

Категорія вразливості	Опис	Приклади атак/загроза	Ключові компоненти
1	2	3	4
Кібернетична вразливість	Вразливості, пов'язані з мережею, комунікаціями, інтелектуальними пристроями, віддаленим доступом і збоями через дії співробітників або постачальників.	Атаки в мережі, наприклад, Stuxnet , Triton , Black Energy .	Комунікаційна мережа, IoT-пристрої, SCADA-системи, ПЛК.
Фізична вразливість	Атаки на фізичні пристрої, що складають інфраструктурні системи, включаючи датчики, виконавчі механізми, трансформатори, насоси, кабелі електропередач та інші фізичні елементи.	Несанкціонований фізичний доступ до обладнання, пошкодження датчиків, кабелів чи трансформаторів.	Датчики, трансформатори, насоси, виконавчі механізми.
Кіберфізична вразливість	Вразливості на стику кібер- і фізичних компонентів систем, які можуть призвести до збоїв у роботі критичної інфраструктури.	Ін'єкція логіки управління, атаки на відмову в обслуговуванні (DoS).	Комунікація між кібер- та фізичними компонентами, ПЛК, SCADA.

Кінець таблиці 1.5

1	2	3	4
Вразливості ПЛК (Програмованих логічних контролерів)	Інтеграція ПЛК з IoT робить їх вразливими до атаки на комунікаційну мережу, ін’єкційної логіки управління, атаки на відмову в обслуговуванні.	Ін'єкція логіки управління, DoS-атаки, передача шкідливих пакетів для перевантаження системи.	ПЛК, SCADA-системи, комунікаційна інфраструктура.
Безпека протоколів зв'язку	Використання незахищених протоколів зв'язку в системах управління, що впливає на конфіденційність, доступність та цільність даних.	Атаки на комунікаційні протоколи між інженерними станціями та ПЛК, вразливості Індустрії 4.0.	Протоколи зв'язку (наприклад, між SCADA та ПЛК), системи управління промисловістю.
Моніторинг та управління	Вразливості, пов'язані з недостатньою безпекою моніторингу центрального процесора ПЛК або відсутністю захисту даних у системах SCADA.	Аномалії в моніторингу, маніпуляції даними центрального процесора ПЛК для збоїв у роботі.	Центральний процесор ПЛК, системи моніторингу (SCADA).

З цієї точки зору, кіберфізична система представляє нові слабкі місця в її роботі, які відомі як кібер-, фізичні та кібер-фізичні вразливості. Кібернетична вразливість пов'язана з мережевою системою, комунікаціями, інтелектуальними пристроями, віддаленим доступом і ненавмисними збоями в роботі співробітників і постачальників [29]. Фізична вразливість пов'язана з фізичними атаками на пристрої, що складають інфраструктуру кіберфізичної системи, такі як датчики, перетворювачі, виконавчі механізми, двигуни, циліндри, насоси, клапани, кабелі ліній електропередач, розподільчі та передавальні трансформаторні вежі, серед інших фізичних пристроїв, що складають промислову систему [30]. Нарешті, існує кіберфізична вразливість, яка представляє собою новий тип вразливості, пов'язаний зі слабкими місцями і збитками, що виникають на стику кібер- і фізичних пристроїв і компонентів критичної інфраструктури промислової кіберфізичної системи [31]. Сучасні системи моніторингу, контролю та управління промисловістю реалізуються за допомогою SCADA-систем або інших систем управління промисловістю, які

використовують в якості основного елемента набір систем з програмованих логічних контролерів (ПЛК) [32]. ПЛК через свої входи відповідають за прийом і обробку даних, отриманих від датчиків і перетворювачів, підключених до промислового процесу, і за допомогою програмної логіки і видаваного сигналу можуть визначати, як будуть працювати виконавчі механізми, двигуни, перетворювачі частоти, реле, трансформатори та інші кінцеві елементи управління в промисловому процесі [32]. З цієї точки зору, інтеграція ПЛК з новими інтернет- технологіями робить його мішенню для кібератак на його комунікаційну мережу, таких як Stuxnet [33], Triton та Black Energy [34], а отже, такі пристрої становлять вразливість у сфері кібербезпеки і є частиною критичної інфраструктури промислового система управління СЕС.

ПЛК підключені до Інтернету речей та інтегровані в нього, тому вони вразливі до зловмисних загроз у своїй логіці управління. Цей тип атаки називається ін'єкцією логіки управління і має на меті спричинити збої та перебої в процесах, що контролюються ПЛК. З цієї точки зору, в роботі [34] представляє нещодавні дослідження атак на логіку управління та вказує на рекомендації та поточні проблеми у сфері безпеки та захисту інформації в системах, керованих ПЛК. Крім атаки на ін'єкцію керуючої логіки, існує атака на відмову в обслуговуванні, при якій надсилається та передається велика кількість шкідливих пакетів, що використовують можливі вразливості безпеки системи ПЛК. Так, в роботі [35] обговорено методологію, здатну виявляти аномалії на основі моніторингу поведінки центрального процесора ПЛК в системі управління резервуаром для води.

Кібербезпека в системах управління та контролю з ПЛК важлива для підтримки доступності, цілісності та конфіденційності технологічних даних і забезпечення належної та відмовостійкої роботи промислової системи. Так, автор роботи [36] представляє дослідження, яке вказує на проблеми інформаційної безпеки та обговорює безпеку протоколів зв'язку в системах Індустрії 4.0, що використовують ПЛК та SCADA. Автор роботи [37] використовує підхід,

відмінний від загальноприйнятого, розглядаючи мережу зв'язку між інженерними станціями та ПЛК як об'єкт дослідження та аналізу кібербезпеки.

Ці уразливості створюють ризики для надійного функціонування КФС, особливо в контексті кібератак типу Denial of Service (DoS), ін’єкції помилкових даних і атак на конфіденційність.

Інтелектуальні енергомережі мають особливі слабкі місця, зумовлені їхньою архітектуро, що викликає додаткові загальні вразливості кіберфізичних систем. Основними проблемними зонами є комунікаційні уразливості кіберкомпонентів, вразливість програмного забезпечення, загрози конфіденційності, проблеми в мережевій взаємодії та фізичні вразливості інтелектуальних мереж. Інформаційна інфраструктура Smart Grid значною мірою базується на стандартизованих інтернет-протоколах, які відповідають відомим вразливостям, які можуть використовуватися для атаки. Наприклад, TCP/IP є основним комунікаційним стандартом, проте його використання для зв’язку з центрами управління є фактичною загрозою через можливість несанкціонованого доступу. Неправильна конфігурація мережевої інфраструктури може привести до прямого або опосередкованого підключення енергомереж до відкритого Інтернету, що створює додаткові ризики. Окрім цього, TCP/IP містить критичну вразливість, таку як переповнення буфера, яка може бути використана для зловмисних цілей.

Вразливість програмного забезпечення є одним із критичних аспектів кібербезпеки інтелектуальних мереж. Інтелектуальні лічильники, які підтримують можливість віддаленого керування, є вразливі через те, що зловмисники можуть використовувати цю функцію для вимкнення електроенергії або маніпуляції даними. Програмні помилки також можуть спричинити вразливість, що робить всю систему вразливою до кібератак. Значна частина компонентів енергетичних мереж знаходиться у відкритому доступі, що дозволяє атакуючим використовувати їх як точки входу до загальної інфраструктури. Деякі виробники залишають бекдори в програмному

забезпеченні інтелектуальних лічильників, які можуть дозволити зловмисникам отримати контроль над пристроями, змінювати параметри роботи або навіть маніпулювати ціноутворенням. Дослідження [38] демонструє наявність прихованого програмного запису "Factory Login" у лічильниках, що дає повний контроль над пристроєм. Крім того, доступ відбувається через незахищений протокол telnet, що передає дані у відкритому вигляді, роблячи систему ще більш вразливою.

Конфіденційність даних в інтелектуальних мережах також піддається серйозним загрозам через двосторонню передачу інформації між лічильниками та комунальними підприємствами. Перехоплення цього трафіку дозволяє отримати чутливу інформацію про споживання електроенергії, розпорядок життя користувачів та їх присутність удома. Зловмисники можуть використовувати ці дані для планування атак або маніпуляції енергоспоживанням.

Загрози, пов'язані зі зв'язком у мережах, зумовлених використанням у Smart Grid протоколів Modbus та DNP3, які не підтримують механізми шифрування трафіку. DNP3 має лише базові засоби перевірки цілісності даних на основі контрольних сум CRC, тоді як Modbus взагалі не виконує жодних заходів захисту. Обидва протоколи не підтримують автентифікацію, що відкриває можливість для маніпуляцій з даними та атак на мережеву інфраструктуру. Застосування протоколу IEC 61850 частково покращує безпеку, але все ще не забезпечує належного рівня захисту від зовнішніх атак. Відсутність шифрування дозволяє зловмисникам перехоплювати трафік і виконувати атаки типу "man-in-the-middle". Це може привести до несанкціонованого отримання даних про поведінку користувачів, внесення хибної інформації або навіть ініціювання DoS-атаки шляхом перевантаження мережі фіктивними пакетами. Вразливість таких комунікаційних систем ускладнюється ще й тим, що інтелектуальні мережі складаються з гетерогенних компонентів, які контролюються іншими операторами. Наприклад, генеруючі установки взаємодіють із передавальними станціями, які, у свій час, з'єднані з розподільними підстанціями. Кожен з цих

етапів знаходиться під контролем різних організацій, що створює додаткові ризики через розрізненість відповідальності та показ єдиного підходу до кібербезпеки.

Фізичні вразливості інтелектуальних мереж також становлять серйозну проблему, порушення енергетичних об’єктів можуть бути піддані фізичним атакам, саботажу чи несанкціонованому доступу. Велика кількість мережевих пристроїв входу та датчиків, розміщених у відкритому доступі, створює створені точки для атакуючих, які можуть модифікувати або вивести з ладу критично важливі компоненти системи. Враховуючи складність та інтелектуальну мережу, забезпечення їхньої кібербезпеки вимагає багаторівневого масштабного підходу, що включає зміцнення мережевих протоколів, підвищення безпеки програмного забезпечення, впровадження сучасних методів шифрування даних та розробку єдиних стандартів управління кіберризиками.

1.5 Огляд ключових стандартів та протоколів кібербезпеки

Для забезпечення безпеки КФС застосовуються стандарти та протоколи, розроблені міжнародними організаціями [39]:

NIST SP 800-53 - забезпечує рамки для оцінки та впровадження кібербезпеки.

IEC 62351 - регламентує захист енергетичних мереж, включаючи SCADA-системи.

ISO/IEC 27001 - стандарт управління інформаційною безпекою.

Впровадження цих стандартів забезпечує системний підхід до захисту енергетичної інфраструктури, знижуючи ризики потенційних атак.

Захист кіберфізичних енергетичних систем (КФС) базується на використанні міжнародних стандартів та протоколів, які регламентують заходи

щодо забезпечення безпеки даних, управління доступом і захисту від кібератак. Вони спрямовані на зниження вразливостей та забезпечення кіберстійкості систем.

NIST SP 800-53 - Цей стандарт розроблений Національним інститутом стандартів і технологій США (NIST) і є одним із найпоширеніших документів у сфері кібербезпеки. Він надає рамкові рекомендації для впровадження технічних, управлінських і операційних заходів безпеки, які допомагають організаціям знижувати ризики кіберзагроз. Для КФС NIST SP 800-53 регламентує використання аутентифікації, шифрування даних, контролю доступу до мережевих і фізичних компонентів, а також управління інцидентами кібербезпеки.

IEC 62351- Стандарт IEC 62351 розроблений Міжнародною електротехнічною комісією і зосереджений на захисті комунікацій у енергетичних системах. Він охоплює протоколи SCADA-систем, інтелектуальних мереж і інших компонентів КФС. Особливу увагу приділено захисту протоколів обміну даними, таких як DNP3, Modbus і IEC 61850. IEC 62351 включає рекомендації щодо аутентифікації, шифрування, виявлення та запобігання атакам типу "людина посередині" (Man-in-the-Middle), а також аналізу аномалій у мережевому трафіку.

ISO/IEC 27001 - Цей стандарт є глобальним еталоном у сфері управління інформаційною безпекою. Він описує вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Впровадження ISO/IEC 27001 дозволяє систематично ідентифікувати загрози, оцінювати ризики, впроваджувати заходи контролю, такі як шифрування даних і резервне копіювання, та забезпечувати безперервність операцій.

NERC CIP - стандарт, розроблений Північноамериканською корпорацією з надійності енергопостачання (NERC), визначає вимоги до захисту критичної інфраструктури в енергетичному секторі. NERC CIP охоплює такі аспекти, як

захист фізичних об’єктів, контроль доступу до систем, моніторинг і реагування на кіберзагрози. Особливістю цього стандарту є його адаптація для енергетичних компаній у Північній Америці.

Стандарт IEC 61850 - цей стандарт регламентує комунікацію в інтелектуальних мережах і підстанціях. Він зосереджений на забезпеченні інтероперабельності різних систем, але не включає заходи безпеки "з коробки". Для усунення цих прогалин IEC 62351 пропонує додаткові рекомендації.

Протоколи безпеки SCADA-систем - у рамках SCADA-систем основними використовуваними протоколами є Modbus, DNP3 та ICCP:

Modbus не забезпечує шифрування чи автентифікацію, що робить його вразливим до ін’єкції помилкових даних.

DNP3 містить лише базові заходи цілісності даних, наприклад CRC, і також не забезпечує повноцінного захисту.

ICCP застосовується для обміну даними між центрами управління, але вразливий до переповнення буфера.

Міжнародна стратегія кіберстійкості ENISA (Європейське агентство з кібербезпеки) та CISA (Агентство з кібербезпеки США) пропонують рекомендації, які фокусуються на забезпеченні стійкості систем до атак і швидкому відновленні після них. Ці стратегії передбачають побудову комплексної кіберстійкості, що включає як превентивні заходи, так і механізми відновлення.

Використання зазначених стандартів і протоколів дозволяє створити системний підхід до забезпечення кібербезпеки кіберфізичних енергетичних систем. Це знижує ризики, пов’язані з кібератаками, і підвищує загальну стійкість інфраструктури до загроз сучасного світу.

1.6 Висновки розділу 1

Результати аналізу сучасного стану кібербезпеки в кіберфізичних енергетичних системах, включаючи визначення основних загроз, вразливостей та відповідних стандартів захисту узагальнені в наступних висновках:

- у результаті дослідження архітектури та компонентів кіберфізичних систем було встановлено, що ці системи складаються з трьох основних рівнів: сприйняття, транспортного та прикладного. Особливості архітектури КФС забезпечують ефективне управління енергетичними об’єктами, однак створюють численні уразливості, які зловмисники можуть використати для реалізації атак;
- аналіз уразливостей енергетичних систем до кібератак продемонстрував значні ризики, пов’язані з використанням незахищених комунікаційних протоколів, застарілого програмного забезпечення та фізичної доступності обладнання. Основними типами загроз є атаки на конфіденційність, цілісність і доступність даних, які можуть спричинити серйозні перебої у функціонуванні енергосистем;
- дослідження типології та історії кібератак на енергетичну інфраструктуру підтвердило, що кількість і складність атак постійно зростають. Такі інциденти, як атаки Stuxnet, NotPetya та кібератака на українську енергетичну систему у 2015 році, продемонстрували вразливість енергетичних систем і необхідність впровадження сучасних методів кіберзахисту для запобігання схожим інцидентам у майбутньому;
- огляд ключових стандартів і протоколів кібербезпеки підтвердив важливість системного підходу до захисту кіберфізичних енергетичних систем. Стандарти, такі як NIST SP 800-53, IEC 62351, ISO/IEC 27001 та NERC CIP, забезпечують комплексні рекомендації щодо управління ризиками, захисту комунікацій і відновлення систем після кібератак. Їхнє впровадження є критичним для підвищення кіберстійкості енергетичної інфраструктури.

2 ЗАСТОСУВАННЯ ТА МЕТОДОЛОГІЯ КІБЕРБЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ

У цьому розділі розглядається сучасний стан методів та рішень з кібербезпеки для кіберфізичних систем. Дослідження базується на аналізі широкого спектру наукових та прикладних джерел, включаючи провідні бази даних, такі як Science Direct, IEEE Xplore, Google Scholar та MDPI. Особливу увагу приділено трьом ключовим аспектам: забезпечення кібербезпеки в системах моніторингу, управління та захисту кіберфізичних систем, що візуалізовано на рис. 2.1.

У цьому розділі кожна з названих категорій досліджується з точки зору використання сучасних підходів, технологій та стандартів, а також визначення їх ролі в підвищеній стійкості кіберфізичних систем до загроз. Представлені підрозділи систематично висвітлюють доступні наукові та практичні розробки з кожної з перерахованих тем, що дозволяє обґрунтувати рекомендації щодо підвищення рівня кібербезпеки кіберфізичних енергетичних систем.

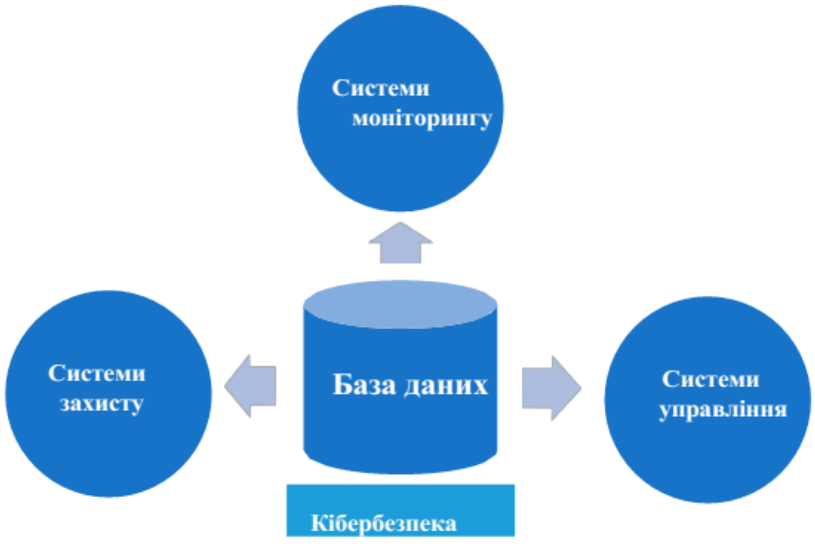


Рисунок 2.1 - Алгоритм пошуку інформації щодо сучасного стану методів та рішень з кібербезпеки для кіберфізичних систем енергетичного сектору

2.1 Кібербезпека в системах моніторингу

Кібербезпека системи моніторингу КФС є надзвичайно важливою, оскільки вона враховує безпеку інформації, зібраної датчиками та вимірювальними приладами. Тому для досягнення задовільних результатів система моніторингу повинна забезпечувати інформаційну безпеку та надійність. У цій категорії було відібрано 10 ключових робіт, які наведені в таблиці 2.1.

Таблиця 2.1. - Кібербезпека системи моніторингу [40-49].

Метод	Точка атаки	Мета	Сфера застосування	Симуляція	Джерело
1	2	3	4	5	6
Монітор безпеки в режимі реального часу	Атаки на рівні додатків та комунікацій	Виявлення відхилень, спричинених атак на рівні комунікацій і додатків, та запобігання їхньому поширенню на інших рівнях управління.	Кіберфізичні системи (ICPS)	Система розподілу води	[40]
Регульована модель розрідженої глибокої мережі (RSDBN)	Ієрархічно розподілені атаки	Виявлення показаних кібератак через ієрархічно розподілену систему виявлення вторгнень.	Кіберфізичні системи (ICPS)	Чисельна симуляційна платформа ICPS за допомогою OPNET та моделі Tennessee Eastman	[41]
Три алгоритми машинного навчання без учителя (OCSVMs, LOF, AEs)	Сканування мережі, DoS-атаки та ін'єкція шкідливих команд	Виявлення кібер- та фізичних аномалій.	Критична інфраструктура CPS	Модель шини IEEE-33	[42]

Продовження таблиці 2.1

1	2	3	4	5	6
Алгоритми машинного навчання	Атаки на критичну інфраструктуру	Виявлення кібер- та фізичних аномалій.	Критична інфраструктура CPS	Електростанція	[43]
Багатокритеріальна система прийняття рішень (MCDM)	Зловмисні та випадкові відмови в мікромережах	Підвищення стійкості, надійності та безпеки мікромережі через створення надійної метрики оцінки кібербезпеки.	Кіберенергетичні системи	Тестування на основі реальної моделі мікромережі	[44]
Архітектура платформи великих даних для аналізу журналів	Аномалії журналів	Запропонувати та реалізувати архітектуру для аналізу журналів, здатних виявляти аномалії в енергосистемі.	Мережі управління гідроелектростанціями	Тестування проведено на реальному наборі даних, записаному за 3 місяці	[45]
Методологія нечітких ієрархій та техніка TOPSIS	Доступність, цільність та конфіденційність даних	Аналіз і оцінка ризиків за допомогою операційної процедури для забезпечення кібербезпеки промислових систем.	Системи управління в енергетичному секторі	Обчислювальна симуляція шести різних альтернатив	[46]
Блокчейн-технології	Зловмисна ін'єкція помилкових даних у ПЛК	Точний моніторинг даних і захисту ПЛК від кібератаків, а також забезпечення роботи систем захисту реакторів.	Ізольовані мережі атомних електростанцій	Тестування методу за допомогою експерименту з ін'єкцією фіктивних даних у ПЛК	[47]
Алгоритми штучного інтелекту (AI)	Виявлення аномалій в електричних пристроях	Збір даних, управління збоями та реальний моніторинг енергетичних даних за допомогою алгоритмів AI.	Промисловий Інтернет речей	Створення апаратного забезпечення, серверів і баз даних в умовах відкритого програмного забезпечення	[48]

Кінець таблиці 2.1

1	2	3	4	5	6
Адаптивний метод і багатокрите ріальна оптимізація	Кібератаки та виявлення мережевих аномалій	Розробка адаптивної системи управління та моніторингу інформаційної безпеки.	Кіберфізич ні системи (CPS)	Експериментальне дослідження інтелектуальної системи виявлення вторгнень у домашніх умовах	[49]

Промислові кіберфізичні системи (ПКС) беруть участь у забезпеченні моніторингу та управління промисловими процесами. Вони складаються з інтегрованих програмних і апаратних компонентів, що дозволяє ефективно реагувати на зміни у фізичному просторі та підтримувати стабільність системи. Наприклад, методологія Multilayer Run-Time Security Monitor (ML-RSM), представлена в роботі [40], дозволяє виявляти аномалії, спричинені атаками на комунікаційному та прикладному рівнях, запобігаючи їх поширенню на інші рівні управління. Надійність цього підходу підтверджено на прикладі системи моніторингу розподілу води, що демонструє його практичну ефективність.

Для захисту ПКС від кібератак у роботі [41] пропонується використання ієрархічно розподілених систем виявлення вторгнення, які інтегрують адаптивний фільтр Калмана. Цей підхід дозволяє не тільки виявити можливі аномалії, але й адаптуватися до змін у системі, що забезпечує їй більш високу стійкість до нападу.

У контексті взаємозалежності фізичних і кібернетичних збоїв у ПКС у роботі [42] розроблено систему виявлення аномалій (ADS). Ця система використовує дані, зібрані давачами у фізичному просторі та кібердавачами, для аналізування в режимі реального часу. Методологія була протестована на моделі шини IEEE-33 із використанням трьох алгоритмів машинного навчання без учителя: однокласних машинних опорних векторах (OCSVM), локального фактора відхилення (LOF) і автокодерів (AE). Такий підхід дозволяє оцінювати й реагувати на критичні збої, які виникли в системі.

Критичні інфраструктури ПКС часто стоять об'єктами кібератак. Для їхнього захисту у роботі [43] пропонується методологію виявлення аномалій, засновану на алгоритмах машинного навчання. Ця методика забезпечує інтеграцію фізичних і кіберфізичних аспектів для підвищення рівня безпеки, що є основною для функціонування таких об’єктів, як електростанції.

Стійкість є ключовою характеристикою, яка забезпечує надійність ПКС. У роботі [44] розроблено методологію для її безперервного вимірювання та моніторингу. Ця методика включає аналіз імовірнісних концепцій, графіків, теорії ігор та оцінювання вразливостей. Метрика CP-SAM, що забезпечує оцінку стійкості, була протестована на реальних моделях мікромережі, що підтверджує її практичну ефективність.

Моніторинг ризиків безпеки в енергосистемі є місцем для розслідування збоїв та виявлення вразливостей. У роботі [45] пропонується створити платформу для аналізу журналів і алгоритм прогнозування на основі часових рядів, що дозволяє виявляти аномальні ситуації в енергосистемах. Цей підхід спрямований на раннє виявлення та запобігання можливим загрозам.

Для оцінки кібербезпеки енергетичних систем у роботі [46] використано методологію нечіткої логіки, зокрема метод аналізу ієрархій (MAI) та техніку TOPSIS. Автор протестував шість альтернативних проектів для перевірки ефективності підходу, що демонструє його універсальність у сценаріях.

Ізольовані мережі, такі як мережі ПЛК на атомних електростанціях, також мають бути захищені від атак. У роботі [47] представлено технологію блокчейн, що забезпечує точний моніторинг даних і захист ПЛК від кібератак. Додатково пропонується система, яка гарантує стабільність роботи системи захисту реактора (СЗР).

Зростання використання технології промислового Інтернету речей (IIoT) вимагає підвищення рівня кібербезпеки. У цьому контексті робота [48] пропонує підхід для збору, аналізу та моніторингу енергетичних даних у реальному часі за

допомогою алгоритмів штучного інтелекту (ШІ). Метод дозволяє швидко виявити несправності та мінімізувати ризики.

Інформаційна безпека на рівні моніторингу системи управління процесами (СУП) також має вирішальне значення. У роботі [49] пропонується адаптивний метод, який розв'язує багатокритеріальні оптимізаційні завдання. Цей підхід спрямований на підтримку цілісності даних і системи захисту від зовнішніх утручань.

Таким чином, моделі роботи демонструють широкий спектр сучасних підходів для забезпечення кібербезпеки промислових систем. Вони базуються на методах штучного інтелекту, блокчейну, адаптивного аналізу та прогнозування, що дозволяє ефективно протидіяти фізичним, кібернетичним та кіберфізичним загрозам. Ці інновації спрямовані на підвищення надійності, стійкості та безпеки промислових кіберфізичних систем.

2.2 Кібербезпека управлінського рівня кіберфізичних систем

Кібербезпека централізованої або розподіленої системи управління КФС повинна бути ефективною проти кібератак від найпростішої до найскладнішої форми систем. Це пов'язано з тим, що система управління відповідає за корекцію параметрів, що постійно змінюються для досягнення задовільних робочих параметрів. Щоб процес підтримував задовільні результати, система управління повинна ґрунтуватися на інформації про безпеку та надійність. Сучасна енергосистема характеризується розподіленою генерацією та пристроями, пов'язаними з силовою електронікою, генераторами, двигунами та трансформаторами, з'єднаними в мережу. Таким чином, кібербезпека управління частотою та напругою в цих пристроях є проблемою для забезпечення перехідної

та стаціонарної стабільності системи. У цій категорії було відібрано 10 ключових робіт, які наведені в Таблиці 2.2.

Таблиця 2.2 - Кібербезпека системи управління [50 - 59]

Метод	Точка атаки	Мета	Сфера застосування	Симуляція	Джерело
1	2	3	4	5	6
Модельне прогнозне управління (MPC)	Кібератаки типу DoS та ін'єкції помилкових даних	Розробка підходу до управління частотою, стійкою до кібератаки, з використанням методології тестування в реальному часі.	Управління частотою енергосистем	Контролер протестований на еталонній системі IEEE	[50]
Адаптивне управління на основі інтелектуального аналізу в реальному часі (CI)	Кібератаки на енергосистему	Розробка методики аналізу та управління стабільністю та кібербезпекою енергосистеми.	Енергетична система	Тестування базується на OPAL-RT та системі захисту SEL351S	[51]
Надійний контролер на основі порт-контрольованого гамільтоніана з дисипацією (PCHD)	Ін'єкції помилкових даних	Оборонний підхід, заснований на перспективах енергетичного перетворення.	Система управління синхронним двигуном з постійними магнітами	Протестований на промисловій КФС, яка керує синхронною машиною	[52]
Довга короткострокова пам'ять (LSTM) з тимчасовою згортковою нейронною мережею (TCN)	Ін'єкції помилкових даних	Мультиваріативний підхід для точного виявлення ін'єкцій помилкових даних у КФС у реальному часі.	Система управління "розумною" мережею	Ефективність підтверджена на основі системи IEEE і навчання з використанням TensorFlow та Keras	[53]
Методологія ковзного управління (SMC) на основі адаптивного динамічного програмування (ADP)	Ін'єкції помилкових даних	Децентралізований підхід до забезпечення безпеки великомасштабних систем із невідомими ін'єкціями.	Децентралізована задача оптимального управління	Тестування проведено на двомашинній енергетичній системі під впливом трьох різних атак	[54]

Кінець таблиці 2.2

1	2	3	4	5	6
Контролер для марківських систем із випадковими ін'єкціями	Випадкові ін'єкції помилкових даних	Підхід до управління, що підтримує ймовірну ін'єкцію помилкових даних.	Марківські кіберфізичні системи	Тестування проведено на моделі створеного плеча з одним з'єднанням	[55]
Контролер на основі спостерігача	Кібератаки типу DoS	Запропоновано алгоритм управління, стійкий до атаки типу DoS.	Клас двотемпоральних кіберфізичних систем	Ефективність протестована через порівняння імітацій та через інверсний маятник, керований двигуном DC.	[56]
Контролер H∞	Кібератаки типу DoS	Проведення дослідження для пом'якшення наслідків типу DoS за допомогою контролера Hoo.	Кіберфізичні системи (CPS)	Для демонстрації ефективності запропонованого підходу проведено чисельні симуляції	[57]
Стійки управління за допомогою динамічного нелінійного кодування/декодування та хаотичних осциляторів	Зловмисні атаки, приховані атаки на цільність системи, підслуховування	Розробка структури управління з пристроями для кодування та декодування сигналів, здатних ідентифікувати приховані атаки на кіберфізичну систему.	Кіберфізичні системи (ICPS)	Тестування та валідація проведені на моделі чотирибакового процесу	[58]
Модель гри "напад-захист"	Атаки з використанням шкідливого ПЗ	Представлення онлайн-техніки, заснованої на ігровій моделі "напад-захист", здатної ідентифікувати такі атаки.	Електромобілі	Чисельна та динамічна симуляція у програмному забезпеченні GAMS і MATLAB	[59]

Енергетичні системи, як критична частина інфраструктури об'єднаної енергетичної системи (ОЕС), за рахунок автоматизації операцій генерації, передачі та розподілу електроенергії, грають важливу роль. Водночас, вони є однією з основних мішеней для кібератак. Процес регулювання частоти часто

піддається атакам. У роботі [50] представлено розподілену методику регулювання частоти на основі модельного предиктивного управління. Підхід спрямований на покращення динамічної системи та пом'якшення результатів збоїв, що виникає через атаки. Тестування контролера на еталонній системі IEEE показало, що він ефективно протидіє кібератакам, таким як "відмова в обслуговуванні" (DoS) та "введення фальшивих даних".

Для забезпечення стабільності енергосистеми та кібербезпеки в роботі [51] розроблено стенд CPS, який працює в режимі реального часу. Він дозволяє користувачам імітувати несправності та аналізувати їхні дослідження. Крім того, методологія адаптивного управління для багатомашинної енергосистеми, що забезпечує її надійність навіть під час кібератак.

Одним із найбільш розширених типів атак є ін'єкція неправдивих даних. Такі атаки спрямовані на компрометацію системи роботи шляхом введення викривлених даних у вимірювання датчиків або керуючих сигналів. У роботі [52] пропоновано контролер, який адаптується до атаки, динамічно змінюючи свої параметри для стабілізації системи роботи. Відповідно, регулювання кількості демпфуючих елементів дозволяє зберегти динамічну стійкість системи навіть під час впливу атак.

Для ефективного визначення місця атаки в реальному часі в роботі [53] розроблено багатовимірний підхід, який використовує довготривалу короткочасну пам’ять (LSTM) та тимчасову згорткову нейронну мережу (TCN). Такий фреймворк дозволяє точно ідентифікувати фальшиві дані в режимі реального часу, підвищуючи загальну систему кібербезпеки.

Децентралізоване управління для великих систем розроблено в роботі [54], де використовується контролер ковзного режиму (SMC) на основі адаптивного динамічного програмування (ADP). Цей підхід дозволяє мінімізувати наслідки невідомих атак, таких як ін'єкції фальшивих даних, і забезпечує стабільність роботи системи. Випадкові ін’єкції фальшивих даних також розглянуті у роботі [55], де передбачається регулятор ковзного режиму для маркових

стрибкоподібних систем, який дозволяє керувати такими атаками на основі ймовірного підходу.

Комунікаційні технології в управлінні кіберфізичними системами роблять їх уразливими до атаки типу DoS. Для боротьби з цим типом атаки в роботі [56] пропонується алгоритм управління на основі концепції спостерігача для двомасштабних кіберфізичних систем (TTSCPS). А для системи із гібридними тригерними механізмами (HTM) у роботі [57] розроблено H∞-контролер, який ефективно мінімізує наслідки при типі DoS.

Деякі атаки спрямовані на маніпуляцію умовами роботи технологічного обладнання з порушенням цілісності системи. У роботі [58] пропонується структуру управління, яка з пристроями кодування та декодування сигналів здатна ідентифікувати приховані атаки, забезпечуючи стабільність роботи системи навіть у разі зовнішнього втручання.

Електромобілі також є наявними об'єктами кібератаки через їхню інтеграцію з бездротовими датчиками та мережами. У роботі [59] представлено ігрову модель «напад-захист», яка дозволяє ідентифікувати шкідливі програми, запобігаючи їх проникненню до електромобілів.

2.3 Кібербезпека систем захисту енергосистеми

Сучасна енергосистема все частіше використовує в своїй роботі, плануванні, контролі та захисті інформацію про ситуацію, електроніку та комп'ютерні технології. Як наслідок, суттєво вдосконалюючи обчислювальні процеси, вона також стала особливо вразливою до кібератак. Серед цих вразливостей варто відзначити, що атаки на реле аварійної сигналізації та інші пристрої безпеки, які складають систему захисту в енергосистемах, є критичними подіями, які можуть спричинити відключення електроенергії та інші

серйозні перебої в роботі системи. Таким чином, через можливість роботи мережі в ізольованому режимі або нових з'єднань ізольованих мереж, система захисту стає одним з головних об'єктів інтересу для забезпечення кібербезпеки в МГ. У цій категорії було відібрано 10 ключових робіт, які наведені в табл. 2.3.

Таблиця 2.3 - Кібербезпека систем захисту енергосистеми [60-69]

Метод	Точка атаки	Мета	Сфера застосування	Симуляція	Джерело
1	2	3	4	5	6
На основі різниці між розрахованими та виміряними перекриваючими напругами для LCDRs	Ін'єкція фальшивих даних у LCDRs	Запропонована методологія спрямована на виявлення типів ін'єкцій фальшивих даних проти LCDRs.	LCDR	Розроблена методологія підтверджена на основі моделі шини IEEE-39 та симулятора OPAL.	[60]
Спостерігач стану з невідомим вхідним сигналом	Ін'єкція фальшивих даних у LCDRs	Виявлення ін'єкцій фальшивих даних та їх відокремлення від внутрішніх збоїв роботи LCDRs.	LCDR	Розроблена методологія підтверджена на основі моделі шини IEEE-39.	[61]
Розроблений метод, що включає пасивні осциляторні контури	Ін'єкція фальшивих даних у LCDRs	Представлення дослідження впливу атак на синхронізацію часу та фальшивих даних у мікромережах для вирішення проблеми з фізичної перспективи.	LCDR	Запропонований метод протестований у симуляції підтверджений та числовим аналізом.	[62]
Модель на основі інтелектуального навчання з багатошаровим перцептроном	Ін'єкція фальшивих даних у LCDRs	Виявлення кібератак проти LCDRs виробляється за допомогою структури, заснованої на навчанні.	LCDR	Розроблена методологія підтверджена на основі моделі шини IEEE-39.	[63]

Кінець таблиці 2.3

1	2	3	4	5	6
Методологія на основі виявлення аномалій із використанням алгоритму Isolation Forest	Ін'єкція фальшивих даних у LCDRs	Виявлення кібератак і диференціація між реальною та фальшивою атаками на системи із захистом LCDRs.	LCDR	Розроблена методологія підтверджена на еталонній моделі IEEE-9 у середовищі PSCAD/EMTDC.	[64]
Методологія на основі теорії ігор	Кібератаки на конфігурацію реле в системах розподілу енергії	Визначення оптимального плану захисту та зменшення пошкодження системи захисних реле.	Система розподіл у енергії	Розроблена методологія протестована на тестовій моделі IEEE з 123 вузлами.	[65]
Методологія розподіленого глибокого навчання з використанням агентів	Ін'єкція фальшивих даних у реле	Виявлення ін'єкції фальшивих даних до моменту, коли вони імітують хибну несправність.	Система захисту енергоси стем	Запропонований метод протестований в мережах IEEE: 6-вузловий, 14-вузловий і 118-вузловий.	[66]
Адаптивна техніка	Ін'єкція фальшивих даних у реле	Пом'якшення наслідків фальшивих атак на захисні реле та уникнення перебоїв у енергопостачанні.	Захисні реле	Для підтвердження підходу використано цифровий симулятор реального часу.	[67]
Алгоритм на основі правил та принцип координації реле	Зловмисні атаки на захисні реле	Представлення стратегії захисту від зловмисних атак та небажаних змін у системах захисних реле.	Захисні реле	Техніка протестована та підтверджена в середовищі із захисними реле та цифровим симулятором для кіберфізичних систем.	[68]
Рекурентна нейронна мережа з осередками LSTM	Кібератаки та аномалії в системах захисту	Інтелектуальний алгоритм для моніторингу та виявлення аномалій у системі захисту в реальному часі, викликаних зловмисними атаками.	Системи захисту передачі енергії	Пропонований підхід підтверджено на тестовій моделі IEEE із реле.	[69]

Лінійні диференціальні реле струму дедалі частіше використовують для захисту енергосистем за рахунок їх здатності швидко та точно виявляти несправності. Інтеграція технологій кіберфізичних систем викликала значний інтерес до вивчення вразливостей таких реле до кібератак. У дослідженні [60] було запропоновано методологію, яка ґрунтується на аналізі різниці між виміряною та розрахованою напругою, для ідентифікації введення фальшивих даних у лінійні диференціальні реле струму (LCDR). Ця методика успішно підтверджена на моделі шини IEEE-39 із використанням симулятора OPAL.

Для покращення виявлення фальшивих даних є і інший підхід, представлений у роботі [61], він використовує процес моніторингу і виявлення невідомих вхідних сигналів, що дозволяє розрізняти фальшиві дані та виявляти внутрішні збої. У роботі [62] акцент зроблено на стійкість системи із LCDR. Автори досліджують вплив на синхронізацію частоти та виявлення фальшивих даних у мікромережах, пропонуючи пасивну генераторну схему, яка генерує затухаючі коливання з частотою відповіді на збій. Водночас у роботі [63] для розв’язання цих проблем використовується модель на основі багатошарового персептрона (MLP), що виокристовує принципи штучного інтелекту для підвищення ефективності виявлення атак.

Для системи, що вибирає LCDR як захист, у роботі [64] пропонується фреймворк на основі виявлення аномалії з використанням алгоритму Isolation Forest. Ця методика спрямована на розпізнавання кібератак та їх відокремлення від хибних сигналів, що підтверджено за допомогою моделі шини IEEE-9. Система розподілу електроенергії, як і LCDR, також є вразливою до кібератак. У роботі [65] представлено методологію, що базується на теорії ігор, яка шукає оптимальний план захисту та мінімізує вплив при атаці на реле захисту.

Система захисту електромереж із дистанційними реле особливо вразливою до атаки. У дослідженні [66] описано багатоагентне розподілене глибоке навчання (MADDL), яке здатне ідентифікувати введені фальшиві дані до моменту виникнення помилкової несправності. Адаптивна методика [67]

забезпечує взаємодію реле для перевірки змінених у вхідній точці захисної системи, що дозволяє уникнути перебоїв у живленні, викликаних хибними атаками. Крім того, у роботі [68] розроблено кооперативну стратегію захисту від модифікацій налаштування реле через зловмисні дії. Алгоритм базується на принципах управління захисними реле.

Системи передачі енергії також популярні для атак через використання сучасних електронних компонентів і технологій. У роботі [69] представлено інтелектуальний алгоритм, здатний у реальному часі виявляти атаки, що спричиняють аномалії в системах захисту. Тестування проводилося на системі IEEE із захисними реле.

Таким чином, наведені дослідження демонструють різноманітні стратегії підвищення кібербезпеки системи та захисту мікромереж. Основними інструментами цих стратегій є штучний інтелект, глибоке навчання, адаптивні методи, пасивні генераторні схеми, теорія ігор та методи контролю моніторингу стану. Ці рішення спрямовані на підвищення стійкості, надійності та безпеки енергосистем, забезпечуючи захист від кібератак та мінімізуючи їх вплив на критичну інфраструктуру.

2.4 Захисні стратегії та майбутні тенденції у сфері кібербезпеки

Сучасні енергосистеми є вразливими до численних і постійних кібератак, які можуть суттєво впливати на планування, експлуатацію, обслуговування та постачання електроенергії. Вище представлено різні аспекти кібербезпеки в сферах моніторингу, контролю та захисту кіберфізичних систем. Найпоширенішими типами атак визначено: введення фальшивих даних, атаки шкідливими програмами, DoS-атаки та підслуховування. Основні стратегії захисту зосереджені на двох ключових напрямках: запобігання кібератакам та їх

виявлення. Захист фізичних компонентів системи зосереджується на захисті фізичної частини, таких як датчики, виконавчі механізми, захисні пристрої та інші елементи. Ідентифікація загроз спрямована на зменшення наслідків атак, використовуючи статичні методи стабілізації системи або динамічні підходи з аналізом поточної інформації.

Розглянуті стратегії ґрунтується на сучасних методах управління, таких як адаптивне, робастне та предикативне управління, а також на технологіях штучного інтелекту, машинного навчання та глибокого навчання. додаткових традиційних підходів, у дослідженнях пропонуються інноваційні рішення, включаючи методи цифрової обробки сигналів, технології блокчейн і криптографічні алгоритми на основі квантових обчислень. Наприклад, у системі енергетичного керування була використана технологія блокчейн для захисту управління реактором атомної електростанції. Удосконалення стандартів і протоколів також залишається важливою складовою кібербезпеки.

З огляду на сучасний стан енергетичного сектора, майбутні тенденції кібератак та виклики для кібербезпеки можна виділити у двох основних напрямках. По-перше, модернізація електроенергетичної системи полягатиме в поступовому заміщенні традиційної генерації електроенергії чистою енергією, що збільшує інтеграцію локальних генераторів відновлюваних джерел енергії, змінює поведінку та додає системі характеристику переривчастої генерації. Крім того, використання нових технологій Інтернету речей та інтеграція між пристроями і секторами забезпечують появу "розумних" мереж, які через залежність від Інтернету для роботи і зв'язку мають кібернетичну вразливість. Таким чином, МГ потребує надійного та стійкого кіберзахисту, щоб не завдати шкоди її комунікації, оцінці стану, контролю частоти, регулюванню напруги та виконанню її функцій, таких як можливість роботи в ізольованому режимі та підключення інших ізольованих мереж.

По-друге, електрифікація транспорту є стратегічним напрямком, що сприяє зниженню викидів забруднюючих речовин, але також створює нові

ризики. Процес електрифікації транспорту - це стратегія, яка заохочує розробку, виробництво і використання автобусів, автомобілів, поїздів і метро на електричній тязі, а також є важливим фактором зменшення викидів забруднюючих газів в атмосферу. Ці технологічні транспортні засоби, підключені до зарядних станцій, модифікують і є частиною МГ. Таким чином, цей новий вид транспорту стає об'єктом кібератак, а безпека зарядних станцій вважається вразливою точкою і представляє дослідницький інтерес [70]. З цієї точки зору автор роботи [71] розробив програмне забезпечення для моделювання для оцінки кібернетичної вразливості зарядних споруд та пристроїв для електромобілів. Таким чином, Кібербезпека при електрифікації транспорту є актуальною проблемою, яка перебуває на стадії дослідження та розробки.

Загалом, роботи, пропозиції в дослідженні, демонструють ефективність існуючих та інноваційних підходів до забезпечення кібербезпеки, підкреслюючи важливість подальших розробок для підвищення надійності, стійкості та захисту енергетичної інфраструктури в умовах сучасних викликів.

2.5 Висновки розділу 2

У цьому розділі проаналізовано сучасні методи та підходи до забезпечення кібербезпеки кіберфізичних систем у трьох основних сферах: моніторинг, управління та захист. Нижче наведено основні результати дослідження:

- показано, що ефективний моніторинг залежить від здатності виявляти та запобігати аномаліям у реальному часі. Запропоновано рішення на основі машинного навчання, зокрема з використанням алгоритмів OCSVM, LOF і автокодерів, які продемонстрували здатність ідентифікувати критичні збої в режимі реального часу. Технології блокчейну та платформи аналізу великих даних підтвердили свою ефективність у моніторингу критичної інфраструктури;

- результати демонструють високу вразливість системи управління до атак, таких як DoS і введення фальшивих даних. Для пом'якшення цих ризиків пропонуємо низку підходів: адаптивні та прогнозні контролери, інтеграцію LSTM та TCN для виявлення аномалій, а також децентралізовані методики управління, засновані на теорії ігор. такі стратегії забезпечують збереження стабільності енергосистем навіть під час кібератак;

- захисні пристрої, як-от лінійні диференціальні реле струму, показали вразливість до атаки на введення фальшивих даних та маніпуляцій з параметрами роботи. Методики, засновані на штучному інтелекті, глибокому навчанні (MADDL), алгоритмах Isolation Forest та адаптивному управлінні дозволяють зменшити вплив кібератак на захист системи, мінімізуючи ризики відключення електроенергії та забезпечуючи надійність роботи.

Розглянуті підходи демонструють важливість інтеграції сучасних технологій, таких як штучний інтелект, блокчейн, теорія ігор та адаптивні методи, для забезпечення надійності кіберфізичних систем. Виявлені тенденції вказують на необхідність розробки комплексних стратегій кібербезпеки, що спрямовані на підвищення стійкості, надійності та безпеки енергетичної інфраструктури в сучасних умовах.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ТА ПРАКТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ МЕТОДІВ КІБЕРБЕЗПЕКИ В КІБЕРФІЗИЧНИХ ЕНЕРГЕТИЧНИХ СИСТЕМАХ

3.1 Визначення основних критеріїв ефективності кібербезпеки в КФС

Основні критерії ефективності кібербезпеки кіберфізичних систем включають швидкість виявлення атаки, точність визначення вразливостей, адаптивність до нових загроз та мінімізацію впливу на критичні процеси.

Захист конфіденційних даних має ключове значення для будь-якої компанії. Будь-який витік інформації може призвести до жахливих наслідків: шкоди репутації, фінансових втрат, втрати позицій на ринку, відтоку клієнтів тощо. Внутрішня система кібербезпеки повинна забезпечувати надійний захист даних, а також бути проактивною – вчасно виявляти та запобігати кібератакам.

Щоб відстежувати рівень кібербезпеки, необхідно мати чек-лист і аналізувати ключові показники ефективності (KPI), які є ефективним способом вимірювання успіху та ефективності будь-якої програми, включно з кібербезпекою. Без аналізу роботи системи кібербезпеки неможливо оцінити реальний стан безпеки та рівень захисту.

В табл. 3.1 наведено ключові показники ефективності кібербезпеки, які враховують специфіку енергетичного сектору, зокрема вплив кібератак на ключові об’єкти інфраструктури, такі як SCADA-системи, трансформаторні вузли та диспетчерські центри, а також забезпечує інтегровану оцінку ефективності заходів кібербезпеки.

Кіберзлочинці динамічно розвиваються і постійно винаходять нові та більш витончені методи атак. Відповідно змінюються процеси та технології їх запобігання. Важливо регулярно оцінювати ефективність засобів захисту та своєчасно замінювати та/або оновлювати застарілі засоби.

Аналіз ключових показників ефективності (KPI), ключових показників ризику (KRI) і заходів безпеки дозволяє отримати повну картину роботи команди безпеки, зрозуміти, що працює, а що ні, і вжити відповідних заходів. Показники надають кількісну інформацію, яку можна легко зібрати у звіт і поділитися з усіма зацікавленими сторонами.

Таблиця 3.1 - Ключові показники ефективності кібербезпеки кіберфізичних систем

Ризик	Показник	Опис показника
1	2	3
Атаки на критичні енергетичні об'єкти	Рівень готовності	Визначає кількість оновлених пристроїв в енергосистемі, а також здатність системи швидко виявляти та усувати вразливості на різних рівнях (фізичному, комунікаційному, інформаційному).
Несанкціоноване втручання в мережу	Виявлення несанкціонованих пристроїв	Ідентифікація підключень до енергетичних мереж, включаючи пристрої IoT, які можуть створювати кіберризики або становити загрозу стабільності системи.
Викрадання або маніпуляція даними	Спроба проникнення	Кількість спроб отримати несанкціонований доступ до інформаційних систем енергетичного сектору, що може призвести до втрати даних чи викривлення сигналів.
Збої в роботі через кібератаки	Безпека інцидентів	Кількість випадків порушення роботи енергетичних систем внаслідок кібератаки на диспетчерські центри, генератори, трансформатори та інші ключові компоненти.
Підтримка виявлення атак	Середній час виявлення (MTTD)	Час, необхідний для виявлення загроз у кіберфізичній енергетичній системі, таких як атаки на SCADA-системи чи введення фальшивих даних у датчики.
Підтримка реагування	Середній час реагування (MTTR)	Час, потрібний для реагування на атаку та мінімізації її впливу, включаючи відновлення роботи системи у разі DoS-атаки чи маніпуляції з параметрами захисного обладнання.
Вразливість до нападних осіб	Рейтинги безпеки	Загальна оцінка рівня безпеки критичних елементів енергетичної інфраструктури, зокрема автоматизованих систем управління, диспетчеризації та трансформаторних вузлів.
Відкладене оновлення	Патчінг Cadence	Час, потрібний для впровадження оновлень системи кібербезпеки, що захищають енергетичну інфраструктуру від нових загроз.

Кінець таблиці 3.1

1	2	3
Неконтрольований доступ	Контроль доступу та аналіз прав доступу	Перевірка прав доступу до системи управління енергосистемами, зокрема виявлення невиправданих адміністративних прав користувачів.
Ризики від підрядників чи третіх сторінок	Час реагування третьої сторони на інцидент	Час, який потрібен підрядникам чи партнерам для реагування на кібератаку, може негативно вплинути на функціонування системи енергозабезпечення.

Рівень готовності вказує на здатність системи оперативно реагувати на загрози. Показник виявляє, наскільки справними є пристрої, наскільки актуальним є програмне забезпечення та як швидко можна усунути вразливість. Високий рівень готовності мінімізує ризики збоїв, спричинених застарілим обладнанням чи відсутністю оновлень.

Виявлення несанкціонованих пристроїв проявляється при появі деяких дефектів на безпеці мережевої інфраструктури. Якщо в мережі є невідомі пристрої, вони можуть бути джерелом загроз, таких як несанкціонований доступ або маніпуляція даними. Високий рівень виявлення дозволяє уникнути цих ризиків.

Спроби проникнення відображають активність зловмисників і рівень захисту системи. Велика кількість спроб підвищує ризики успішної атаки, що може вплинути на стабільність роботи енергетичних систем. Ефективні заходи захисту знижують частоту таких інцидентів.

Безпека інцидентів впливають на здатність системи виконувати свої функції без порушення. Кількість інцидентів вказує на вразливість системи та ефективність поточних заходів кібербезпеки. Зміна цього показника знижує ймовірність збоїв у постачанні електроенергії.

Середній час виявлення (MTTD) досягнення швидкості реакції на загрозу. Чим коротший цей час, тим менший ризик того, що встигне завдати значних збитків. Це вказує на ефективність моніторингових систем і аналітики загроз.

Середній час реагування (MTTR) впливає на тривалість збоїв у роботі системи. Швидке реагування дозволяє мінімізувати наслідки кібератаків і забезпечити швидке відновлення нормальної роботи. Високий показник MTTR можна призвести до значних втрат через тривалі зупинки.

Рейтинги безпеки відображають загальний рівень захищеності інфраструктури. Ці рейтинги впливають на довіру до системи з боку регуляторів, партнерів та клієнтів. Високий рейтинг безпеки забезпечує стабільність і знижує ризики репутаційних втрат.

Патчінг Cadence впливає на ризик успішних атак через вразливість у програмному забезпеченні. Чим швидше впроваджуються оновлення, тим менше шансів, що зловмисники використають відомі вразливості. Затримки в оновленнях збільшують ризики атаки.

Контроль доступу та аналіз прав доступу до системи захисту критичних функцій. Неправильно налаштовані права доступу можуть дозволити зловмисникам маніпулювати параметрами системи роботи. Ефективний контроль доступу зменшує ці ризики.

Час реагування третьої сторони впливає на здатність партнерів чи підрядників підтримувати безпеку системи. Затримки у реакції можуть призвести до розширення атак та збільшення збитків. Ефективна робота з третіми сторонами створює загальну стійкість системи.

Відстеження цих показників є необхідним для виявлення слабких місць у системі кібербезпеки, оцінки її поточного стану та ефективності впровадження захисних заходів. Це дозволяє не тільки виявити поточні загрози та точки вразливості, але й забезпечити основу для розробки комплексних стратегій своєчасного реагування на кібератаки, оптимізації процесів захисту, стабільної та безперебійної роботи енергетичної інфраструктури

3.2 Розроблення рекомендацій щодо впровадження захисних стратегій

У цьому підрозділі представлені практичні рекомендації щодо впровадження інноваційних технологій для підвищення кібербезпеки. Основну увагу приділено таким напрямкам:

- використання штучного інтелекту для виявлення аномалій у реальному часі;
- інтеграція технологій блокчейну для забезпечення захисту даних;
- впровадження адаптивних алгоритмів, що дозволяють динамічно реагувати на нові загрози.

Рекомендації базуються на аналізі успішних кейсів впровадження та досвіді попередніх досліджень.

У сучасних кіберфізичних системах енергетичного сектора впровадження інноваційних технологій є ключовим для підвищення рівня кібербезпеки. Нижче наведено рекомендації щодо використання таких технологій.

3.2.1 Використання штучного інтелекту для виявлення аномалій у реальному часі

Штучний інтелект є одним із ключових інструментів для підвищення рівня кібербезпеки в сучасних кіберфізичних системах енергетичного сектора. Завдяки своїм унікальним можливостям, ШІ може аналізувати велику кількість ідентифікаційних даних, враховувати нормальну поведінку системи та оперативно реагувати на кібератаки. Використання алгоритмів машинного навчання, таких як нейронні мережі LSTM і метод ізоляційного лісу (Isolation

Forest), демонструє високу ефективність при виявленні аномалій у часових рядах даних.

Нейронні мережі LSTM, зокрема, використовують для моделювання часових рядів, що дозволяє ідентифікувати як короткострокові, так і довгострокові аномалії. Їхня здатність адаптуватися до динамічних змін у даних забезпечує ефективне реагування на нові загрози. Метод Isolation Forest, наприклад, використовує для ізоляції аномальних точок у великих наборах даних. Він особливо корисний для виявлення рідкісних подій, які можуть залишитися непоміченими іншими методами. Такі підходи підтверджені результатами наукових досліджень, зокрема у роботі [72], що описує переваги цих методів на етапі попередньої обробки даних.

Кодувальники-декодувальники також знаходять своє застосування в завданнях глибокого навчання. Ці моделі дозволяють виявити аномалії шляхом реконструкції даних, що є особливо корисним для роботи з наборами даних без міток.

Запропоновано алгоритм виявлення аномалій, що охоплює весь процес: від завантаження та попередньої обробки даних до порівняльного аналізу методів Isolation Forest і LSTM. На першому етапі здійснюється імпорт даних, перевірка їх якості, заповнення відсутніх значень і нормалізація. Потім аналізуються часові ряди, що включає візуалізацію трендів і виявлення особливостей, таких як сезонність чи раптові зміни.

На наступних етапах створюються та навчаються моделі Isolation Forest і LSTM. Перший фокусується на ізоляції аномальних точок через багатовимірний аналіз, тоді як другий аналізує функцію втрат, що визначає аномалії на основі порогового значення. Оцінка ефективності цих моделей проводиться шляхом порівняння їхньої точності, швидкості роботи та здатності ідентифікувати рідкісні події.

Штучний інтелект також активно використовується для аналізу мережевого трафіку. Він здатний у реальному часі ідентифікувати підозрілі

події, які свідчать про кібератаки, та автоматизувати реагування на загрози. Це включає класифікацію та нейтралізацію загрози без втручання людини, що знижує ризик помилок і прискорює час реагування.

З постійним розвитком технологій ШІ та алгоритмів машинного навчання з'явилися нові можливості для виявлення аномалій і реагування на загрози. Вдосконалення моделей спрямоване на підвищення їх точності та адаптивності до нових типів атак. Це відкриває широкі перспективи для використання ШІ не тільки в енергетиці, а й у фінансовій сфері, охороні здоров'я та інших галузях, де надійність і безпека мають критичне значення.

3.2.2 Інтеграція технологій блокчейну для забезпечення захисту даних

Блокчейн забезпечує децентралізоване, незмінне та захищене зберігання даних, що гарантує їхню цільність та захист від несанкціонованого доступу. В енергетичному секторі ця технологія може використовуватися для захисту інформації про транзакції, моніторинг енергоспоживання, а також управління розподіленими джерелами генерації. Дослідження підтверджують, що впровадження блокчейну сприяє підвищенню прозорості операцій та зміцненню рівня кібербезпеки енергетичних систем.

Однією з ключових переваг блокчейну є можливість відстеження походження відновлюваної енергії від генерації до кінцевого споживача. Це дозволяє сформувати достовірні дані щодо низьковуглецевих характеристик виробленої електроенергії та її відповідності екологічним стандартам. Технологія блокчейну містить інформацію про час роботи генераційних потужностей, їх місце розташування та рівень вуглецевих викидів, що відкриває нові перспективи для створення «зелених» сертифікатів. Наприклад,

високоінтелектуальні сонячні панелі можуть напряму передавати дані про власну генерацію в блокчейн, що унеможливлює фальсифікацію даних [73].

Ще одним напрямом розвитку блокчейну в енергетиці є використання цифрових контрактів, які явно можуть замінити традиційні договірні угоди у сфері електропостачання. Ці цифрові контракти автоматично виконуються при виконанні визначених умов, оминаючи потребу у посередниках. Вони можуть включати механізми автоматизованих платежів та передачі активів за умови утримання договірних умов. Завдяки цьому можна оптимізувати розрахунки між учасниками ринку, зменшити витрати на адміністрування та підвищити рівень довіри до проведених операцій. Кожна транзакція в межах розумного договору проходить перевірку та фіксується в розподіленому реєстрі, що виключає можливість її підробки чи несанкціонованого коригування.

Великі міжнародні енергетичні компанії активно розробляють проекти, спрямовані на об'єднання споживачів в єдину децентралізовану мережу, що дозволяє значно оптимізувати операційні процеси. Впровадження блокчейн-рішень спрощує багаторівневу структуру електроенергії, в яку входять виробники, оператори розподільних мереж, постачальники послуг, фінансові інститути ринку, трейдери та кінцеві споживачі. Завдяки взаємодії з використанням технології блокчейн виконання умов контрактів між усіма цими суб'єктами може відбуватися без посередників, що не лише зменшує транзакційні витрати, а й дасть можливість зниження вартості електроенергії для кінцевого споживача.

Використання блокчейну також дасть можливість значно підняти рівень захисту енергетичної інфраструктури. Завдяки децентралізованій природі цієї технології забезпечується стійкість до кібератак, оскільки відсутній єдиний максимальний точковий вузол, який може бути скомпрометований. Усі потоки електроенергії та фінансові операції фіксуються у розподіленому реєстрі, що робить їх незмінними та захищеними від зовнішніх утручань. Крім того,

блокчейн може використовуватися для сертифікації електроенергії та контролю за дотриманням квот на викиді парникових газів.

Децентралізована структура блокчейну також дозволяє створити універсальну базу даних, в якій зберігаються дані про встановлені тарифи, рахунки за електроенергію, історію платежів та контрактів. Усі записи доступні в режимі реального часу, що забезпечує прозорість ринку та зменшує можливості для шахрайства [74].

Розвиток блокчейн-технологій у секторі електроенергетики включає створення спеціалізованих додатків, що вибирають концепцію цифрових контрактів для управління децентралізованими енергетичними мережами (табл. 3.2.). Таким рішенням заборонено формувати автономні організаційні підрозділи , які можуть працювати з мінімальним втручанням операторів.

Таблиця 3.2 - Застосування блокчейну в енергетиці [75]

Транзакції та цифрові контракти	Права власності та управління активами	Децентралізовані інформаційні системи
1	2	3
Можливість угод між виробниками та споживачами без посередників, що знижує вартість транзакцій та забезпечує прозорість обігу електроенергії.	Забезпечення цифрової ідентифікації власників енергетичних ресурсів, виключаючи можливість шахрайських маніпуляцій.	автоматизований моніторинг за витратами енергії та формування розрахунків на основі фактичного споживання.
Доступ до персоналізованих пропозицій від постачальників, що дозволяє досконало вибирати тарифи та джерела енергії.	Блокчейн забезпечує прозорий механізм реєстрації "зелених" сертифікатів	Створення локалізованої системи обліку, що зменшує витрати та підвищує ефективність комунальних розрахунків.
Можливість здійснення розрахунків у цифрових активах, що спрощує міжнародні енергетичні угоди та дозволяє оптимізувати фінансові потоки.	Впровадження блокчейну дозволяє прозоро обліковувати викиди та дотримуватись екологічних стандартів.	Безпечні транзакції без потреби у проміжних фінансових установах, в тому числі і за зарядку електромобілів

Кінець таблиці 3.2

1	2	3
Зарядка електромобілів - створення децентралізованих станцій для автономного процесу керування зарядкою.	Реєстрація даних про власників та стан зарядних станцій - створення єдиного реєстру для управління інфраструктурою електротранспорту.	Збереження всіх даних під час зарядки у блокчейні, що виключає можливість маніпуляції або фальсифікації.
Управління SMART-пристроями - створення автономних енергетичних систем на основі розумних пристроїв.	Інтеграція в інтернет-речей для покращення управління споживанням - застосування смарт-контрактів для оптимізації роботи пристроїв залежно від енергетичного навантаження.	Взаємодія між «розумними» системами для підвищення енергоефективності - блокчейн забезпечує автоматичний обмін даними між IoT-пристроями, підвищуючи ефективність їх роботи.

Впровадження децентралізованого механізму укладення угод на енергетичний ринок може суттєво збільшити частки електроенергії, отриманої із відновлюваних джерел. Завдяки блокчейну створюється прозора, надійна та незмінна система обліку, яка дозволяє виробникам зеленої енергії напряму взаємодіяти із споживачами без посередників. Такий підхід забезпечує підвищення довіри до ринку та сприяє більш ефективному розподілу електроенергії між учасниками.

Однією з ключових переваг блокчейну є можливість чіткого відстеження джерела енергії, що надходить у загальну мережу. Це дозволяє кожному покупцеві отримувати гарантії того, що придбана ним електроенергія вироблена саме з використанням відновлюваних джерел. Завдяки цьому механізму блокчейн може стати основою для формування «зелених» сертифікатів та підтвердження вуглецевої нейтральності електроенергії. Крім того, така технологія дозволяє автоматично контролювати відповідність постачальників екологічним стандартам та вимогам до квот на викиди.

Для успішного впровадження блокчейну в енергетичну галузь необхідно створити спеціальні правові рамки та нормативні акти, які виконують особливості цієї технології та забезпечують її законність. Регулювання має

охоплювати аспекти захисту даних, конфіденційності, використання смарт-контрактів, механізмів транзакцій та інтеграції блокчейн-систем із традиційними моделями ринку. Відповідне нормативне забезпечення дозволить мінімізувати правові ризики, які можуть виникати при впровадженні цієї технології в регульованому секторі енергетики [76].

Загалом, застосування блокчейну в енергетичному секторі створює передумови для децентралізації ринку, підвищує прозорість взаємодії між учасниками та ефективного використання відновлюваних джерел енергії.

3.2.3 Впровадження адаптивних алгоритмів для динамічного реагування на нові загрози

Адаптивні алгоритми здатні навчатися на основі нових даних та аналізувати зміни в структурі атаки, що дозволяє їм динамічно реагувати на нові загрози. Такі ваші системи можуть автоматично коригувати ваші методи захисту та захисту в реальному часі, забезпечуючи проактивний підхід до кібербезпеки. Застосування ШІ в системі та запобіганні кібератакам дозволяє підвищити ефективність, точність та автоматизацію процесу виявлення загроз [77].

Ефективність адаптивних алгоритмів базується на ключових підходах. Наприклад, системи на основі машинного навчання можуть аналізувати мережевий трафік, виявляючи приховані аномалії або шаблони, які свідчать про ці загрози. Використання нейронних мереж з автокодерами дозволяє виявити аномалії шляхом аналізу відхилень між вихідними даними та їх реконструкцією. Алгоритми ізоляційного лісу забезпечують ідентифікацію рідкісних аномальних подій завдяки ефективній кластеризації даних.

Практичне впровадження таких алгоритмів потребує врахування низки аспектів. По-перше, необхідно забезпечити якість вхідних даних, включаючи

видалення дублікатів, заповнення відсутніх значень та нормалізацію даних. По-друге, необхідно адаптувати алгоритми до особливостей кіберфізичних систем енергетичного сектора, враховуючи специфічні сенсорні дані та рівні комунікації між пристроями.

В табл. 3.3. наведено рекомендації щодо впровадження адаптивних алгоритмів у кіберфізичних системах

Таблиця 3.3 - Рекомендації щодо впровадження адаптивних алгоритмів у кіберфізичних енергетичних системах

Етап	Рекомендація	Очікуваний результат
1	2	3
Попередня обробка даних	Використовуйте методи заповнення пропущених значень, видалення аномальних точок та нормалізації даних.	Забезпечення високої якості вхідних даних для аналізу.
Вибір моделей	Оберіть алгоритми, які відповідають специфікації даних, наприклад Isolation Forest для рідкісних подій або LSTM для часових рядів.	Підвищення точності виявлення загроз.
Навчання алгоритмів	Використовуйте методи перехресної перевірки та гіперпараметричної оптимізації для налаштування моделей.	Оптимізація роботи моделей та зменшення ризику гібнопозитивних результатів.
Інтеграція в системи	Інтегруйте алгоритми в існуючі платформи моніторингу, забезпечуючи їх взаємодію з іншими компонентами кіберфізичних систем.	Змінення часу реакції на загрози та автоматизація процесів реагування.
Оцінка ефективності	Регулярно перевіряйте точність, повноту та швидкість роботи моделей на нових даних, застосовуючи KPI, наприклад середній час виявлення загрози (MTTD) або середній час реагування (MTTR).	Забезпечення постійного вдосконалення алгоритмів та їх адаптації до нових загроз.

Використання адаптивних алгоритмів дозволяє значно підвищити ефективність захисту кіберфізичних систем. таким чином, це зменшує ризик втрати даних та запуску в роботі системи, забезпечує благополучне реагування на загрози та підтримує стабільність функціонування енергетичних об'єктів.

3.3 Потенційні заходи протидії загрозам кібербезпеки

Як показано, заходи протидії загрозам кібербезпеки в КФС мають класифікуватися за категоріями моделей безпеки. Однак категорія атаки може впливати на кілька категорій моделей безпеки. Зокрема, атаки, які впливають на цілісність і конфіденційність, вимагають розгортання доступу до мережі. З цієї причини заходи протидії загрозам цілісності та конфіденційності були об'єднані в цьому розділі, тоді як заходи протидії загрозам доступності розглядаються окремо. Короткий опис контрзаходів, викладених у цьому розділі, можна знайти в табл. 3.4.

Таблиця 3.4 - Опис контрзаходів при атаках на розумні мережі (SmartGrid)

Категорія безпеки	Тип атаки	Опис атаки	Контрзаходи
1	2	3	4
Доступність	Відмова в обслуговуванні (DoS)	Атаки, що спрямовані на перевантаження системи або порушують її роботу шляхом перевищення доступних ресурсів.	SIEM, IDS, контроль ентропії, аналіз сили сигналу, вимірювання часу, методи реконфігурації.
	Введення фальшивих даних (FDIA)	Створення даних у критичних системах (AMI, SCADA) для маніпуляції операційними рішеннями.	FDIA-детектори, TLS, SSL, PKI для шифрування, аутентифікації.
	Глушіння сигналу	Приглушення сигналів комунікацій через створення інтерференції.	Антиглушіння (FHSS, DSSS), системи JADE.
Цілісність	Впровадження шкідливого ПЗ	Введення вірусів або іншого шкідливого програмного забезпечення в SCADA, PMU.	DLP, IDS, SIEM, антивіруси, використання різноманітності в захисних технологіях.
	Підміна (Маскарадна атака)	Заміна автентичних даних підробленими у PLC або інших системах.	DLP, IDS, шифрування TLS/SSL, аутентифікація PKI.
	Людина всередині (MitM)	Перехоплення та модифікація даних між відправником і отримувачем (наприклад, HMI, PLC).	Протоколи DNP3, PKI, TLS/SSL, багатофакторна аутентифікація.

1	2	3	4
	Відтворення (Replay Attack)	Повторення перехоплених даних із системою маніпуляції надходженнями.	TLS, SSL, PKI, аутентифікація, захищений зв'язок.
Конфіденційність	Порушення конфіденційності	Незаконний доступ до чутливих даних (наприклад, "розумні" лічильники, програми управління попитом).	Протоколи TLS/SSL, автентифікація PKI, захист передачі даних.
	Системи сканування (сканування)	Аналіз мережевих протоколів для вразливостей (Modbus, DNP3).	SIEM, IDS, автоматизовані перевірки безпеки, фільтрація мережевого трафіку.
	Соціальна інженерія	Використання людського фактора для обману або отримання доступу до критичних даних.	Автентифікація PKI, протоколи DNP3, багатофакторна аутентифікація.
	Аналіз трафіку (Traffic Analysis)	Аналіз патернів мережевого трафіку для отримання інформації про вразливість чи структуру системи.	Шифрування PKI, SSL, захист мережевих даних.

У цій таблиці акцентовано увагу на детальних характеристиках контрзаходів, які допомагають зменшити ризик кіберзагрози та підтримати надійність і безпеку кіберфізичних систем.

3.3.1 Потенційні заходи протидії загрозам доступності

Забезпечення доступності є одним із ключових викликів для кібербезпеки в розумних енергомережах (Smart Grid). Як було раніше вказано, загрози доступності можуть мати катастрофічні наслідки, впливаючи на стабільність мережевих послуг, оцінки системи та управління. Крім того, загрози типу DoS (відмова в обслуговуванні) та FDIA (атаки з використанням помилкових даних) становлять серйозну небезпеку через можливість порушення операційних процесів і доступу до критичних даних.

Для протидії таким загрозам необхідно використовувати широкий спектр технічних та організаційних заходів, спрямованих на запобігання, виявлення та

реагування на атаки. Одним із ключових напрямків є використання фільтрації. Ефективні правила брандмауера допомагають обмежити вхідний трафік, дозволяючи лише дозволеним мережевим адресам і портам. Наприклад, у спеціалізованих розподільчих мережах (SDG) використовується "розумний відстежуючий брандмауер", який здатний ідентифікувати зловмисні вузли й блокувати їхній доступ до мережі.

Система виявлення та запобігання вторгненню (IDS/IPS) є більш гнучкими рішеннями для виявлення складних атак. IDS може розшифровувати мережевий трафік і визначати аномалії або небезпечні дії за допомогою сигнатурних, аномальних та специфікаційних підходів. Наприклад, IDS на основі сигнатури використовує базу відомих шаблонів атак, тоді як аномальні системи складаються на алгоритми машинного навчання для ідентифікації невідомих загроз. Водночас, специфікаційні IDS можуть визначити порушення шляхом порівняння систем поведінки з визначеними нормами.

Криптографічна автентифікація є ще одним компонентом протидії загрозам. Вона захищає канали передачі даних від підробки та вручення, забезпечуючи аутентифікацію та шифрування. Тим не менш, у розумних мережах криптографічні алгоритми мають легкі та енергоефективні, враховуючи використання пристроїв з обмеженими ресурсами. Наприклад, у сучасних дослідженнях пропонуються гібридні підходи, які поєднують симетричне та асиметричне шифрування для підвищення ефективності.

Архітектурні рішення також замінюють ключову роль у забезпеченні доступності. Впровадження так званих "острівних" систем дозволяє ізолювати частини мережі у разі атак, які дозволяють іншим сегментам продовжувати роботу до повного відновлення основної мережі. Наприклад, технології "острівного" дизайну можуть бути застосовані для мінімізації впливу DoS-атак на критичні вузли.

"Медові горщики" є перспективним інструментом для виявлення атаки на ранніх стадіях. Ці пристрої імітують поведінку легітимних систем, приваблюючи

зловмисників та дозволяючи службам безпеки ідентифікувати методи атак. Наприклад, Conpot є ефективним інструментом з відкритим вихідним кодом, який використовується для виявлення загроз в інтелектуальних мережах.

Системно-теоретичні рішення зосереджені на виявленні за типом FDIA. Алгоритми, засновані на моделях і даних, дозволяють ідентифікувати аномалії в реальному часі, використовуючи машинне навчання та методи інтелектуального аналізу. Наприклад, методи динамічної оцінки стануть отримані історичні дані для прогнозування аномалій і корекції операцій.

Можливо, одним з найскладніших аспектів захисту мереж ІКС в цілому є впровадження ефективних заходів протидії загрозам шкідливого програмного забезпечення. Деякі нещодавні гучні атаки, включаючи Stuxnet і Havex, використовували вразливості нульового дня і приховування. Як правило в таких випадках пропонується використовувати багаторівневі стратегії (тобто, глибокий захист) для пом'якшення деяких з цих загроз, серед іншого. Ефективний захисний периметр для КФС мережі, як показано на рис.3.2, може запобігти запуску деяких з цих атак. Однак, через неправильні конфігурації, бекдори тощо, це не є гарантією. IT-сторона мережі також повинна використовувати захист кінцевих точок, SIEM тощо, щоб виявити відомі загрози. Однак існують також загрози "нульового дня", загрози ланцюжка поставок, загрози соціальної інженерії, USB-пристрої зі шкідливим програмним забезпеченням тощо.

Результатом реалізації таких заходів є підвищення стійкості енергосистеми до загроз, пов’язаних із порушенням доступності, а також створення надійного середовища для функціонування критичної інфраструктури. Впровадження цих заходів потребує інтеграції новітніх технологій, удосконалення процесів управління та навчання персоналу, що забезпечує захист від нападу нового покоління.

На рис. 3.2 проілюстровано варіант багаторівневої архітектури кібербезпеки, яка спрямована на захист критичних компонентів виробничої

системи. Вона складається з кількох зон, що забезпечують сегмент мережі для мінімізації ризиків та ізоляції критично важливих елементів.

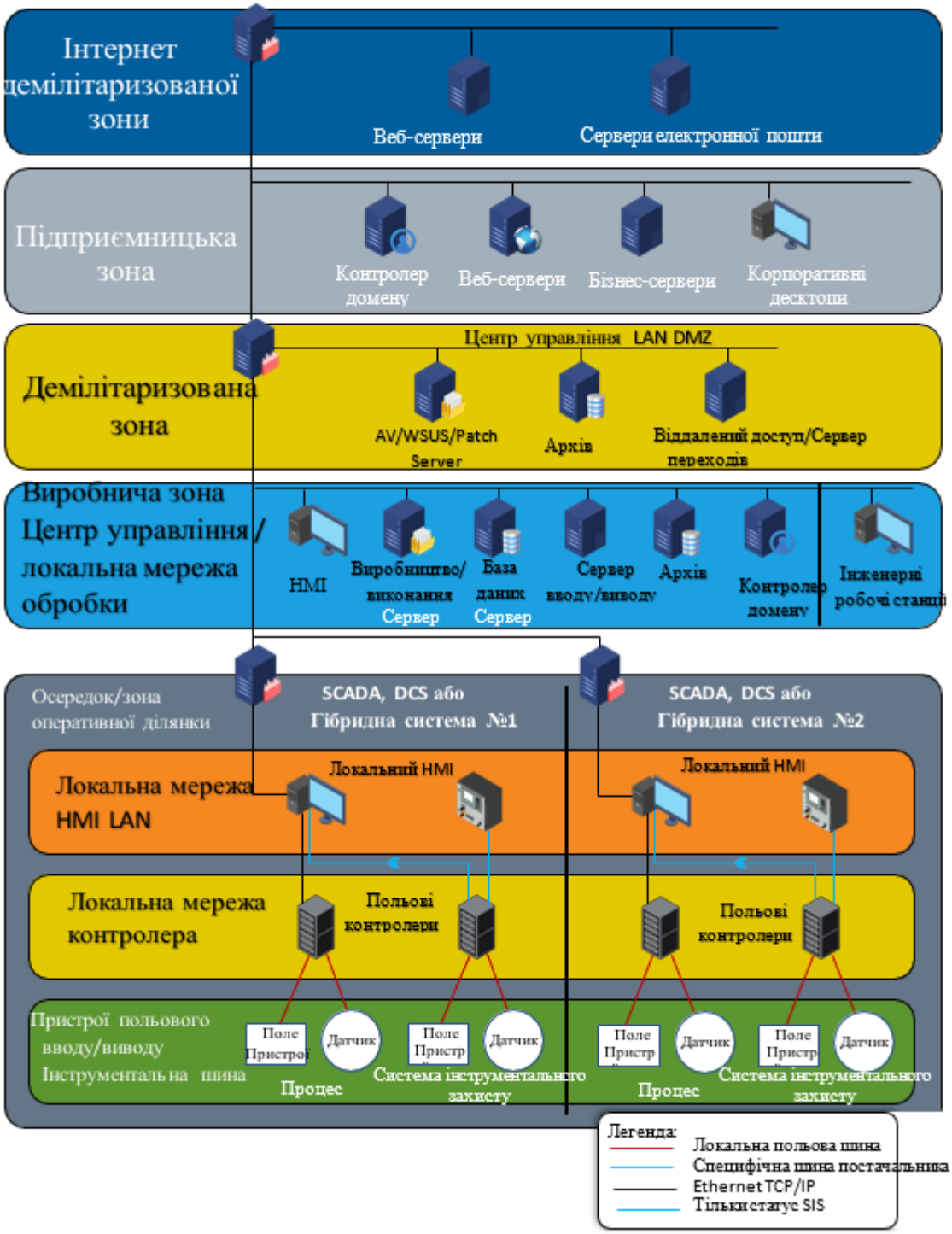


Рисунок 3.2 - Рекомендована безпечна архітектура КФЕС

У верхній частині зображено інтернет-демілітаризовану зону, яка містить веб-сервери та сервери електронної пошти, що забезпечують зв’язок із зовнішнім світом. Нижче розташована підприємницька зона з контролером домену, бізнес-серверами, веб-серверами та корпоративними десктопами, які керують офісними операціями.

Демілітаризована зона використовується для захисту внутрішньої мережі від зовнішніх загроз і включає сервери патчів, хронологічні історичні сервери, архіви, інструменти для моніторингу доступу, а також центри управління локальною мережею.

Виробнича зона та локальна мережа обробки даних забезпечують безперебійну роботу критичних систем, включаючи HMI, виробничі сервери, архіви даних та інструменти для аналізу виробничих процесів. Осередки управління та SCADA-системи об'єднують локальні мережеві контролери з пристроями польового рівня, забезпечуючи моніторинг та управління технологічними процесами.

Захист кожного рівня досягається за допомогою сегментації мережі, використання брендмауерів, контролю доступу, архітектурних рішень та інтегрованих засобів моніторингу. Легенда малюнка демонструє основні протоколи зв'язку та схеми підключення, які використовують для забезпечення безпеки.

3.3.2 Потенційні заходи протидії загрозам цілісності та конфіденційності

Загрози кібербезпеці, що впливають на цілісність комунікації ІКС, часто націлені на конкретні протоколи. Протоколи Modbus та DNP3, сумісні зі старими послідовними пристроями, особливо вразливі до підслуховування та зміни даних. Основні загрози кібербезпеці, які впливають на конфіденційність в

інтелектуальній мережі, в першу чергу зосереджені на вдосконаленій інфраструктурі обліку (AMI). AMI - це система інтелектуальних лічильників, комунікаційних мереж та систем управління даними, яка забезпечує двосторонній зв'язок між споживачами та комунальними службами. Цей двосторонній зв'язок забезпечує кращий моніторинг та більш точне виставлення рахунків за комунальні послуги, а також більш точну поведінку споживачів щодо споживання. Однак, оскільки все більше споживачів використовують цю модель, збільшується кількість точок доступу для атак на безпеку.

В обох цих випадках шифрування є ефективним контрзаходом для забезпечення цілісності та конфіденційності даних. Протокол захищеного зв'язку IEEE Secure SCADA Communications Protocol (SSCP) – це спрямовані на застосування шифрування при послідовній реалізації протоколів. Поєднання цих контрзаходів усуває розрив між безпекою застарілих пристроїв та їхніх сучасних аналогів СВУ.

3.4 Рекомендовані стратегії аналізу прогалин для забезпечення кібербезпеки в енергетичному секторі

Аналіз прогалин у кібербезпеці є критичним місцем для енергетичного сектора, де загрози можуть суттєво вплинути на доступність, цільність і конфіденційність критичних систем. NIST пропонує структуру кібербезпеки, яка базується на п'яти функціях: ідентифікація, захист, виявлення, реагування та відновлення. Ця структура надає системний підхід до досягнення прогалин та їх подальшого усунення, забезпечуючи комплексну основу для управління ризиками [78].

Функція «Ідентифікація» зосереджується на визначених активах організації та їхніх ризиків у контексті результатів кіберзагроз. Організація має

розробити чіткий перелік критичних функцій та активів, включаючи компоненти мережі, обладнання та дані, які потребують захисту. Управління ризиками ланцюга постачання, оцінка ризиків та бізнес-середовище є ключовими категоріями, які дозволяють організації адаптувати свій профіль ризиків. Недоліки на цьому етапі можуть призвести до серйозних прогалин у захисті, після чого нерозпізнані активи залишаються незахищеними.

Функція «Захист» має на меті створення гарантій для забезпечення надання інфраструктурних послуг навіть у разі загрози. Вона охоплює заходи безпеки, зокрема контроль доступу, безпеку даних, навчання персоналу, технічне обслуговування та захисні технології. Наприклад, впровадження системи контролю доступу до допомоги запобігти атакам типу "людина посередині", а криптографічні технології забезпечують захист від порушення конфіденційності. У цій функції інтегруються ключові контрзаходи, представлені в попередніх розділах, з акцентом на практичну реалізацію захисних технологій.

Функція «Виявлення» орієнтована на ідентифікацію будь-яких кіберінцидентів через безперервний моніторинг та аналіз. Це включає виявлення аномалій, моніторинг подій і застосування алгоритмів штучного інтелекту для швидкої ідентифікації загроз. Наприклад, виявлення системи вторгнення (IDS) може розпізнавати складні сценарії атаки, використовуючи алгоритми машинного навчання та моделі аномальної поведінки. вибір вибору загроз, ця функція також оцінює їх масштаб та можливості слідки для системи.

Функції «Реагування» і «Відновлення» спрямовані на мінімізацію впливу атак та забезпечення швидкого повернення до нормального функціонування. Реагування передбачає розробку планів дій, аналіз ситуацій, пом'якшення наслідків та вдосконалення процесів. Наприклад, певне планування комунікацій між цікавими сторонами може скоротити час реакції на кіберзагрозу. Функція відновлення охоплює розробку процедури відновлення сервісів після інциденту та врахування уроків для покращення майбутніх заходів. Ці функції базуються

на плануванні заздалегідь, що дозволяє мінімізувати вплив інцидентів і підвищити готовність до майбутніх загроз.

Ключовим елементом впровадження цієї системи є розробка профілю організації, що забезпечує її рівень захищеності. NIST пропонує чотири рівні кібербезпеки: частковий, інформований про ризики, повторюваний та адаптивний. Кожен із рівнів характеризується дедалі суворішими стандартами захисту. Наприклад, на початковому рівні організації реагує на ризики без формалізованих політик, тоді як адаптивний рівень включає передові технології та розвинені практики управління ризиками.

Мета цієї системи - допомогти зацікавленим сторонам будь-якої організації ідентифікувати, оцінювати та управляти будь-якими ризиками, які можуть бути в їхній організаційній мережі. Відповідність цій системі може виглядати дуже по-різному в різних організаціях, тому NIST також пропонує кроки для впровадження або вдосконалення програми кібербезпеки:

- визначте пріоритети та сферу застосування;
- визначте напрямок руху;
- створіть поточний профіль;
- проведіть оцінювання ризиків;
- створіть цільовий профіль;
- виокремте, проаналізуйте та визначте пріоритети;
- впроваджуйте план дій.

Щоб допомогти у визначенні цільового профілю, NIST також пропонує набір з чотирьох рівнів, на які організація може посилатися для своїх цілей управління. Існує 4 рівні: частковий, інформований про ризики, повторюваний та адаптивний. Чим вищий рівень, тим суворіші засоби захисту, які застосовуються в організації. Наприклад, на рівні 1 (частковому) не існує формалізованих політик, а організація вирішує кожен ризик індивідуально, без процедури, що розвивається. Ці рівні розширюють обізнаність про кібербезпеку та пом'якшення ризиків аж до адаптивного, де впроваджуються передові технології та

розвиваються практики управління ризиками для боротьби з поточними та минулими загрозами кібербезпеки.

3.5 Висновки розділу 3

В розділі розроблені рекомендації і практичні аспекти застосування методів кібербезпеки в кіберфізичних енергетичних системах. Представлено також заходи протидії загрозам доступності, цілісності та конфіденційності в розумних мережах (Smart Grid).

В результаті отримали такі висновки:

- запропоновані метрики, такі як середній час виявлення та реагування на загрози, що дозволяють оцінювати ефективність захисту системи. Розробка KPI та KRI дозволяє ідентифікувати слабкі місця та вдосконалювати заходи кібербезпеки;
- використання штучного інтелекту забезпечить аналіз аномалій у реальному часі, блокчейн дозволяє підвищити прозорість транзакцій і захист даних, а адаптивні алгоритми створюють можливість динамічного реагування на нові загрози;
- впровадження системи IDS/IPS, криптографічних алгоритмів, фільтрації мережевого трафіку та архітектурних рішень, таких як "острівний дизайн", мінімізує ризики нападу на доступність, цільність та конфіденційність;
- методологія NIST із п'ятьма функціями (ідентифікація, захист, виявлення, реагування та відновлення) надає ефективний інструментарій для виявлення та усунення прогалин у кібербезпеці енергетичних систем.

ВИСНОВКИ

На основі виконаного дослідження в магістерській роботі сформульовано наступні висновки:

- у ході дослідження визначено, що енергетичний сектор залишається критично важливою інфраструктурою, яка постійно піддається ризику кіберзагроз. Вивчено типологію кібератак, серед яких найбільш поширені DoS-атаки, ін'єкція фальшивих даних (FDIA), та атаки на конфіденційність даних. Проаналізовано архітектуру кіберфізичних систем і виявлено ключові вразливості, що стосуються синхронізації часу, автентифікації та безпеки мережевих протоколів. Проведено огляд актуальних стандартів кібербезпеки, таких як NIST CSF і IEC 62351, та визначено необхідність їх адаптації до сучасних загроз;
- запропоновано методологію, що включає використання штучного інтелекту, блокчейну та адаптивних алгоритмів для забезпечення моніторингу, управління та захисту кіберфізичних систем. Розроблено критерії оцінки ефективності запропонованих стратегій, включаючи швидкість виявлення загроз, точність і адаптивність до нових видів атак. Методи, засновані на нейронних мережах LSTM і ізоляційних лісах (Isolation Forest), довели свою ефективність у виявленні аномалій у часових рядах енергетичних систем;
- запропоновано використання адаптивних алгоритмів для аналізу та виявлення аномалій у даних, зібраних з енергетичних систем. Алгоритми LSTM і Isolation Forest показали високу точність у виявленні аномалій, забезпечуючи зменшення часу реакції на загрози. Проведено порівняльний аналіз, який продемонстрував переваги адаптивних алгоритмів у реальних умовах. На основі аналізу результатів запропоновано рекомендації щодо впровадження захисних стратегій, що включають побудову інтегрованих рішень на базі хмарних обчислень і децентралізованих технологій;

- для забезпечення комплексного захисту запропоновано впроваджувати системи на основі блокчейну для безпечного обміну даними, використовувати IDS/IPS для безперервного моніторингу та впроваджувати політики управління ризиками. Визначено перспективи застосування квантових технологій для забезпечення криптографічного захисту, а також розробки нових стандартів для адаптації до викликів цифрової трансформації.

Перспективи подальших досліджень. Робота підтверджує важливість інтеграції інноваційних технологій у забезпечення кібербезпеки кіберфізичних енергетичних систем. Отримані результати створюють основу для подальшого розвитку кібербезпеки кіберфізичних енергетичних систем. Перспективними напрямами є створення багаторівневих платформ для моделювання кібератак, впровадження квантово-стійких алгоритмів шифрування та адаптація наявних стандартів до нових загроз. Також важливим залишається дослідження впливу новітніх технологій, таких як Інтернет речей і квантові обчислення, на безпеку енергетичних систем. У перспективі дослідження має бути зосереджено на вдосконаленні адаптивних рішень, розробленні нових моделей оцінювання ризиків та стандартизації технологій для підвищення стійкості енергетичних систем до сучасних загроз.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Карпуков Л.М., Павленко В.М. Інтеграція відновлюваних джерел і кіберзахист у сучасних енергетичних системах. Матеріали VIII Міжнародної науково-технічної конференції "Енергоефективність та енергетична безпека електроенергетичних систем", НТУ "Харківський політехнічний інститут", 26-29 листопада 2024р. Харків, 2024.
2. Сердюк А.І, Павленко В.М., Інтелектуальні системи управління енергетичними потоками для забезпечення стійкості електромереж. Матеріали VIII Міжнародної науково-технічної конференції "Енергоефективність та енергетична безпека електроенергетичних систем", НТУ "Харківський політехнічний інститут", 26-29 листопада 2024р. Харків, 2024.
3. Institute for Security Technology Studies. Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report. 2004. Available online: https://priv.gg/e/ISTSLawEnforcementResearchandDevelopmentAgendaJune2004.pdf.
4. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Cybersecurity and cyber terrorism-in energy sector–a review. *J. Cyber Secur. Technol.***2018**, *2*, 111–130.
5. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. IEEE Trans. Smart Grid 2019, 11, 2218–2234.
6. Liu, C.C.; Bedoya, J.C.; Sahani, N.; Stefanov, A.; Appiah-Kubi, J.; Sun, C.C.; Lee, J.Y.; Zhu, R. Cyber–Physical System Security of Distribution Systems. Found. Trends®Electr. Energy Syst. 2021, 4, 346–410.
7. Vaidya, T. 2001–2013: Survey and Analysis of Major Cyberattacks. arXiv 2015, arXiv:1507.06673.

8. Hemsley, K.; Fisher, R. A History of Cyber Incidents and Threats Involving Industrial Control Systems. In Critical Infrastructure Protection XII, Proceedings of the 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, 12–14 March 2018; Springer: Berlin/Heidelberg, Germany, 2018; Volume 542.
9. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064.
10. Baezner, M.; Robin, P. *Stuxnet*; Center for Security Studies (CSS), ETH Zürich: Zürich, Switzerland, 2017; pp. 1–14.
11. Saxena, S.; Bhatia, S.; Gupta, R. Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey. *Designs* **2021**, *5*,52.
12. Case. Defense Use. Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *388*, 1–29. Available online: https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf
13. Muthuppalaniappan, M.; Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Int. J. Qual. Health Care* **2021**, *33*, mzaa117.
14. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Cybersecurity and cyber terrorism-in energy sector–a review. *J. Cyber Secur. Technol.* **2018**, *2*, 111–130.
15. Pate, A. Terrorism Trends with a Focus on Energy and Mining. *START Res. Brief* **2015**, 1–2. Available online: https://www.start.umd.edu/pubs/START_TerrorismEnergyAttacks_ResearchBrief_June2015.pdf
16. Karamdel, S.; Liang, X.; Faried, S.O.; Mitolo, M. Optimization Models in Cyber-Physical Power Systems: A Review. *IEEE Access* **2022**, *10*, 130469–130486.

17. He, S.; Zhou, Y.; Lv, X.; Chen, W. Detection Method for Tolerable False Data Injection Attack Based on Deep Learning Framework. In Proceedings of the Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; pp. 6717–6721.
18. Du, D.; Zhu, M.; Li, X.; Fei, M.; Bu, S.; Wu, L.; Li, K. A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 727–743.
19. Surya, S.; Srinivasan, M.K.; Williamson, S. Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review. *Appl. Sci.* **2021**, *11*, 8780.
20. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27.
21. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inf.* **2017**, *13*, 411–423.
22. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 14226.
23. Brar, H.S.; Kumar, G. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.* **2018**, *2018*, 1798659.
24. Baheti, R.; Gill, H. Cyber-physical systems. *Impact Control Technol.* **2011**, *12*, 161–166.
25. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97.
26. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
27. Cyber-Physical Systems Security -- A Survey [Електронний ресурс] // IEEE Internet of Things Journal PP(99). – 2017

28. ADMS Advanced Distribution Management System Grid Modernization Redefined. Integrated Distribution Planning, eSCADA, DMS & OMS Solution 2017 ETAP / Operation Technology, Inc. B12-ETAPADMS- JAN2017
29. Paul, S.; Ding, F.; Utkarsh, K.; Liu, W.; O'Malley, M.J.; Barnett, J. On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review. *IEEE Syst. J.* **2022**, *16*, 2367–2378.
30. Gabbar, H.A. Chapter 2—Smart energy grid infrastructures and interconnected micro energy grids. In *Smart Energy Grid Engineering*; Academic Press: Cambridge, MA, USA, 2017; pp. 23–45.
31. Gumaei, A.; Hassan, M.M.; Huda, S.; Hassan, M.R.; Camacho, D.; Ser, J.D.; Fortino, G. A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Appl. Soft Comput.* **2020**, *96*, 106658.
32. Davidson, C.; Andel, T.; Yampolskiy, M.; McDonald, T.; Glisson, B.; Thomas, T. On SCADA PLC and fieldbus cyber-security. In Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018, Washington, DC, USA, 8–9 March 2018; pp. 140–148.
33. Ghaleb, A.; Zhioua, S.; Almulhem, A. On PLC network security. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 62–69.
34. Alsabbagh, W.; Langendörfer, P. A Flashback on Control Logic Injection Attacks against Programmable Logic Controllers. *Automation* **2022**, *3*, 596–621.
35. Han, S.; Lee, K.; Cho, S.; Park, M. Anomaly Detection Based on Temporal Behavior Monitoring in Programmable Logic Controllers. *Electronics* **2021**, *10*, 1218.
36. Hajda, J.; Jakuszewski, R.; Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems. *Appl. Sci.* **2021**, *11*, 9785.
37. Khan, M.T.; Tomi´c, I. Securing Industrial Cyber–Physical Systems: A Run-Time Multilayer Monitoring. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6251–6259.

38. І.В. Касаткіна, С.М. Бойко, О.А. Жуков. Інтелектуальні системи електропостачання. Навчальний посібник/ І.В. Касаткіна, С.М. Бойко, О.А. Жуков – 2023. – 151 с.

39. Hasan, M.K.; Habib, A.K.M.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *J. Netw. Comput. Appl.* 2023, *209*, 103540.

40. Khan, M.T.; Tomi´c, I. Securing Industrial Cyber–Physical Systems: A Run-Time Multilayer Monitoring. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6251–6259.

41. Liu, J.; Zhang, W.; Ma, T.; Tang, Z.; Xie, Y.; Gui, W.; Niyoyita, J.P. Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection. *Expert Syst. Appl.* **2020**, *158*, 113578.

42. Marino, D.L.; Wickramasinghe, C.S.; Tsouvalas, B.; Rieger, C and M. Manic. Data-Driven Correlation of Cyber and Physical Anomalies for Holistic System Health Monitoring. *IEEE Access* **2021**, *9*, 163138–163150.

43. Fausto, A.; Gaggero, G.B.; Patrone, F.; Girdinio, P.; Marchese, M. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures. *Sensors* **2021**, *21*, 6970.

44. Venkataramanan, V.; Hahn, A.; Srivastava, A. CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency. *IEEE Trans. Smart Grid* **2020**, *11*, 1055–1065.

45. Li, Q.; Meng, S.; Zhang, S.; Wu, M.; Zhang, J.; Ahvanooey, M.T.; Aslam, M.S. Safety Risk Monitoring of Cyber-Physical Power Systems Based on Ensemble Learning Algorithm. *IEEE Access* **2019**, *7*, 24788–24805.

46. Alghassab, M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* **2022**, *15*, 218.

47. Choi, M.K.; Yeun, C.Y.; Seong, P.H. A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access* **2020**, *8*, 118732–118740.

48. Bin Mofidul, R.; Alam, M.M.; Rahman, M.H.; Jang, Y.M. Real-Time Energy Data Acquisition, Anomaly Detection, and Monitoring System: Implementation of a Secured, Robust, and Integrated Global IIoT Infrastructure with Edge and Cloud AI. *Sensors* **2022**, *22*, 8980.

49. Poltavtseva, M.; Shelupanov, A.; Bragin, D.; Zegzhda, D.; Alexandrova, E. Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring. *Symmetry* **2021**, *13*, 2425.

50. Chen, C.; Zhang, K.; Ni, M.; Wang, Y. Cyber-attack-tolerant Frequency Control of Power Systems. *J. Mod. Power Syst. Clean Energy* **2021**, *9*, 307–315.

51. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133.

52. Zhao, Y.; Chen, Z.; Zhou, C.; Tian, Y.C.; Qin, Y. Passivity-Based Robust Control Against Quantified False Data Injection Attacks in Cyber-Physical Systems. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1440–1450.

53. Hegazy, H.I.; Tag Eldien, A.S.; Tantawy, M.M.; Fouda, M.M.; TagElDien, H.A. Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach. *Energies* **2022**, *15*, 5312.

54. Song, J.; Huang, L.Y.; Karimi, H.R.; Niu, Y.; Zhou, J. ADP-Based Security Decentralized Sliding Mode Control for Partially Unknown Large-Scale Systems Under Injection Attacks. *IEEE Trans. Circuits Syst. I. Regul. Pap.* **2020**, *67*, 5290–5301.

55. Cao, Z.; Niu, Y.; Song, J. Finite-Time Sliding-Mode Control of Markovian Jump Cyber-Physical Systems Against Randomly Occurring Injection Attacks. *IEEE Trans. Automat. Contr.* **2020**, *65*, 1264–1271.

56. Zhang, Y.; Ma, L.; Wang, G.; Yang, C.; Zhou, L.; Dai, W. Observer-Based Control for the Two-Time-Scale Cyber-Physical Systems: The Dual-Scale DoS Attacks Case. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 3369–3379.

57. Wang, M.; Geng, Y.; Wang, J.; Liu, K.; Che, X.; Wei, Q. H ∞ Control for ICPS with Hybrid-Triggered Mechanism Encountering Stealthy DoS Jamming Attacks. *Actuators* **2022**, *11*, 193.
58. Joo, Y.; Qu, Z.; Namerikawa, T. Resilient Control of Cyber-Physical System Using Nonlinear Encoding Signal Against System Integrity Attacks. *IEEE Trans. Automat. Contr.* **2021**, *66*, 4334–4341.
59. Alsokhiry, F.; Annuk, A.; Kabanen, T.; Mohamed, M.A. A Malware Attack Enabled an Online Energy Strategy for Dynamic Wireless EVs within Transportation Systems. *Mathematics* **2022**, *10*, 4691.
60. Ameli, A.; Hooshyar, A.; El-Saadany, E.F. Development of a Cyber-Resilient Line Current Differential Relay. *IEEE Trans. Ind. Informat.* **2019**, *15*, 305–318.
61. Ameli, A.; Hooshyar, A.; El-Saadany, E.F.; Youssef, A.M. An Intrusion Detection Method for Line Current Differential Relays. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 329–344.
62. Ameli, A.; Saleh, K.A.; Kirakosyan, A.; El-Saadany, E.F.; Salama, M.M.A. An Intrusion Detection Method for Line Current Differential Relays in Medium-Voltage DC Microgrids. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3580–3594.
63. Ameli, A.; Ayad, A.; El-Saadany, E.F.; Salama, M.M.A.; Youssef, A.M. A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays. *IEEE Trans. Power Deliv.* **2021**, *36*, 2274–2286.
64. Saber, A.M.; Youssef, A.; Svetinovic, D.; Zeineldin, H.H.; El-Saadany, E.F. Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays. *IEEE Trans. Smart Grid* **2022**, *13*, 4787–4800.
65. Ganjkhani, M.; Hosseini, M.M.; Parvania, M. Optimal Defensive Strategy for Power Distribution Systems Against Relay Setting Attacks. *IEEE Trans. Power Deliv.* **2022**, *38*, 1499–1509.
66. Rajaee, M.; Mazlumi, K. Multi-Agent Distributed Deep Learning Algorithm to Detect Cyber-Attacks in Distance Relays. *IEEE Access* **2023**, *11*, 10842–10849.

67. Gutierrez-Rojas, D.; Demidov, I.; Kontou, A.; Lagos, D.; Sahoo, S.; Nardelli, P.J. Operational Issues on Adaptive Protection of Microgrids due to Cyber Attacks. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**.

68. Nuqui, R.; Hong, J.; Kondabathini, A.; Ishchenko, D.; Coats, D. A Collaborative Defense for Securing Protective Relay Settings in Electrical Cyber Physical Systems. In Proceedings of the Resilience Week (RWS), Denver, CO, USA, 20–23 August 2018; pp. 49–54.

69. Ahmed, A.; Krishnan, V.V.G.; Foroutan, S.A.; Touhiduzzaman, M.; Rublein, C.; Srivastava, A.; Wu, Y.; Hahn, A.; Suresh, S. Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems. *IEEE Trans. Ind. Appl.* **2019**, *55*, 6313–6323.

70. Feng, H.; Tavakoli, R.; Onar, O.C.; Pantic, Z. Advances in High-Power Wireless Charging Systems: Overview and Design Considerations. *IEEE Trans. Transp. Electrif.* **2020**, *6*, 886–919.

71. Sanghvi, A.; Markel, T. Cybersecurity for Electric Vehicle Fast-Charging Infrastructure. In Proceedings of the 2021 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 21–25 June 2021.

72. Гавриленко С., Зозуля В. Дослідження методів виявлення аномалій на етапі попередньої обробки даних , Системи управління, навігації та зв'язку. Збірник наукових праць: Том 1 № 67 (2022): Системи управління, навігації та зв'язку. DOI: https://doi.org/10.26906/SUNZ.2022.1.052

73. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance. CRC Press.

74. Lestari, R., Moorsel, A., & Radanliev, P. (2020). Blockchain for energy: A systematic literature review. Renewable and Sustainable Energy Reviews, 133, 110315.

75. Реалізація використання блокчейн-технологій у енергетичному секторі . [Електроннийресурс].URL:https://www.econ.vernadskyjournals.in.ua/journals/2019/30_69_4/30_69_4_2/28.pdf

76. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
77. Котенко, Д., Хлапонін, Ю. (2024). Штучний інтелект у системах виявлення і запобігання кібератакам: перспективи та виклики. Pidvodni Tehnologii, 1(14), 48–55. https://doi.org/10.32347/uwt.2024.14.1203
78. Allnutt, J.; Anand, D.; Arnold, D.; Goldstein, A.; Li-Baboud, Y.; Martin, A.; Nguyen, C.; Noseworthy, R.; Subramaniam, R.; Weiss, M. Timing challenges in the smart grid. *NIST Spec. Publ.* **2017**, *1500*, 08.
79. Шведчикова І., Трихліб А., Трихліб С., Демішонкова С. та Павленко В. (2024). Визначення ефективності відновлених фотоелектричних модулів в умовах природного освітлення. *Східно-Європейський журнал підприємницьких технологій* , *6* (8 (132), 16–24. https://doi.org/10.15587/1729-4061.2024.317829

ДОДАТОК А ПРЕЗЕНТАЦІЯ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА НАНОЕЛЕКТРОНІКИ

Дослідження та розроблення рекомендацій щодо застосування методів з кібербезпеки в кіберфізичних енергетичних системах

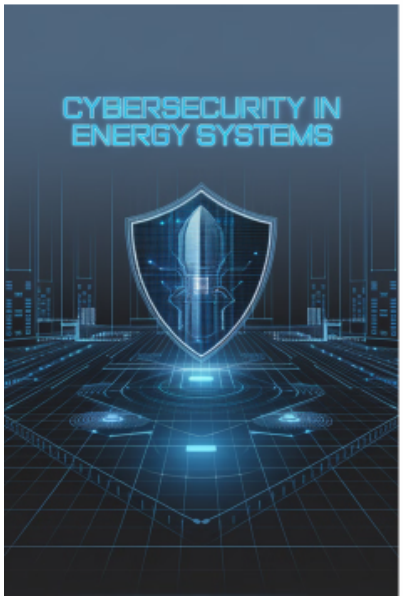
Виконав студент гр. БК-813м
спеціальності 125 - Кібербезпека та захист інформації освітня програма «Безпека інформаційних і комунікаційних систем»
Володимир ПАВЛЕНКО

Науковий керівник:
Леонід КАРПУКОВ

1

Дослідження та розроблення рекомендацій щодо застосування методів з кібербезпеки в кіберфізичних енергетичних системах

2



Сучасний енергетичний сектор активно трансформується під впливом цифровізації та впровадження кіберфізичних систем (КФС). Інтеграція цифрових технологій у традиційні енергетичні мережі забезпечує ефективне управління та моніторинг, проте створює нові проблеми у сфері кібербезпеки.

Дослідження спрямоване на пошук інноваційних рішень для забезпечення безпеки кіберфізичних енергетичних систем в умовах зростаючих викликів.

Метою дослідження є розроблення та обґрунтування рекомендацій задля впровадження в сучасні методи кібербезпеки за умови підвищення стійкості КФЕС.

Для досягнення цієї мети потрібно вирішити наступні задачі:

- Провести аналіз архітектури та компонентів КФС з визначенням основних вразливостей.
- Вивчити типологію кібератак на енергетичні системи та їхні наслідки.
- Розробити рекомендації щодо впровадження інтелектуальних алгоритмів для виявлення аномалій у реальному часі.
- Запропонувати стратегії пом'якшення наслідків атак та відновлення системи після інцидентів.

ОБ'ЄКТОМ ДОСЛІДЖЕННЯ є процес забезпечення кібербезпеки кіберфізичних енергетичних систем, а саме кіберфізичні енергетичні системи, що інтегрують інформаційні та енергетичні технології.

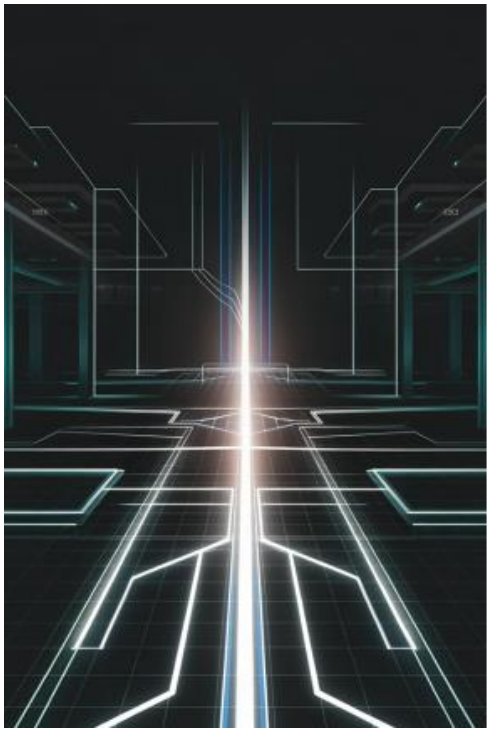
ПРЕДМЕТОМ ДОСЛІДЖЕННЯ є методи забезпечення кібербезпеки КФЕС, включаючи адаптивні алгоритми та інтегровані системи моніторингу.

НАУКОВА НОВИЗНА роботи полягає в розробленні та обґрунтуванні рекомендацій щодо пом'якшення наслідків кібератак на кіберфізичні енергетичні системи.

ПРАКТИЧНА ЦІННІСТЬ дослідження полягає в можливості впровадження розроблених механізмів захисту в реальні енергетичні системи, що забезпечить підвищення їхньої стійкості до кібератак.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ТА ПУБЛІКАЦІЇ. Результати дослідження були представлені на міжнародній науковій конференції

СТРУКТУРА РОБОТИ. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел.



Актуальність та мотивація дослідження

Цифрова трансформація

Енергетичний сектор активно впроваджує кіберфізичні системи, що створює нові виклики для кібербезпеки.

Зростання кібератак

Значна кількість кібератак на критичну інфраструктуру підкреслює необхідність комплексних рішень.

Інноваційні рішення

Потреба в розробці ефективних механізмів протидії новим типам загроз, таким як BlackEnergy чи Stuxnet.

Географія кібератак в енергетичному секторі

439

Пакистан

Найбільша кількість терористичних атак на енергетичний сектор.

170

Ємен

Друга країна за кількістю атак на енергетичну інфраструктуру.

161

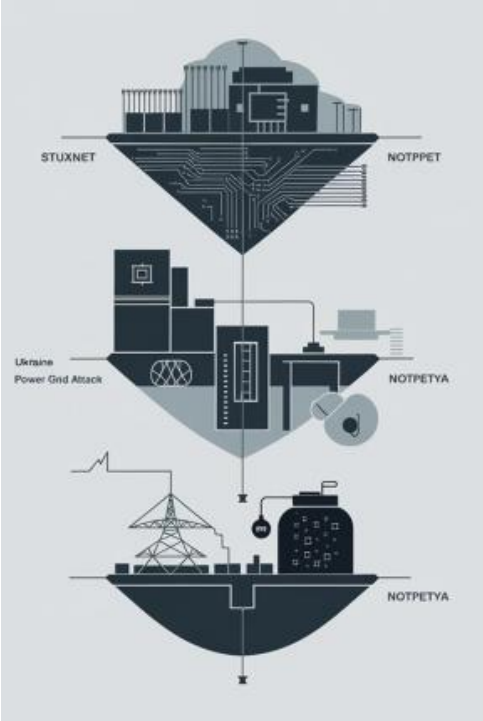
Колумбія

Третя за кількістю кібератак на енергетичний сектор.

146

Ірак

Четверта країна за кількістю терористичних атак на енергетичні об'єкти.



6

Аналіз кібератак на енергетичну інфраструктуру

1. **Stuxnet (2010)**

   Перший документований випадок використання шкідливого програмного забезпечення для фізичного руйнування інфраструктури. Атака на ядерні об'єкти Ірану.

2. **Атака на енергосистему України (2015)**

   Масове знеструмлення, що вплинуло на 225 000 користувачів. Вважається найгіршим відключенням енергосистеми, спричиненим кібератакою.

3. **NotPetya (2017)**

   Масована атака з використанням вірусу-шифрувальника, спрямована на критичну інфраструктуру України та інших країн.

7

Типологія кібератак на енергетичні системи

Маніпуляція кодом

Зміна програмного забезпечення для порушення роботи систем управління, як у випадку з трубопроводом у Сибіру (1982) та SCADA-системою в Беллінгемі (1999).

Шкідливе програмне забезпечення

Використання вірусів та троянів для проникнення в системи та викрадення даних. Приклади: Stuxnet, Night Dragon, Shamoon.

Атаки на відмову в обслуговуванні (DDoS)

Перевантаження систем запитами для порушення їх нормальної роботи. Часто використовуються для відключення енергосистем.

8

Рівні архітектури кіберфізичних систем

1 **Фізичний рівень**

Включає основні енергетичні об'єкти, такі як генератори, трансформатори та мережеві вузли. Тут знаходиться обладнання, яке інтерпретує фізичні явища та перетворює їх на електричні сигнали та інформацію.

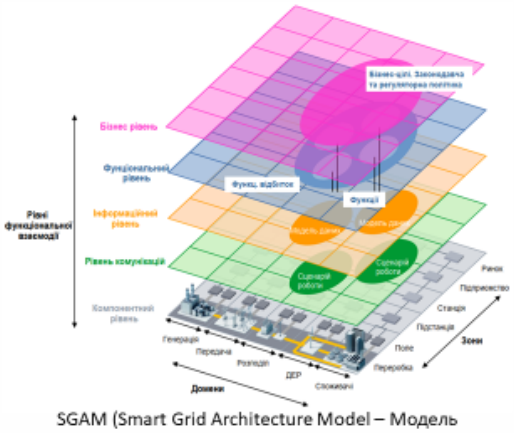
2 **Комунікаційний рівень**

Відповідає за передачу даних між рівнями, забезпечуючи безперебійний зв'язок через різні технології, включаючи дротові та бездротові мережі, Bluetooth, 4G і 5G, та інтернет-протоколи.

3 **Рівень управління**

Отримує інформацію від комунікаційного рівня, аналізує її та надсилає командні сигнали пристроям на фізичному рівні. Генерує інтелектуальні алгоритми прийняття рішень для належного функціонування фізичної системи.

Кіберфізичні енергетичні системи (КФС) - це складні інтегровані структури, що поєднують фізичні енергетичні компоненти з сучасними інформаційними технологіями. Основні складові КФС включають системи моніторингу, управління та передачі даних, що забезпечуються через SCADA-системи, інтелектуальні лічильники та мережеві протоколи.



SGAM (Smart Grid Architecture Model – Модель архітектури Smart Grid) Кіберфізичної енергосистеми

Ключові компоненти кіберфізичних систем

SVG

SCADA-системи

Забезпечують віддалений моніторинг та управління енергетичними об'єктами.

Інтелектуальні сенсори

Використовуються для збору даних про стан системи.

Програмовані логічні контролери (PLC)

Відповідають за локальні процеси управління.

Людино-машинний інтерфейс (HMI)

Забезпечує інтерактивну взаємодію оператора з системою.

Вразливості енергосистем

Інформаційні технології

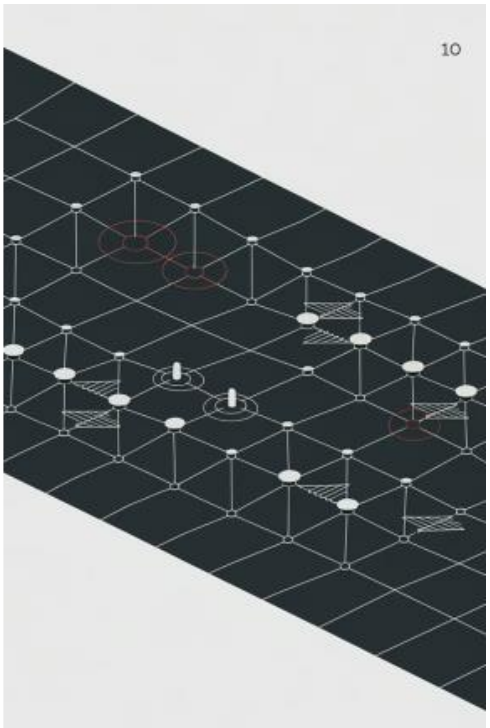
Широке використання електроніки та комп'ютерних технологій для планування, контролю та захисту.

Критичні компоненти

Атаки на реле аварійної сигналізації та пристрої безпеки можуть спричинити відключення електроенергії.

Ізольовані мережі

Можливість роботи мережі в ізольованому режимі створює додаткові виклики для безпеки.



11

Вразливості кіберфізичних систем

1. Синхронізація часу
   Проблеми з точністю часової синхронізації можуть призвести до збоїв у роботі системи
2. Автентифікація
   Недоліки в процесах автентифікації створюють ризики несанкціонованого доступу
3. Безпека мережевих протоколів
   Вразливості в протоколах можуть бути використані для проникнення в систему

12

Вразливості кіберфізичних енергетичних систем

Кібернетична вразливість
Пов'язана з мережею, комунікаціями, інтелектуальними пристроями та віддаленим доступом. Приклади атак: Stuxnet, Triton, Black Energy.

Фізична вразливість
Атаки на фізичні пристрої інфраструктури, включаючи датчики, виконавчі механізми, трансформатори та кабелі.

Кіберфізична вразливість
Вразливості на стику кібер- і фізичних компонентів. Приклади: ін'єкція логіки управління, атаки на відмову в обслуговуванні (DoS).

13

Основні стандарти кібербезпеки

NIST SP 800-53

Рамкові рекомендації для впровадження технічних, управлінських і операційних заходів безпеки.

IEC 62351

Зосереджений на захисті комунікацій у енергетичних системах, включаючи SCADA-системи.

ISO/IEC 27001

Глобальний еталон у сфері управління інформаційною безпекою.

14

ПРОТОКОЛИ БЕЗПЕКИ ТА СТРАТЕГІЇ КІБЕРСТІЙКОСТІ

Протоколи SCADA

Modbus, DNP3 та ICCP мають обмежені можливості захисту. Потребують додаткових заходів безпеки.

Стратегії кіберстійкості

ENISA та CISA пропонують рекомендації щодо забезпечення стійкості систем до атак і швидкого відновлення.

Протоколи безпеки SCADA-систем

Modbus

Не забезпечує шифрування чи автентифікацію. Вразливий до ін'єкції помилкових даних.

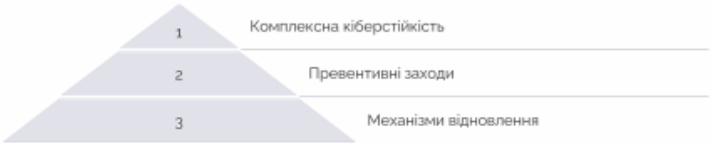
DNP3

Містить лише базові заходи цілісності даних. Не забезпечує повноцінного захисту.

ICCP

Застосовується для обміну даними між центрами управління. Вразливий до переповнення буфера.

Міжнародна стратегія кіберстійкості



15

Кібербезпека в системах моніторингу

Важливість безпеки інформації

Система моніторингу повинна забезпечувати інформаційну безпеку та надійність даних, зібраних датчиками та вимірювальними приладами.

Ключові методи

Монітор безпеки в режимі реального часу, регульована модель розрідженої глибокої мережі, алгоритми машинного навчання без учителя.

Сфери застосування

Кіберфізичні системи, критична інфраструктура, мережі управління гідроелектростанціями, системи управління в енергетичному секторі.

16

Кібербезпека управлінського рівня кіберфізичних систем

Ключові виклики

Забезпечення ефективного захисту від кібератак різної складності в централізованих та розподілених системах управління КФС.

Фокус уваги

Управління частотою та напругою в пристроях, пов'язаних з силовою електронікою, для забезпечення перехідної та стаціонарної стабільності системи.

Основні методи

Модельне прогнозне управління, адаптивне управління на основі інтелектуального аналізу, надійні контролери на основі різних підходів.

17

Інноваційні методи захисту від кібератак кіберфізичних енергетичних систем

1 **Виявлення атак**

Використання LSTM та TCN для точного виявлення ін'єкцій помилкових даних у реальному часі.

2 **Адаптивне управління**

Застосування методології ковзного управління на основі адаптивного динамічного програмування для децентралізованого захисту.

3 **Стійке управління**

Розробка контролерів, стійких до атак типу DoS, з використанням спостерігачів та Hoo-контролерів.

4 **Ігрові моделі**

Застосування моделей гри "напад-захист" для ідентифікації та запобігання атакам з використанням шкідливого ПЗ.

18

Сфери застосування методів кібербезпеки

Енергетичні системи

Захист критичної інфраструктури об'єднаної енергетичної системи від кібератак на процеси генерації, передачі та розподілу електроенергії.

Промислові КФС

Забезпечення безпеки промислових кіберфізичних систем, включаючи системи управління синхронними двигунами та інші промислові процеси.

Електромобілі

Захист електромобілів від кібератак, спрямованих на бездротові датчики та мережі, інтегровані в сучасні транспортні засоби.

19

Інтелектуальні методи захисту

Багатошаровий перцептрон

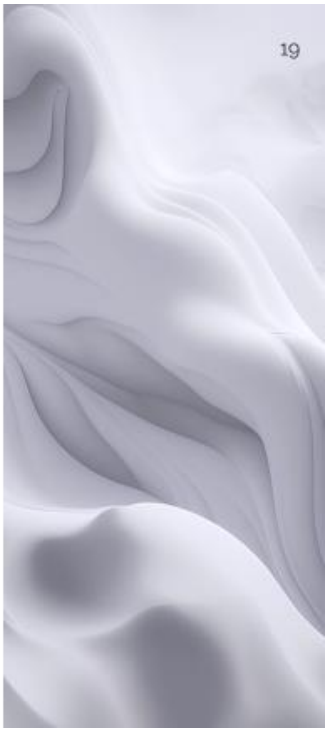
Модель на основі інтелектуального навчання для виявлення кібератак проти LCDR.

Isolation Forest

Методологія на основі виявлення аномалій для диференціації між реальними та фальшивими атаками.

Розподілене глибоке навчання

Використання агентів для виявлення ін'єкції фальшивих даних до моменту імітації хибної несправності.



20

Стратегії захисту енергосистем

Запобігання кібератакам

Захист фізичних компонентів системи

Виявлення атак

Ідентифікація загроз та зменшення наслідків

Адаптивне управління

Динамічні підходи з аналізом поточної інформації

Інноваційні технології

Блокчейн, квантові обчислення, ШІ

21

Критерії ефективності кібербезпеки

Швидкість виявлення атаки

Здатність системи оперативно ідентифікувати потенційні загрози

Точність визначення вразливостей

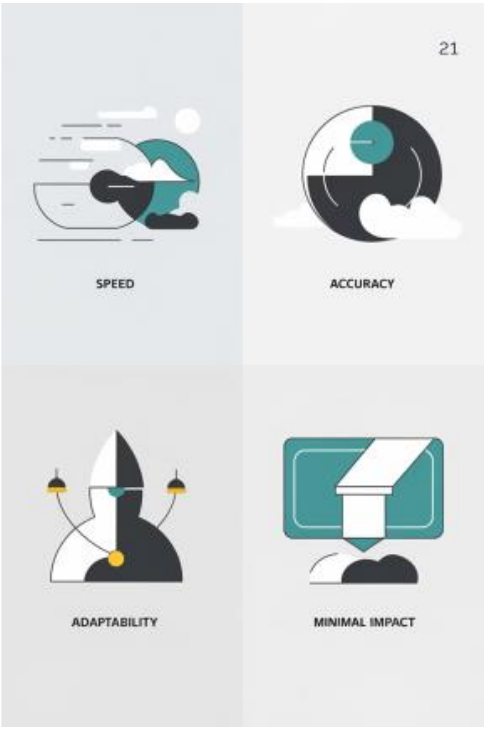
Ефективність у виявленні слабких місць системи

Адаптивність до нових загроз

Гнучкість у реагуванні на нові типи кібератак

Мінімізація впливу на критичні процеси

Забезпечення безперервності роботи енергетичних систем



22

Ключові показники ефективності (KPI)

1. **Рівень готовності**

   Визначає кількість оновлених пристроїв та здатність системи швидко виявляти та усувати вразливості

2. **Виявлення несанкціонованих пристроїв**

   Ідентифікація підключень до енергетичних мереж, які можуть створювати кіберризики

3. **Спроби проникнення**

   Кількість спроб отримати несанкціонований доступ до інформаційних систем енергетичного сектору

4. **Безпека інцидентів**

   Кількість випадків порушення роботи енергетичних систем внаслідок кібератак

23

Інноваційні методи захисту

Штучний інтелект

Використання ШІ для моніторингу та виявлення аномалій

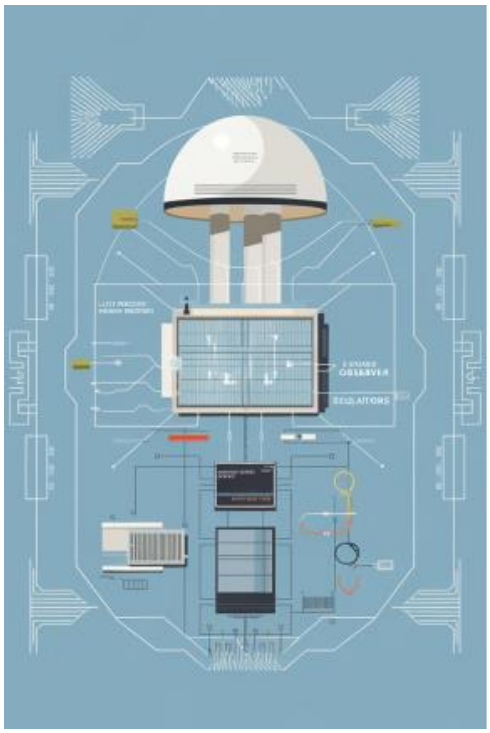
Блокчейн

Забезпечення безпечного обміну даними та підвищення прозорості

Адаптивні алгоритми

Динамічне налаштування систем захисту під нові загрози

Ці технології дозволяють створювати більш ефективні системи захисту кіберфізичних енергетичних систем.



24

Методи захисту LCDR

1. **Аналіз різниці напруг**

   Методологія на основі різниці між розрахованими та виміряними перекриваючими напругами для виявлення ін'єкцій фальшивих даних.

2. **Спостерігач стану**

   Використання спостерігача стану з невідомим вхідним сигналом для виявлення та відокремлення фальшивих даних від внутрішніх збоїв.

3. **Пасивні осциляторні контури**

   Метод, що включає пасивні осциляторні контури для вирішення проблеми синхронізації часу та фальшивих даних у мікромережах.

25

Блокчейн для захисту даних

Децентралізоване зберігання

Забезпечення цілісності та захисту даних від несанкціонованого доступу

Прозорість операцій

Відстеження походження відновлюваної енергії від джерела до споживача

Розумні контракти

Спрощення багаторівневої системи взаємодії між учасниками енергетичного ринку

26

Варіанти використання блокчейну в енергетиці

Транзакції та "розумні контракти"

Децентралізована торгівля електроенергією, криптовалюти в енергетиці

Права власності та управління активами

Реєстрація власності на енергетичні активи, "зелені" сертифікати

Децентралізовані інформаційні системи

Облік споживання електроенергії, автоматизація оплати зарядки електромобілів

27

Адаптивні алгоритми для аналізу даних

1 **Збір даних**
Отримання інформації з енергетичних систем

2 **Аналіз**
Застосування LSTM і Isolation Forest для ефективного виявлення аномалій

3 **Реагування**
Швидке реагування на виявлені загрози

Порівняльний аналіз адаптивних алгоритмів для аналізу даних

Алгоритм	Точність	Швидкість	Адаптивність
LSTM	Висока	Середня	Висока
Isolation Forest	Висока	Висока	Середня
Традиційні методи	Середня	Низька	Низька

28

Ефективність адаптивних алгоритмів

LSTM нейронні мережі
Показали високу точність у виявленні аномалій у часових рядах енергетичних систем

Isolation Forest
Ефективний метод для ідентифікації нетипових паттернів у даних енергосистем

Адаптивні алгоритми для реагування на загрози

1 **Аналіз мережевого трафіку**
Виявлення прихованих аномалій або шаблонів, що свідчать про загрози

2 **Нейронні мережі з автокодерами**
Виявлення аномалій шляхом аналізу відхилень між вихідними даними та їх реконструкцією

3 **Алгоритми ізоляційного лісу**
Ідентифікація рідкісних аномальних подій завдяки ефективній кластеризації даних

29

Рекомендації щодо впровадження

1 **Попередня обробка даних**
Забезпечення високої якості вхідних даних для аналізу

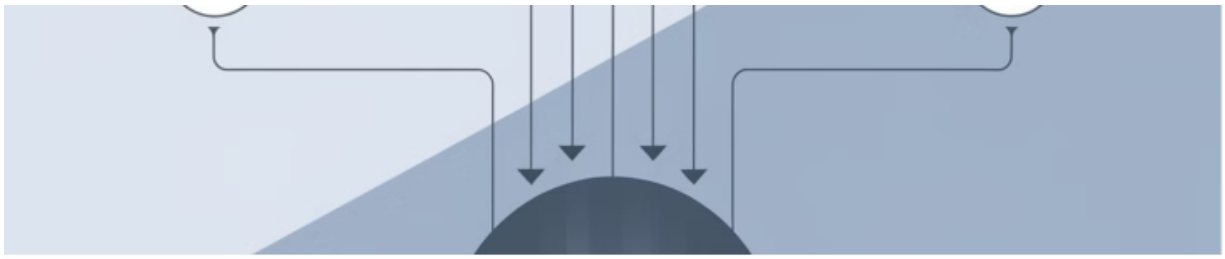
2 **Вибір моделей**
Підвищення точності виявлення загроз

3 **Навчання алгоритмів**
Оптимізація роботи моделей

4 **Інтеграція в системи**
Зменшення часу реакції на загрози

Регулярна оцінка ефективності за допомогою KPI, таких як середній час виявлення загрози (MTTD) або середній час реагування (MTTR), є ключовою для підтримки високого рівня кібербезпеки.

30



Висновки та рекомендації

Комплексний підхід
Необхідність інтеграції різних технологій для забезпечення кібербезпеки

Постійна адаптація
Важливість регулярного оновлення систем захисту

Міжнародна співпраця
Розвиток глобальних стандартів та обмін досвідом

Перспективи подальших досліджень

31

Моделювання кібератак

Створення багаторівневих платформ для симуляції атак

Квантово-стійкі алгоритми шифрування

Розробка алгоритмів шифрування, стійких до квантових обчислень

Адаптація стандартів

Оновлення існуючих стандартів відповідно до нових загроз

Інтеграція IoT та квантових обчислень

Дослідження впливу новітніх технологій на безпеку енергосистем

Розробка нових стандартів

1. Аналіз поточних стандартів
   Виявлення недоліків існуючих норм
2. Розробка пропозицій
   Створення нових стандартів з урахуванням сучасних загроз
3. Впровадження та адаптація
   Інтеграція нових стандартів у галузі

32

Майбутні виклики кібербезпеки

Модернізація енергосистеми

Інтеграція відновлюваних джерел енергії та "розумних" мереж створює нові вразливості. Залежність від Інтернету для роботи і зв'язку збільшує кібернетичну вразливість системи.

Електрифікація транспорту

Розвиток електричного транспорту створює нові ризики. Зарядні станції стають вразливими точками і представляють дослідницький інтерес для забезпечення кібербезпеки.