Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Українська інженерно-педагогічна академія»
Кафедра електротехніки та електроенергетики

КВАЛІФІКАЦІЙНА РОБОТА

магістра

на тему

ДОСЛІДЖЕННЯ ВПЛИВУ ЦИФРОВІЗАЦІЇ ЕНЕРГОСИСТЕМ НА ПІДВИЩЕННЯ РІВНЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ЕЛЕКТРОСТАНЦІЇ ПІД ЧАС КІБЕРЗАГРОЗ В УМОВАХ ВОЄННОГО СТАНУ

(тема кваліфікаційної роботи)

Виконав: студент 2 маг. курсу, групи ДЕА-Е23мг-1
спеціальності : 141 Електроенергетика, електротехніка та електромеханіка
_____/___Ілля ЛЕВЧЕНКО
(підпис) (ім'я та прізвище)
Керівник _____/__Павло БУДАНОВ
(підпис) (ім'я та прізвище)
Рецензент _____/_____
(підпис) (ім'я та прізвище)

«До захисту допущено»

Завідувач кафедри _____/_Артем ЧЕРНЮК
(підпис) (ім'я та прізвище)
Нормоконтроль_____/_Юлія ОЛІЙНИК
(підпис) (ім'я та прізвище)
Секретар ЕК _____/_____
(підпис) (ім'я та прізвище)

Харків – 2024 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

Навчально – науковий інститут Українська інженерно-педагогічна академія
Кафедра електротехніки та електроенергетики
Спеціальність 141 Електроенергетика, електротехніка та електромеханіка
Освітньо-професійна програма Енергетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
(підпис)

к.т.н., доцент Артем ЧЕРНЮК
(науковий ступінь, вчене звання, ім'я, прізвище)

«___» _____2024 р.

ЗАВДАННЯ
на кваліфікаційну роботу дипломну роботу
другого (магістерського) рівня вищої освіти

здобувачу вищої освіти Ілля ЛЕВЧЕНКО
1. Тема «Дослідження впливу цифровізації енергосистем на підвищення рівня енергетичної безпеки електростанції під час кіберзагроз в умовах воєнного стану»
затверджена наказом по академії №____від «___»_____ 20___р.

2. Термін здачі закінченої роботи «____»_____20___р.

3. Вихідні дані до роботи/проєкту: Параметри енергетичної безпеки електростанції. Методи розрахунку стану кіберзагроз.

4. Зміст роботи/проєкту (перелік питань, які належить розробити):
ВСТУП; РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЦИФРОВІЗАЦІЇ ЕНЕРГОСИСТЕМ; РОЗДІЛ 2. ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ ДЛЯ ЕНЕРГЕТИЧНИХ ОБЄКТІВ В УМОВАХ ВОЄННОГО СТАНУ; РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ЕЛЕКТРОСТАНЦІЙ ЧЕРЕЗ ЦИФРОВІ ТЕХНОЛОГІЇ.

5.Перелік графічного матеріалу (презентаційний матеріал):
Слайди презентації

6. Консультант:

Розділ	Консультант	Підпис, дата		Оцінка (бали)
		Завдання видав	Завдання прийняв	

7. Дата видачі завдання«___»_____20___р.

Керівник _____ Павло БУДАНОВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____Ілля ЛЕВЧЕНКО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН-ГРАФІК
виконання кваліфікаційної дипломної роботи

№ з/п	Назва етапів роботи та питань, які мають бути розроблені відповідно до завдання	Термін виконання	Позначки керівника про виконання завдань
1	Визначення актуальності теми дослідження	02.10.24 – 05.10.24	
2	Проведення аналізу наукової літератури	06.10.24 – 15.10.24	
3	Виконання першого розділу дипломної роботи	16.10.24 – 29.10.24	
4	Виконання другого та третього розділу дипломної роботи	30.10.24 – 26.11.24	
5	Оформлення пояснювальної записки	27.11.24 – 07.12.24	

Студент (ка) _____ Ілля ЛЕВЧЕНКО
(підпис) (ім'я, прізвище)

Нормоконтроль _____ Юлія ОЛІЙНИК
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Сторінок тексту – ____ ; рисунків – ___ ; таблиць – ___ ;

літературних джерел – ___ .

Тема магістерської роботи: «Дослідження впливу цифровізації енергосистем на підвищення рівня енергетичної безпеки електростанції під час кіберзагроз в умовах воєнного стану».

Метою роботи є дослідження впливу цифровізації енергосистем на підвищення рівня енергетичної безпеки електростанцій у контексті кіберзагроз, зокрема в умовах воєнного стану.

Об'єктом дослідження є процес впливу цифрових технологій на підвищення стійкості та енергобезпеки електростанцій до кіберзагроз у умовах воєнного стану.

Предметом дослідження є енергетичні системи, зокрема електростанції, в контексті їх цифровізації та підвищення рівня енергетичної безпеки, а також впливу кіберзагроз на їх функціонування під час воєнного стану. Дослідження охоплює як технічні аспекти цифрових технологій, так і питання кібербезпеки в енергетичному секторі.

Для досягнення поставленої мети в рамках цієї роботи визначено низку **завдань**:

- вивчити теоретичні основи цифровізації енергетичних систем, її складові та вплив на ефективність функціонування енергетичних об'єктів;

- описати поняття енергетичної безпеки та ключові принципи, що забезпечують надійність та стійкість електростанцій до зовнішніх і внутрішніх загроз;

- проаналізувати основні види кіберзагроз, їх вплив на енергетичні об'єкти, зокрема в умовах воєнного стану;

Ключові слова: цифровізація, енергетична безпека електростанції, кіберзагроза, умови воєнного стану.

ABSTRACT

Pages of text – ____ ; pictures – ___ ; tables – ___ ;

literary sources – ___ .

The topic of the Master's thesis: "Research on the Impact of Energy System Digitalization on Enhancing the Energy Security of Power Plants During Cyber Threats in Wartime Conditions."

The aim of the work is to study the impact of energy system digitalization on enhancing the energy security of power plants in the context of cyber threats, particularly under wartime conditions.

The object of the study is the process of how digital technologies influence the resilience and energy security of power plants against cyber threats during wartime.

The subject of the study is energy systems, specifically power plants, in the context of their digitalization and enhancement of energy security, as well as the impact of cyber threats on their operation during wartime. The study covers both the technical aspects of digital technologies and issues related to cybersecurity in the energy sector.

To achieve the goal of the work, the following tasks are defined:

Study the theoretical foundations of energy system digitalization, its components, and its impact on the efficiency of energy facility operation;

Describe the concept of energy security and the key principles ensuring the reliability and resilience of power plants to external and internal threats;

Analyze the main types of cyber threats, their impact on energy facilities, particularly in wartime conditions.

Keywords: digitalization, energy security of power plants, cyber threat, wartime conditions.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність теми дослідження зумовлена, як швидким розвитком технологій, так і постійно зростаючими ризиками, які супроводжують цифровізацію енергетичних мереж. Успішне впровадження цифрових інструментів у сфері енергетичної безпеки є необхідною умовою для забезпечення надійності енергетичних систем, що в умовах сучасних глобальних та регіональних викликів є надзвичайно важливим для економічної стабільності і національної безпеки кожної країни [1-5].

Сучасний розвиток енергетичних систем та їх інтеграція з цифровими технологіями є одним із найбільш важливих напрямів для забезпечення стабільності, ефективності та безпеки енергетичних інфраструктур. Одним із найбільших викликів, з якими стикається енергетичний сектор, є забезпечення високого рівня енергетичної безпеки, особливо в умовах зовнішніх і внутрішніх загроз [6-13].

В останні десятиліття цифровізація енергетичних систем, зокрема через впровадження таких технологій, як Інтернет речей (IoT), штучний інтелект (AI), машинне навчання та блокчейн, відкриває нові можливості для оптимізації управління енергетичними потоками, інтеграції відновлювальних джерел енергії та забезпечення більш ефективного захисту від кіберзагроз [14-17].

Водночас, разом із зростанням залежності енергетичних об'єктів від цифрових технологій, виникають нові ризики, зокрема вразливості перед кіберзагрозами, які можуть спричинити значні перебої в енергопостачанні або навіть серйозні аварії на енергетичних об'єктах. У період воєнного стану ці загрози набувають особливої актуальності, оскільки енергетична інфраструктура стає важливою мішенню для кібератак, що можуть мати катастрофічні наслідки для національної безпеки [18-21].

Метою роботи є дослідження впливу цифровізації енергосистем на підвищення рівня енергетичної безпеки електростанцій у контексті

кіберзагроз, зокрема в умовах воєнного стану. У роботі будуть розглянуті основні аспекти інтеграції цифрових технологій у енергетичні системи, а також їх потенціал для підвищення стійкості до кіберзагроз і зменшення ризиків для критичної інфраструктури. Аналіз буде базуватися на вивченні міжнародного досвіду та сучасних методів кіберзахисту, а також на моделюванні впливу цифрових технологій на безпеку енергетичних об'єктів у реальних умовах.

Об'єктом дослідження є процес впливу цифрових технологій на підвищення стійкості та енергобезпеки електростанцій до кіберзагроз у умовах воєнного стану.

Предметом дослідження є енергетичні системи, зокрема електростанції, в контексті їх цифровізації та підвищення рівня енергетичної безпеки, а також впливу кіберзагроз на їх функціонування під час воєнного стану. Дослідження охоплює як технічні аспекти цифрових технологій, так і питання кібербезпеки в енергетичному секторі.

Для досягнення поставленої мети в рамках цієї роботи визначено низку *завдань*:

- вивчити теоретичні основи цифровізації енергетичних систем, її складові та вплив на ефективність функціонування енергетичних об'єктів;

- описати поняття енергетичної безпеки та ключові принципи, що забезпечують надійність та стійкість електростанцій до зовнішніх і внутрішніх загроз;

- проаналізувати основні види кіберзагроз, їх вплив на енергетичні об'єкти, зокрема в умовах воєнного стану;

- оцінити міжнародний досвід забезпечення енергетичної безпеки в умовах цифровізації та визначити найкращі практики для застосування в Україні.

- розробити рекомендації щодо використання цифрових технологій для підвищення рівня енергетичної безпеки електростанцій, враховуючи кіберзагрози в умовах воєнного стану;

- моделювати потенційні сценарії впливу кіберзагроз на енергетичні об'єкти та оцінити стійкість енергетичних систем до таких загроз;

- розробити практичні рекомендації для енергетичних підприємств щодо впровадження систем моніторингу та захисту від кіберзагроз.

Теоретична значимість роботи полягає в розробці нових підходів до аналізу та впровадження цифрових технологій в енергетичні системи для підвищення їх безпеки, зокрема в контексті кіберзагроз. Розглянуті теоретичні засади цифровізації енергетичних об'єктів дозволяють глибше зрозуміти роль сучасних інформаційних технологій у забезпеченні стабільності енергетичних систем і зменшенні ризиків для критичної інфраструктури. Визначення основних принципів і механізмів захисту енергетичних об'єктів допомагає створити цілісну концепцію забезпечення енергетичної безпеки в умовах швидко змінюваного технологічного середовища.

Практична значимість цієї роботи полягає в розробці рекомендацій для енергетичних компаній щодо ефективного використання цифрових технологій для підвищення рівня енергетичної безпеки. Результати дослідження можуть бути використані для вдосконалення існуючих стратегій захисту енергетичних об'єктів від кіберзагроз, впровадження систем моніторингу та автоматизації управління енергетичними процесами. Крім того, на основі дослідження можна створити моделі для оцінки стійкості енергетичних об'єктів до потенційних кіберзагроз, що дозволяє здійснити більш ефективне планування заходів із забезпечення безпеки в умовах війни чи інших кризових ситуацій. Отже, результати роботи сприятимуть підвищенню надійності енергетичних систем і зменшенню ризиків, пов'язаних з кіберзагрозами в умовах цифровізації.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЦИФРОВІЗАЦІЇ ЕНЕРГОСИСТЕМ

1.1 Поняття та основні складові цифровізації енергосистем

Цифровізація енергосистем є ключовим етапом у розвитку сучасних енергетичних інфраструктур, спрямованим на покращення їх ефективності, гнучкості та безпеки. Вона передбачає інтеграцію новітніх цифрових технологій у всі етапи життєвого циклу енергетичних об'єктів — від виробництва до споживання енергії.

Основні складові цифровізації енергосистем:

Інтелектуальні енергомережі (Smart Grids): Це інтегровані енергетичні мережі, які дозволяють зібрати, обробити та аналізувати дані у реальному часі для ефективного управління потоками енергії. Наприклад, в Європі та США успішно впроваджуються програми “Smart Grid”, де за допомогою цифрових технологій автоматично керуються джерела відновлювальної енергії, знижуються енергетичні втрати і покращується стабільність постачання енергії.

Великі дані та аналітика (Big Data): Зібрані з різних джерел дані (від датчиків на обладнанні до прогнозів погоди) дозволяють оптимізувати управління енергетичними потоками, прогнозувати навантаження на мережу, а також виявляти вразливості. Наприклад, компанія Google використовує аналітику великих даних для оптимізації енергоспоживання в своїх дата-центрах, досягаючи значних енергозбережень.

Штучний інтелект (AI) та машинне навчання: Використання AI для передбачення попиту на енергію та планування виробництва дає змогу значно знизити витрати і покращити управління мережею. Наприклад, DeepMind (підрозділ Alphabet, материнської компанії Google) розробив систему, яка допомагає зменшити споживання енергії для охолодження серверів на 40%, застосовуючи алгоритми машинного навчання.

Інтернет речей (IoT): IoT дозволяє підключати різноманітні пристрої, що збирають інформацію про стан енергетичних систем (наприклад, розподільні щити, турбіни та сонячні панелі) і передають її до централізованої платформи для обробки. Це дає змогу в реальному часі контролювати технічний стан і оперативно реагувати на відхилення. Наприклад, у Великобританії компанія UK Power Networks застосовує датчики IoT для моніторингу стану енергетичних ліній і виявлення поломок до того, як вони викличуть серйозні аварії.

1.2 Енергетична безпека електростанцій: сутність, принципи та компоненти

Енергетична безпека електростанцій визначається як здатність енергетичних об'єктів ефективно, безперебійно і стабільно функціонувати, навіть у випадку виникнення різних загроз: техногенних аварій, природних катастроф чи кіберзагроз.

Розглянемо принципи енергетичної безпеки електростанцій:

Надійність та стабільність: Це здатність станцій забезпечувати постачання енергії без відключень навіть у надзвичайних ситуаціях. Відповідно до цього принципу, енергетичні компанії повинні інтегрувати системи резервного живлення, що можуть забезпечити безперервне функціонування при відключенні основних джерел енергії.

Резистентність: Це здатність енергетичної системи витримувати різноманітні зовнішні і внутрішні впливи, зберігаючи працездатність навіть при часткових збоях. Наприклад, відключення електростанцій у разі кібернападу повинно бути мінімізоване за допомогою протоколів відновлення даних.

Гнучкість: Можливість швидкої адаптації до змін зовнішніх умов, зокрема до нових технологічних вимог чи змін у політичній та економічній

ситуації. Прикладом гнучкої енергосистеми є інтеграція відновлювальних джерел енергії в єдину мережу.

Безпека персоналу та захист критичної інфраструктури: Протидія загрозам не тільки з боку кіберзлочинців, але й фізичним нападам, наприклад, терористичним актам. Зазвичай енергетичні об'єкти оснащуються високим рівнем фізичної охорони і системами відеоспостереження.

Розглянемо компоненти енергетичної безпеки:

Кібербезпека: Особливе значення надається захисту від кіберзагроз, адже зростання цифровізації енергетичних мереж збільшує вразливість до атак. Для цього вживаються заходи щодо захисту SCADA-систем, що керують енергетичними об'єктами.

Фізична безпека: Стосується захисту енергетичних об'єктів від фізичних атак, таких як терористичні акти чи саботаж. Наприклад, після атак на енергетичні об'єкти в Україні (2015, 2016), уряд прийняв серйозні заходи щодо посилення фізичної безпеки енергетичної інфраструктури.

1.3 Види кіберзагроз та їх вплив на енергетичні об'єкти

Кіберзагрози є одними з основних викликів для енергетичних систем у процесі їх цифровізації. З кожним роком зростає кількість кіберінцидентів, спрямованих на енергетичну інфраструктуру.

Основні види кіберзагроз:

Атаки на систему SCADA: SCADA (Supervisory Control and Data Acquisition) — це система управління, що контролює роботу енергетичних мереж. Наприклад, в 2015 році в Україні була здійснена кибер-атака на електричні мережі, яка через вразливість SCADA призвела до відключення електроенергії в деяких регіонах.

Вірусні атаки: Використання вірусів для пошкодження програмного забезпечення, яке керує енергетичними мережами. Один з відомих прикладів

— вірус Stuxnet, який у 2010 році атакував іранські ядерні об'єкти, порушивши роботу центрифуг.

Атаки через Інтернет речей (IoT): Наприклад, пристрої, підключені до Інтернету, можуть стати вразливими до хакерських атак. В 2017 році кіберзлочинці використали IoT-пристрої для здійснення DDoS-атаки на системи керування електростанціями.

Денійсервіс-атаки (DDoS): Метою таких атак є перевантаження серверів енергетичних компаній, що призводить до відключень та блокування доступу до систем.

Вплив кіберзагроз на енергетичні об'єкти:

Збої у роботі електричних мереж: Кіберзагрози можуть призвести до серйозних збоїв у роботі енергетичних об'єктів. Наприклад, атаки на системи SCADA можуть призвести до тимчасового або тривалого відключення постачання електроенергії.

Фінансові втрати: Атаки можуть призвести до величезних витрат на відновлення пошкоджених систем та ліквідацію наслідків. За оцінками, витрати на відновлення після масштабних кібер-атак можуть сягати десятків мільйонів доларів.

1.4 Міжнародний досвід забезпечення енергетичної безпеки в умовах цифровізації

Розглянемо роль цифрових технологій у підвищенні рівня енергетичної безпеки. Цифрові технології є важливим елементом у забезпеченні енергетичної безпеки, оскільки вони дозволяють не лише підвищити ефективність управління енергетичними системами, але й значно знизити ризики, пов'язані з аваріями та кіберзагрозами. Розглянемо конкретні приклади застосування цифрових технологій у цьому контексті:

Застосування великих даних і аналітики: Однією з ключових переваг великих даних є можливість їх аналізу для прогнозування майбутніх подій і оптимізації роботи енергосистем. Наприклад, компанія Siemens впровадила систему збору та аналізу даних на кількох великих енергетичних підприємствах. Застосування алгоритмів машинного навчання та великих даних дозволило їм точно прогнозувати навантаження на мережу та визначати оптимальний графік роботи генераторів. Це не тільки зменшує витрати, а й підвищує надійність мережі, знижуючи ймовірність аварійних ситуацій.

У Фінляндії компанія Fortum використовує дані з інтелектуальних лічильників для моніторингу енергоспоживання та оптимізації процесів виробництва та розподілу енергії. Система на основі великих даних дозволяє своєчасно виявляти аномалії та попереджати про потенційні проблеми, що дає змогу швидко реагувати та уникати аварій.

Інтелектуальні енергетичні мережі (Smart Grids): Впровадження інтелектуальних енергомереж дозволяє не лише знижувати енергетичні втрати, але й поліпшувати моніторинг та управління енергетичними потоками. Це особливо важливо в умовах змінної генерації відновлювальних джерел енергії, таких як сонце та вітер, які можуть бути непередбачуваними.

Наприклад, у Німеччині компанія E.ON реалізує проект Smart Grid на основі концепції "міст майбутнього", в якому енергетичні мережі інтегрують різні джерела енергії і дозволяють здійснювати автоматичний контроль за рівнем споживання. Система дозволяє інтегрувати нові технології, такі як домашні батареї для зберігання енергії, і регулювати навантаження на мережу в режимі реального часу, що підвищує її стійкість до можливих кризових ситуацій. Інший приклад — в Іспанії проект "Smart Grid 2020", який передбачає інтеграцію систем моніторингу та управління з усіма рівнями енергетичної мережі. Ця система дозволяє реальним часом контролювати стан електричних мереж, виявляти аварії на початкових етапах і оперативно їх усувати.

Блокчейн у енергетичній безпеці: Блокчейн є потужним інструментом для підвищення прозорості та безпеки у енергетичних операціях. Відкриті та незмінні записи в блокчейні забезпечують точність і достовірність інформації, що особливо важливо в умовах цифровізації та зростання ризиків кіберзагроз.

Одна з основних переваг блокчейн-технології в енергетичній безпеці — це захист від фальсифікації даних, що робить її ідеальним інструментом для моніторингу та запису операцій на енергетичних ринках.

Наприклад, у рамках проекту Energy Web Foundation, який реалізується в декількох країнах, впроваджено блокчейн для управління дистрибуцією енергії. Цей проект дозволяє створювати "розумні контракти" для автоматизованих угод між споживачами та постачальниками енергії, що підвищує ефективність та безпеку операцій.

У Ізраїлі компанія EnergiMine застосовує блокчейн для створення платформи енергетичної безпеки, де всі учасники мають доступ до незмінних та прозорих даних про виробництво та споживання енергії, що дозволяє забезпечити кращий контроль та знижує можливість маніпуляцій.

Автоматизація та захист SCADA-систем: Система управління SCADA є основною ланкою для контролю і керування енергетичними об'єктами в реальному часі. Захист SCADA-систем від кіберзагроз є критично важливим для забезпечення безпеки енергетичних інфраструктур. У деяких країнах, таких як США та Японія, для захисту SCADA-систем від атак розроблені спеціалізовані програмні рішення, які забезпечують постійний моніторинг і виявлення аномалій.

Наприклад, компанія Honeywell розробила інноваційне рішення для захисту SCADA-систем в енергетичних підприємствах. Система включає в себе механізми виявлення та нейтралізації кіберзагроз у реальному часі, а також автоматичне відновлення операцій після інцидентів.

1.5 Вплив війни та кризових ситуацій на енергетичну безпеку в умовах цифровізації

У контексті війни, зокрема, в умовах воєнного стану, цифровізація енергетичних систем набуває особливої значущості. Кіберзагрози та фізичні атаки можуть завдати серйозної шкоди енергетичним мережам, і саме тому потрібно розробляти стратегії для їх захисту та відновлення в умовах надзвичайних ситуацій.

Розглянемо адаптацію енергетичних мереж до умов воєнного часу. Одним з важливих аспектів цифровізації в умовах воєнного часу є адаптація енергетичних мереж до умов постійних кіберзагроз і фізичних атак. Створення дистанційних систем управління, які можуть працювати автономно навіть при пошкодженні центральних командних пунктів, є одним з основних напрямків захисту енергетичних об'єктів. Приклад: Після атаки на енергетичну інфраструктуру України у 2015 році, в результаті якої відбулося відключення частини електричних мереж, уряд країни почав розробляти заходи для модернізації енергосистем, зокрема для підвищення їх стійкості до кібернападів. У 2020 році було впроваджено нові стандарти кібербезпеки для енергетичних об'єктів, що включають застосування цифрових технологій для моніторингу стану енергомереж в реальному часі.

Розглянемо використання інтелектуальних технологій для відновлення після атак. Інтелектуальні технології не тільки забезпечують безпеку, але й дозволяють швидко відновити енергетичні системи після атак або інших критичних подій. Адаптивні системи управління дають можливість перерозподіляти навантаження на мережі, автоматично налаштовувати параметри генерації та доставки енергії в разі потреби.

Приклад: В Ізраїлі компанії, що управляють енергетичними мережами, використовують технології автоматизованого управління для створення “резервних маршрутів” доставки енергії, що дозволяють підтримувати енергопостачання навіть у разі руйнування частини інфраструктури.

Розглянемо перспективи цифровізації енергетичних систем в умовах глобальних викликів. Цифровізація енергетичних мереж дозволяє не тільки ефективно забезпечувати енергетичну безпеку, але й сприяє розвитку глобальних ініціатив з енергетичної стійкості. Системи автоматизації та аналітики даних можуть значно знизити вразливість енергетичних об'єктів до кіберзагроз, а також покращити стійкість систем у разі воєнних чи природних катастроф.

Розвиток інтелектуальних мереж та інтеграція технологій блокчейн і AI в енергетичні процеси надасть можливість не лише зберегти, а й постійно вдосконалювати рівень енергетичної безпеки в умовах глобальних криз.

Загалом, роль цифрових технологій у забезпеченні енергетичної безпеки є неоціненною, і лише комплексний підхід до інтеграції цих технологій у практику управління енергетичними системами дозволить знизити ризики та підвищити стійкість інфраструктури у сучасних умовах.

Розглянемо стратегію управління ризиками для енергетичних систем у кризових умовах. В умовах війни або природних катастроф, коли енергетична інфраструктура може бути піддана численним загрозам, важливо розробити стратегії управління ризиками, що передбачають як захист від фізичних, так і від кіберзагроз. Впровадження цифрових технологій дозволяє створити більш адаптивні та швидкісні реакції на кризові ситуації.

Ключові аспекти стратегій управління ризиками:

Моніторинг у реальному часі: Цифрові технології, такі як інтелектуальні сенсори та системи збору даних, дозволяють постійно моніторити стан енергетичних об'єктів і попереджати про потенційні ризики. Наприклад, в Україні впроваджена система моніторингу енергомереж в реальному часі, що дозволяє оперативно виявляти аварії і переконфігурувати мережу для відновлення енергопостачання.

Адаптивне планування: Завдяки цифровим моделям можна створювати сценарії для різних типів кризових ситуацій, таких як атаки на енергетичні мережі або стихійні лиха. Це дозволяє оперативно адаптувати плани

управління та швидко приймати рішення, що важливо для забезпечення безперервного енергопостачання в умовах воєнного стану.

Відновлення після атак: Цифрові технології також дозволяють здійснити швидке відновлення інфраструктури після атак або катастроф. Використання автоматизованих систем для управління енергетичними мережами дозволяє переконфігурувати енергопостачання та забезпечити стабільну роботу навіть після серйозних пошкоджень. Наприклад, у разі пошкодження певних елементів енергомережі, система може перенаправити потоки енергії через інші маршрути без людського втручання.

Розглянемо роль національних та міжнародних організацій у захисті енергетичних мереж. У відповідь на зростаючу кількість кіберзагроз та воєнних атак на енергетичні об'єкти, національні та міжнародні організації активно працюють над розробкою стандартів та ініціатив, спрямованих на захист енергетичних інфраструктур.

Національний рівень: Національні органи влади відіграють важливу роль у забезпеченні енергетичної безпеки. У багатьох країнах розроблені спеціальні програми для модернізації енергетичних мереж, впровадження кібербезпеки та розробки планів для аварійного відновлення. Наприклад, у США Федеральна енергетична регулююча комісія (FERC) та Міністерство енергетики активно працюють над створенням нормативних актів, які визначають вимоги до кіберзахисту енергетичних компаній.

Міжнародні ініціативи: Організації, такі як Міжнародне енергетичне агентство (IEA) та Європейський Союз, розробляють міжнародні стандарти та пропозиції для забезпечення безпеки енергетичних мереж. Наприклад, Європейська директива щодо кібербезпеки критичної інфраструктури вимагає від держав-членів забезпечення високого рівня захисту енергетичних об'єктів від кіберзагроз.

Розглянемо підвищення стійкості до фізичних і кіберзагроз за допомогою нових технологій. Сучасні технології дають змогу значно підвищити стійкість енергетичних систем до фізичних і кіберзагроз:

Моделі "Інтернету речей" (IoT): Завдяки інтерконектованим пристроям в енергетичних мережах, енергетичні компанії можуть в реальному часі отримувати інформацію про стан інфраструктури. Це дозволяє швидко реагувати на несанкціоновані вторгнення або відмови в роботі окремих частин мережі. Крім того, такі пристрої можуть надавати дані про фізичні загрози, зокрема зміни температури чи вібрацій, що дозволяє оперативно виявляти технічні несправності та аварії.

Штучний інтелект (AI) для прогнозування атак: Алгоритми штучного інтелекту можуть аналізувати величезні обсяги даних про кіберзагрози і створювати прогнози щодо можливих атак на енергетичні об'єкти. Використання машинного навчання для ідентифікації та прогнозування атак дозволяє знижувати ризики від кіберзагроз ще до їх прояву. Наприклад, система AI може ідентифікувати аномальні патерни в трафіку даних і зафіксувати потенційні загрози, такі як DDoS-атаки, ще до їх початку.

Застосування технологій блокчейн для кібербезпеки: Блокчейн може бути використаний для захисту від маніпуляцій з даними, що надходять від енергетичних пристроїв або мереж. Ця технологія дозволяє створювати незмінні записи про операції з енергією, що виключає можливість підробки інформації про стан енергетичних систем.

Розглянемо перспективи цифровізації енергетичних систем у майбутньому. Цифровізація енергетичних мереж відкриває нові можливості для підвищення ефективності та безпеки енергопостачання. Проте для забезпечення максимальної стійкості та надійності енергетичних систем, необхідно враховувати ряд майбутніх викликів:

Інтеграція відновлюваних джерел енергії: З розвитком цифрових технологій можна більш ефективно інтегрувати джерела відновлювальної енергії, що мають непередбачуваний характер (вітер, сонце) в єдину енергетичну мережу. Це дозволяє зменшити викиди CO_2, але водночас збільшує складність управління енергетичними потоками.

Підвищення рівня автоматизації: Автоматизація, що базується на AI та IoT, дозволить створювати самообслуговуючі системи, здатні самостійно виявляти та усувати проблеми. Це знизить необхідність у фізичному втручанні людей та меншить людський фактор як джерело помилок.

Безпека даних: Як енергетичні мережі стають більш взаємопов'язаними, зростає ризик витоку чи маніпуляції з даними. Проблеми з безпекою даних потребують розробки більш досконалих механізмів захисту, зокрема через використання квантових технологій для шифрування.

Глобальна співпраця: Оскільки енергетична безпека є глобальним викликом, важливо продовжувати розвивати міжнародне співробітництво в сфері захисту енергетичних мереж від кіберзагроз і природних катастроф. Це потребує створення єдиних стандартів і стратегій для забезпечення кібербезпеки.

Таким чином, цифровізація енергетичних систем має потенціал значно підвищити рівень енергетичної безпеки, дозволяючи оперативно реагувати на різноманітні загрози, оптимізувати енергопостачання та знижувати ризики, пов'язані з аваріями та атакою на інфраструктуру. Разом з тим, цифрові технології створюють нові виклики, які потребують постійного вдосконалення систем безпеки та розвитку міжнародного співробітництва для ефективного захисту енергетичних об'єктів.

1.6 Роль цифрових технологій у підвищенні рівня енергетичної безпеки

Цифрові технології сьогодні стали не лише основою для модернізації енергетичних систем, але й важливим інструментом підвищення рівня енергетичної безпеки. В умовах постійно зростаючих викликів — від кіберзагроз до зміни клімату — здатність енергетичних систем швидко адаптуватися до нових умов і своєчасно реагувати на потенційні загрози стає критично важливою. Завдяки цифровим технологіям, таким як великі дані (Big

Data), штучний інтелект (AI), автоматизація, блокчейн, а також новітні системи моніторингу і управління, можна не лише значно знизити ризики, але й забезпечити більш ефективну і стійку роботу енергетичних мереж. Розглянемо детальніше, як саме цифрові технології сприяють підвищенню рівня енергетичної безпеки.

Розглянемо покращення моніторингу і діагностики: використання великих даних. Однією з найбільш важливих переваг цифровізації енергетичних систем є здатність здійснювати моніторинг у реальному часі і проводити діагностику на основі аналізу великих даних. Системи збору і обробки даних дають змогу отримувати інформацію про стан енергетичних мереж, обладнання та споживання енергії з величезною деталізацією і частотою, що дозволяє своєчасно виявляти потенційні проблеми ще на етапі їх виникнення.

Великі дані (Big Data): Ці технології дозволяють збирати, обробляти і аналізувати величезні обсяги інформації з різних джерел, таких як датчики на енергетичних об'єктах, споживчі пристрої, метеорологічні станції тощо. Використовуючи аналітичні алгоритми, можна отримати реальну картину стану системи і визначити місця можливих відмов або перегрузок.

Приклад: У проекті Smart Grid в Німеччині, використовуючи сенсори і технології великих даних, забезпечується моніторинг роботи енергомережі на кожному етапі: від генерації до споживання. Система виявляє аномалії в роботі мережі, наприклад, непередбачуване зниження напруги чи перевантаження трансформаторів, і вчасно подає сигнали для втручання.

Штучний інтелект (AI): AI дозволяє не тільки збирати і обробляти інформацію, але й робити прогнозування розвитку подій на основі минулих даних. Наприклад, штучний інтелект може прогнозувати навантаження на мережу в різних умовах, визначати найкращі варіанти для оптимізації енергопостачання та прогнозувати необхідні заходи для запобігання аваріям.

Приклад: В рамках проекту в Іспанії компанія Iberdrola використовує AI для прогнозування потреб у енергопостачанні на основі даних про попередні споживання, погодні умови та інші фактори. Це дозволяє уникнути перевантажень в мережі та забезпечити баланс між попитом та пропозицією.

Автоматизація управління: реакція на інциденти та нейтралізація загроз.

Цифрові технології дозволяють значно підвищити рівень автоматизації в управлінні енергетичними системами. Це означає, що система здатна виявляти загрози або несправності і автоматично приймати рішення щодо усунення проблем без людського втручання.

Автоматизація аварійних реагувань: Використання автоматизованих систем управління дозволяє швидко реагувати на різного роду інциденти, такі як аварії, перевантаження, короткі замикання, чи кіберзагрози. За допомогою систем SCADA (Supervisory Control and Data Acquisition) енергетичні компанії можуть автоматично запускати необхідні процедури для зупинки або перенаправлення енергопотоків, що знижує ризик великих аварій та пошкоджень.

Приклад: В США компанія Pacific Gas and Electric застосовує автоматизовані системи управління для розподілу енергії. В разі виявлення перевантаження на певному етапі мережі, система автоматично перенаправляє потоки енергії по альтернативних маршрутах, запобігаючи поширенню аварії.

Інтелектуальні мережі (Smart Grids): Це сучасні мережі, що інтегрують різні технології для автоматизації управління та реагування на зміну навантажень. Вони здатні не лише автоматично виявляти і ліквідовувати аномалії в роботі мережі, але й автоматично коригувати параметри роботи генерації і споживання енергії.

Приклад: У Норвегії компанія Statkraft реалізує проект Smart Grid, який здатен оперативно реагувати на перепади навантаження, перенаправляючи енергію та оптимізуючи використання відновлювальних джерел енергії, таких як гідроелектростанції, в залежності від погодних умов.

Моделювання ризиків: прогнозування і стратегічне планування. Цифрові технології дозволяють створювати моделі для прогнозування різних сценаріїв розвитку подій та планування стратегії для їх запобігання. Аналітичні системи здатні моделювати поведінку енергетичних мереж в умовах різних загроз і виявляти слабкі місця в системі.

Моделювання ситуацій: Це дозволяє створювати різноманітні сценарії для аналізу потенційних загроз, таких як надзвичайні ситуації, кібернапади, природні катастрофи, або несправності в обладнанні. Моделювання допомагає визначити найкращі стратегії для збереження стабільності енергетичних мереж. Приклад: У Великій Британії компанія National Grid розробила систему для моделювання й аналізу ризиків. Система здатна прогнозувати вплив несприятливих погодних умов на роботу енергетичних мереж і рекомендувати оптимальні заходи для їх стабілізації.

Прогнозування кіберзагроз: Одним з ключових напрямків є створення моделей для прогнозування кібернападів. Технології машинного навчання дозволяють виявляти аномальні поведінкові патерни в мережах і своєчасно виявляти спроби проникнення або атаки на енергетичну інфраструктуру.

Приклад: В рамках ініціативи CyberX в США компанії, що працюють в енергетичному секторі, застосовують аналітику великих даних для прогнозування можливих кіберзагроз. Завдяки цьому, вони можуть швидко реагувати на нові методи атак і запобігати порушенням безпеки.

Забезпечення прозорості: використання блокчейн-технологій. Блокчейн-технології створюють нові можливості для забезпечення прозорості і надійності в управлінні енергетичними операціями. Оскільки енергетичні системи зазвичай включають численні постачальники, споживачі і посередники, забезпечення прозорості кожної операції є важливим для запобігання шахрайству та маніпуляціям.

Захист даних: Блокчейн може бути використаний для фіксації всіх транзакцій і операцій у енергетичних системах, що дає змогу забезпечити їх

прозорість. Завдяки децентралізованій природі блокчейну можна бути впевненими, що дані не були змінені або сфальсифіковані.

Приклад: Проект Power Ledger в Австралії застосовує технологію блокчейн для забезпечення прозорості і надійності обміну електричною енергією між споживачами та постачальниками. Це дозволяє відслідковувати всю інформацію про споживання та постачання енергії, гарантуючи чесність операцій.

Таким чином, цифрові технології, такі як великі дані, штучний інтелект, автоматизація, моделювання ризиків та блокчейн, мають потужний вплив на підвищення рівня енергетичної безпеки. Вони забезпечують моніторинг в реальному часі, швидке реагування на загрози, створення надійних стратегій для управління ризиками та підвищення прозорості в операціях енергетичних компаній. Завдяки цим технологіям енергетичні системи стають більш стійкими до зовнішніх загроз, таких як природні катастрофи, техногенні аварії або кіберзагрози, що значно підвищує рівень їх безпеки і надійності.

ВИСНОВКИ ДО РОЗДІЛУ 1:

У першому розділі магістерської роботи було проведено дослідження теоретичних аспектів цифровізації енергосистем та енергетичної безпеки. Для цього зроблено декілька важливих висновків щодо значення цифрових технологій, принципів енергетичної безпеки та взаємозв'язку між ними.

Показано, що цифровізація енергосистем є ключовим елементом модернізації енергетичної інфраструктури. Цифровізація енергосистем охоплює використання сучасних технологій для автоматизації процесів управління енергетичними мережами, моніторингу, аналізу великих даних і вдосконалення систем безпеки. Основні складові цифровізації — це інтелектуальні мережі (Smart Grids), інтернет речей (IoT), великі дані, штучний інтелект (AI), а також системи кібербезпеки. Вони забезпечують ефективне управління енергетичними потоками, допомагають виявляти і виправляти несправності, оптимізують розподіл енергії та знижують ризики несанкціонованих втручань у систему.

Енергетична безпека електростанцій — це багатогранне поняття. Енергетична безпека електростанцій охоплює захист від фізичних, техногенних і кіберзагроз, а також забезпечення стабільного енергопостачання. Основними принципами енергетичної безпеки є: забезпечення безперебійного енергопостачання, стійкість до природних і техногенних катастроф, захист від кіберзагроз, а також забезпечення стабільної роботи об'єктів енергетичної інфраструктури. Врахування цих принципів дає змогу створити стійкі та адаптивні енергетичні системи.

Кіберзагрози стають все більш серйозним викликом для енергетичних об'єктів. Кіберзагрози мають значний вплив на енергетичну інфраструктуру, зокрема на електростанції та інші критичні елементи енергомереж. Атаки, як-от DDoS-атаки, вторгнення в мережу, маніпуляції з даними або шкідливе програмне забезпечення, можуть призвести до серйозних відмов у роботі енергетичних об'єктів, що вплине на стабільність постачання енергії. Цифрові

технології, зокрема системи кібербезпеки, допомагають вчасно виявляти та нейтралізувати ці загрози, забезпечуючи стійкість енергетичних мереж.

Міжнародний досвід показує важливість інтеграції цифрових технологій у стратегії енергетичної безпеки. Багато країн уже впроваджують цифрові технології для покращення енергетичної безпеки. Досвід таких країн, як США, Німеччина, Японія та країни ЄС, показує важливість створення національних стратегій для цифровізації енергетичних систем та інтеграції кібербезпеки у велику енергетичну інфраструктуру. Вони активно використовують технології для моніторингу стану мереж, прогнозування навантажень, автоматизації управлінських процесів і запобігання аваріям. Міжнародні стандарти, такі як ISO/IEC 27001 і NIST Cybersecurity Framework, слугують основою для захисту критичних енергетичних інфраструктур.

Цифрові технології відіграють ключову роль у підвищенні рівня енергетичної безпеки. Завдяки застосуванню великих даних, AI, IoT, автоматизації управління і блокчейн-технологій, цифрові системи дозволяють значно покращити енергетичну безпеку. Вони забезпечують:

Покращення моніторингу і діагностики — завдяки чому можливо виявляти потенційні проблеми ще до їх виникнення. Автоматизацію управління — що дозволяє оперативно реагувати на інциденти та нейтралізувати загрози. Моделювання ризиків — дає змогу прогнозувати різні сценарії розвитку подій та розробляти стратегії для запобігання кризовим ситуаціям.

Забезпечення прозорості — блокчейн може застосовуватись для підвищення довіри до енергетичних операцій, гарантування чесності і запобігання фальсифікаціям даних.

Показані перспективи розвитку цифровізації енергетичних систем. Цифровізація енергетичних мереж не тільки допомагає підвищити ефективність і стійкість систем, а й відкриває нові можливості для управління ризиками та забезпечення надійності енергопостачання. Однак для забезпечення максимального ефекту від цих технологій необхідно інтегрувати

їх у комплексні стратегії на рівні держав, міжнародних організацій та приватних компаній. Важливою є також подальша інтеграція відновлювальних джерел енергії в енергетичні мережі, що стане ще одним важливим етапом у розвитку цифрових технологій для забезпечення енергетичної безпеки.

Показано, що використання новітніх цифрових технологій дає можливість знизити вплив кіберзагроз, оптимізувати енергетичні потоки та забезпечити стійкість енергетичних систем до зовнішніх і внутрішніх загроз, що робить їх більш стійкими та адаптивними до кризових ситуацій.

Таким чином, цифровізація енергетичних систем є важливим кроком у забезпеченні надійності, ефективності та безпеки енергопостачання в умовах глобальних викликів. Вона дозволяє суттєво підвищити рівень енергетичної безпеки завдяки покращенню моніторингу, автоматизації управління, моделюванню ризиків та забезпеченню прозорості.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ ДЛЯ ЕНЕРГЕТИЧНИХ ОБЄКТІВ В УМОВАХ ВОЄННОГО СТАНУ

2.1 Особливості функціонування енергетичних об'єктів під час воєнного стану.

В умовах воєнного стану енергетичні системи стають особливо вразливими не лише до фізичних атак, але й до кіберзагроз, які можуть мати катастрофічні наслідки для стабільності енергопостачання та національної безпеки. Залежність сучасних енергетичних об'єктів від цифрових технологій, а також зростаюча складність енергетичних мереж створюють нові можливості для атак з боку ворога. У цьому контексті важливо ретельно аналізувати особливості функціонування енергетичних об'єктів під час воєнного стану, а також вразливості енергетичних систем і потенційні кіберзагрози.

Розглянемо особливості функціонування енергетичних об'єктів під час воєнного стану. В умовах воєнного стану функціонування енергетичних об'єктів зазнає значних змін, оскільки безперебійне енергопостачання стає одним з пріоритетів для держави. Водночас, зростає ризик атак на енергетичну інфраструктуру, як з фізичної, так і з кібернетичної точки зору.

Забезпечення енергетичних резервів: Під час воєнного стану основне завдання для енергетичних компаній полягає в створенні та підтримці стратегічних резервів енергії, зокрема, забезпечення резервних джерел енергопостачання та підтримка стабільної роботи генерації та трансмісії енергії, незважаючи на бойові дії та зовнішні загрози.

Дефіцит ресурсів та персоналу: У період війни зменшується кількість доступних ресурсів та кваліфікованого персоналу для обслуговування та ремонту енергетичних об'єктів. Це збільшує ризики поломок та аварій, особливо в разі фізичних атак на критичні об'єкти.

Адаптація до нових умов кіберзагроз: Враховуючи високий рівень цифровізації енергетичних систем, війна призводить до необхідності адаптації існуючих засобів кібербезпеки, зокрема, до нових типів атак і стратегій зловмисників, спрямованих на знищення або порушення роботи енергетичних систем.

Загроза інфраструктурі з боку ворожих сил: Фізичні атаки на підстанції, енергетичні мережі, об'єкти генерації можуть бути скоординовані з кібернетичними атаками, що створює додаткові труднощі для забезпечення енергетичної безпеки. Крім того, під час воєнних дій особливо важливим стає захист критичних енергетичних об'єктів від атак безпосередньо через мережу Інтернет.

2.2 Аналіз кіберзагроз для енергетичних об'єктів в умовах війни

Кіберзагрози під час війни значно підвищуються через навмисні атаки на енергетичну інфраструктуру для порушення її роботи. В умовах війни енергетичні об'єкти стають привабливими цілями для кібероперацій. Розглянемо типи кіберзагроз:

DDoS-атаки (розподілені атаки на відмову в обслуговуванні): Можуть бути використані для блокування роботи критичних енергетичних систем або серверів, що управляють енергетичними потоками.

Шкідливе ПЗ (Malware): Ворожі програми, такі як віруси, трояни чи руткіти, можуть бути використані для захоплення енергетичних мереж або модифікації їхніх налаштувань, що веде до масштабних аварій.

Атаки на SCADA-системи: Системи контролю та управління (SCADA), що використовуються для моніторингу і управління енергетичними об'єктами, можуть бути атаковані для зміни параметрів роботи генераторів, підстанцій або розподільчих мереж.

Витік даних: Атаки на інформаційні системи енергетичних компаній можуть призвести до витоку конфіденційної інформації, що може бути використано для підготовки наступних атак або розвідки.

Маніпуляції з даними: Зловмисники можуть намагатися змінити показники стану обладнання чи енергетичних потоків, вводячи систему в оману або перешкоджаючи своєчасному виявленню порушень.

Цілі кібернападів на енергетичні об'єкти в умовах війни:

Порушення енергопостачання: Метою кібернападів може бути не лише тимчасове припинення енергопостачання, але й створення довготривалих проблем, які вимагатимуть значних ресурсів для відновлення.

Підрив стабільності економіки та обороноздатності: Проблеми з енергопостачанням можуть призвести до порушень у роботі критичних інфраструктур, що, в свою чергу, може мати значні наслідки для економічної стабільності і обороноздатності країни.

Психологічний ефект: Атаки на енергетичні об'єкти можуть мати не лише технічний, але й психологічний ефект на населення, знижуючи моральний дух, викликаючи паніку або протест.

Розглянемо вразливості енергетичних систем, пов'язані з цифровими технологіями. Цифровізація енергетичних систем, хоча і підвищує їх ефективність, водночас створює нові вразливості, які можуть бути використані для атак. Зокрема:

Інтеграція старих та нових систем: Багато енергетичних об'єктів по всьому світу мають старі технології, які не були повністю модернізовані для захисту від сучасних кіберзагроз. Це створює «технічні вікна» для зловмисників.

Залежність від зовнішніх постачальників: Підключення до глобальних цифрових мереж або взаємодія з постачальниками енергетичних послуг створює додаткові точки уразливості, через які можуть здійснюватися атаки.

Незахищеність в автоматизованих системах управління: Багато енергетичних об'єктів використовують автоматизовані системи для

управління процесами в реальному часі. Проте, якщо ці системи не мають належного захисту, зловмисники можуть скористатися уразливістю для взяття контролю над критичними елементами енергетичних мереж.

Недостатня увага до захисту інформаційних потоків: Багато енергетичних компаній і організацій не приділяють належної уваги захисту даних, що збільшує ймовірність проникнення у внутрішні мережі.

Кейс-стаді: кібератаки на енергетичні об'єкти під час військових конфліктів.

Один з найбільш резонансних прикладів кібератак на енергетичні об'єкти стався під час конфлікту в Україні. Зокрема, кібератаки на українські енергетичні системи в 2015 і 2016 роках продемонстрували вразливість енергетичних мереж до кіберзагроз в умовах війни:

2015 рік: Перша масштабна кібератака на енергетичні об'єкти в Україні призвела до відключення електрики в декількох регіонах. Атака була здійснена через комп'ютерні віруси, що були направлені на системи управління електричними мережами.

2016 рік: Другий напад на енергетичні об'єкти використовував більш складні інструменти, включаючи шкідливе ПЗ, яке дозволяло зловмисникам не лише блокувати енергопостачання, але й маніпулювати даними в реальному часі.

Розглянемо вплив кіберзагроз на критичну інфраструктуру під час воєнного стану. Кіберзагрози можуть мати руйнівний вплив на критичну інфраструктуру, зокрема на енергетичні об'єкти:

Порушення функціонування енергетичної інфраструктури: Кіберзагрози можуть призвести до припинення роботи критичних енергетичних об'єктів, таких як генератори, підстанції, трансформатори, що зупинить енергопостачання на значних територіях.

Втрата контролю над енергетичними мережами: Атаки можуть не лише блокувати постачання енергії, а й дозволяти зловмисникам здійснювати

маніпуляції з параметрами роботи мереж, що може призвести до серйозних аварій та катастроф.

Довготривалий вплив на відновлення: У разі серйозних атак, відновлення енергетичних мереж може зайняти значний час, що призведе до соціально-економічних наслідків для населення та держави в цілому.

Таким чином, загроза кібернападів на енергетичні об'єкти в умовах воєнного стану є однією з основних небезпек для стабільності енергетичних систем. Цифровізація енергетичних мереж надає зловмисникам нові можливості для атак, і важливою частиною забезпечення енергетичної безпеки є посилення кіберзахисту, розробка ефективних механізмів реагування на кіберзагрози та забезпечення надійності критичної інфраструктури.

2.3 Вплив кіберзагроз на критичну інфраструктуру під час воєнного стану

У умовах воєнного стану, коли країна стикається з масовими кіберзагрозами, енергетична інфраструктура є однією з найбільш уразливих ланок критичної інфраструктури. Вплив кіберзагроз на критичні об'єкти має не тільки технічні, але й геополітичні, економічні та соціальні наслідки. Зокрема, атакуючи енергетичні мережі, ворог може не лише викликати фізичні пошкодження обладнання, але й призвести до більш широких, стратегічних наслідків для країни.

Негативний економічний вплив: Порушення роботи енергетичних мереж через кіберзагрози може призвести до значних економічних втрат:

Зупинка виробничих потужностей: Відключення енергопостачання на виробничих підприємствах може призвести до зупинки великих промислових комплексів, що в свою чергу відображатиметься на ВВП країни.

Ріст витрат на відновлення: Витрати на усунення наслідків кібернападів на енергетичні мережі можуть бути дуже високими, що вимагатиме значних державних інвестицій.

Зниження інвестиційної привабливості: Нестабільність енергопостачання через кіберзагрози може вплинути на інвестиційний клімат країни, оскільки інвестори менш охоче вкладатимуть кошти у країни з високими ризиками кібербезпеки.

Вплив на безпеку громадян: Кібернапади на енергетичну інфраструктуру можуть мати прямий вплив на життя та безпеку громадян:

Відключення енергопостачання: Масові відключення електрики можуть вплинути на роботу лікарень, водо- та теплопостачання, системи транспорту, що може спричинити серйозні соціальні наслідки.

Порушення у наданні базових послуг: Нестабільне енергопостачання може ускладнити доступ до води, харчових продуктів, а також спричинити перебої у роботі життєво важливих об'єктів, таких як медичні заклади.

Масова паніка серед населення: Особливо у разі тривалих відключень або масштабних аварій, кібернапади можуть призвести до соціальних протестів або паніки серед населення, що додатково ускладнює ситуацію.

Криза в обороноздатності: Енергетична інфраструктура є критично важливою не лише для цивільного населення, але й для обороноздатності держави:

Вплив на військові об'єкти: Відключення енергопостачання на об'єктах, які важливі для функціонування армії (комунікаційні центри, радіолокаційні станції, центри управління тощо), може ослабити оборонні можливості країни, підвищуючи її вразливість до військових загроз.

Зриви в роботі критичних оборонних систем: Порушення роботи енергетичних систем може вплинути на роботу автоматизованих оборонних систем, що є критичними для захисту від атак або для оперативного реагування на загрози.

Зниження мобільності сил та засобів: Без стабільного енергопостачання, військові підрозділи можуть втратити мобільність через неможливість забезпечення робочих місць з необхідним енергозабезпеченням.

Міжнародні наслідки: Кіберзагрози на енергетичні об'єкти можуть також мати міжнародні наслідки, зокрема в контексті взаємодії з іншими країнами:

Політична ізоляція: Масштабні кібернапади на критичну інфраструктуру можуть спричинити погіршення міжнародних відносин, особливо якщо зловмисники будуть визнані іноземними державами чи терористичними організаціями.

Відповідальність на міжнародному рівні: У разі виявлення зовнішньої агресії, країна може бути змушена звертатися до міжнародних організацій, таких як ООН або НАТО, для захисту від кібернападів на критичну інфраструктуру.

Розглянемо висновки та рекомендації:

1. Підвищення рівня захисту енергетичних об'єктів: У період воєнного стану необхідно приділяти значну увагу захисту енергетичних систем, зокрема їх кібербезпеці. Для цього варто впроваджувати більш ефективні механізми виявлення та блокування кіберзагроз, оновлення захисту програмного забезпечення та залучення фахівців для постійного моніторингу енергетичних об'єктів.

2. Створення національних стратегій кібербезпеки: Важливо розробити комплексні національні стратегії кібербезпеки, які включатимуть плани на випадок кібератак на енергетичну інфраструктуру та інші критичні об'єкти. Це повинно включати чіткі протоколи для швидкої реакції, а також створення резервних систем управління в разі критичних ситуацій.

3. Інвестування в цифрові технології для кіберзахисту: Для захисту енергетичних об'єктів слід активно впроваджувати новітні цифрові технології, такі як штучний інтелект, великі дані та блокчейн для забезпечення прозорості та моніторингу енергетичних потоків, а також системи виявлення вторгнень і автоматизовані механізми реагування на кіберзагрози.

4. Розвиток співпраці з міжнародними партнерами: Ураховуючи глобальний характер кіберзагроз, важливо укріплювати міжнародну

співпрацю з іншими країнами, особливо в межах організацій, що займаються питаннями кібербезпеки (наприклад, Європейський Союз, НАТО, ООН), для обміну досвідом і технічними ресурсами для забезпечення надійності енергетичної інфраструктури.

5. Постійне навчання і підготовка персоналу: Персонал, який працює в енергетичних компаніях, повинен проходити регулярне навчання з питань кібербезпеки та бути готовим до реагування на різного роду загрози. Це допоможе швидше виявляти потенційні атаки і знижувати їхній вплив на енергетичну систему.

Таким чином, кіберзагрози в умовах воєнного стану є однією з найбільших загроз для енергетичної безпеки. Своєчасне впровадження заходів щодо посилення захисту енергетичних об'єктів, підвищення рівня кібербезпеки та міжнародна співпраця можуть значно знизити ризики від таких атак і забезпечити стійкість енергетичної інфраструктури в умовах сучасних загроз.

2.4 Стратегії протидії кіберзагрозам на енергетичних об'єктах під час воєнного стану

Зважаючи на зростаючі кіберзагрози, енергетичні системи повинні вживати низку стратегій для забезпечення кібербезпеки та підтримання стабільності у разі воєнних дій. Ось кілька ключових напрямків для протидії кіберзагрозам на енергетичних об'єктах:

Інтеграція багаторівневих систем захисту: Системи захисту енергетичних об'єктів мають включати багаторівневий підхід, що дозволяє забезпечити кілька рівнів оборони від кіберзагроз. Така стратегія дозволяє пом'якшити наслідки атак, навіть якщо один із рівнів захисту буде скомпрометовано.

Фізичний рівень захисту: Важливим є захист фізичних об'єктів (енергетичних підстанцій, трансформаторних станцій, генераторів тощо) від

фізичних атак, таких як саботаж, терористичні акти, а також від проникнення в серверні кімнати або інші критичні зони.

Мережевий рівень захисту: Сучасні системи автоматизації енергетичних об'єктів потребують застосування ефективних технологій безпеки на рівні мереж, таких як шифрування трафіку, сегментація мереж, виявлення аномальної активності.

Рівень контролю та моніторингу: Використання засобів моніторингу та виявлення вторгнень, таких як системи IDS/IPS (Intrusion Detection/Prevention Systems), які можуть виявляти спроби несанкціонованого доступу до важливих систем у реальному часі.

Розглянемо запровадження автоматизованих систем реагування. В умовах воєнного стану енергетичні об'єкти повинні мати можливість швидко реагувати на кіберзагрози без втручання людини. Це особливо важливо, оскільки людина не завжди в змозі швидко прийняти необхідні рішення в умовах стресу або після потужної кібератаки.

Автоматичне відновлення функціонування систем: Системи повинні мати механізми автоматичного відновлення після кібернападів. Наприклад, у разі спроби маніпулювання з параметрами генерації чи розподілу енергії, автоматичні алгоритми можуть коригувати ці параметри для збереження стабільності мережі.

Системи на основі штучного інтелекту (AI): Використання AI для аналізу даних з мережі та систем енергетичних об'єктів дозволяє виявляти навіть невеликі аномалії, які можуть вказувати на потенційну атаку або збій у роботі системи.

Розглянемо розвиток резервних та альтернативних систем енергопостачання. Для забезпечення безперервності постачання енергії важливо мати резервні механізми, які дозволять компенсувати втрати в разі кібернападів або фізичних атак на енергетичні об'єкти.

Резервні енергетичні джерела: Потрібно мати резервні джерела енергії, такі як дизельні генератори, батареї або відновлювальні джерела енергії, що можуть забезпечити енергопостачання в разі серйозних атак або природних катастроф.

Децентралізація енергопостачання: Зростаюча залежність від великих централізованих енергетичних мереж робить їх вразливими. Розвиток децентралізованих систем, зокрема мікромереж, може зменшити ризики, оскільки в разі збоїв в одній частині мережі інші частини залишатимуться в роботі.

Розглянемо регулярне оновлення та тестування систем кібербезпеки. В умовах постійної еволюції кіберзагроз, регулярне оновлення та тестування систем безпеки є важливим елементом підтримки високого рівня захисту.

Пенетестація та аудити безпеки: Регулярні пенетестації (тестування на проникнення) та аудити дозволяють виявляти уразливості в системах безпеки і своєчасно їх виправляти.

Поновлення програмного забезпечення та патч-менеджмент: Потрібно постійно оновлювати програмне забезпечення для захисту від новітніх видів шкідливих програм та уразливостей, що можуть бути використані кіберзлочинцями.

Розглянемо навчання персоналу та підвищення кваліфікації. Людський фактор є однією з найбільших вразливостей енергетичних систем у боротьбі з кіберзагрозами. Тому важливо забезпечити постійне навчання персоналу та вдосконалення навичок реагування на інциденти.

Тренування для ситуаційних сценаріїв: Працівники повинні регулярно проходити тренування, що симулюють реальні кіберзагрози, наприклад, тренування з виявлення фішингових атак або дій у разі великих інцидентів, що вимагають скоординованої відповіді.

Підвищення обізнаності серед співробітників: Важливо, щоб кожен працівник був свідомий основних принципів кібербезпеки, наприклад, як

розпізнавати фішингові листи, не натискати на підозрілі посилання або не використовувати слабкі паролі.

Розглянемо міжнародну співпрацю в сфері кібербезпеки. У зв’язку з глобальними кіберзагрозами важливим є обмін досвідом і координація дій на міжнародному рівні. Спільні зусилля з іншими країнами та міжнародними організаціями (наприклад, ЄС, НАТО, ООН) дозволяють створювати спільні механізми захисту критичних інфраструктур.

Обмін інформацією та розвідка: Зміцнення співпраці з міжнародними партнерами у сфері обміну інформацією про нові кіберзагрози, зловмисні групи, а також стратегічний захист інфраструктури.

Спільні тренування та навчання: Участь в міжнародних симуляціях і тренуваннях, що моделюють реальні ситуації з кіберзагрозами до і під час воєнного стану, дозволяє краще підготуватися до потенційних атак.

Розглянемо важливість кіберзахисту для енергетичних систем: Зі збільшенням рівня цифровізації енергетичних мереж необхідно постійно підвищувати рівень кіберзахисту для забезпечення стабільності роботи енергетичних об'єктів у разі воєнного стану або іншого екстреного періоду.

Комплексний підхід до безпеки: Застосування багаторівневих стратегій захисту, автоматизованих систем реагування та резервних енергетичних джерел дозволяє знизити ризики від атак на енергетичні мережі, зберігаючи безперервність енергопостачання.

Міжнародна співпраця та постійний розвиток: Захист енергетичних об'єктів від кіберзагроз вимагає тісної міжнародної співпраці, постійного оновлення технологій безпеки та підвищення кваліфікації персоналу.

Таким чином, в умовах воєнного стану кібербезпека енергетичних систем повинна стати пріоритетом для всіх країн, які хочуть забезпечити стійкість своїх енергетичних інфраструктур і мінімізувати потенційні наслідки від кіберзагроз. Щоб значно підвищити рівень захисту енергетичних об'єктів в умовах воєнного стану, необхідно застосовувати декілька стратегічних підходів, які забезпечать надійний захист від кіберзагроз, збереження

критичних інфраструктур та відновлення роботи енергетичних систем після атак.

Розглянемо створення національних та локальних кібербезпекових центрів. Для ефективного реагування на кіберзагрози енергетичні об'єкти мають бути інтегровані у національні та міжнародні мережі кібербезпеки. Одним із важливих елементів є створення кібербезпекових центрів на національному та локальному рівнях, які займалися б координацією дій, моніторингом загроз, обміном даними і належним реагуванням на кіберінциденти.

Національний центр реагування на кіберзагрози: Створення організацій, що будуть координувати дії між державними установами, енергетичними компаніями та міжнародними партнерами для миттєвого реагування на кібернапади. Такі центри також забезпечують моніторинг та збір інформації про нові кіберзагрози, аналіз ситуацій та спільну підготовку до можливих атак.

Локальні центри кібербезпеки для енергетичних об'єктів: Кожен великий енергетичний об'єкт або група об'єктів повинна мати спеціалізовані команди для реагування на кіберзагрози, які б забезпечували безперервний моніторинг і швидке відновлення постачання енергії в разі атак.

Одна з найбільш ефективних стратегій захисту від кіберзагроз — це концепція "Zero Trust" (нульова довіра). Це підхід, згідно з яким довіряти жодному користувачеві або пристрою не можна, навіть якщо вони знаходяться всередині корпоративної мережі. Такий підхід передбачає:

Перевірку на кожному етапі доступу: Для доступу до будь-якої частини енергетичної інфраструктури або даних кожен запит перевіряється, незалежно від того, чи знаходиться пристрій всередині або поза мережею.

Сегментація мережі та мінімізація прав доступу: Кожен пристрій або користувач отримує доступ лише до тих ресурсів, які необхідні для виконання конкретних завдань, що мінімізує ризик компрометації цілих систем у разі атаки.

Мультифакторна автентифікація (MFA): Використання додаткових методів автентифікації, таких як одноразові паролі або біометричні дані, значно ускладнює доступ до критичних систем навіть у разі отримання пароля зловмисниками.

Розглянемо підвищення рівня автоматизації та штучного інтелекту. Умови воєнного стану вимагають швидкої реакції на будь-яку кіберзагрозу, тому енергетичні компанії повинні впроваджувати автоматизовані рішення на основі штучного інтелекту (ШІ), які допоможуть не лише виявляти загрози, але й автоматично усувати їх.

Використання ШІ для виявлення аномалій: Системи штучного інтелекту можуть здійснювати постійний моніторинг енергетичних мереж, виявляючи навіть незначні аномалії, які можуть вказувати на потенційну кібератаку. Наприклад, у разі несанкціонованих спроб змінити параметри енергетичної системи, ШІ може миттєво виявити такі зміни та вжити заходів щодо їх нейтралізації.

Прогнозування та моделювання загроз: ШІ та аналітичні системи можуть використовувати історичні дані та алгоритми для моделювання можливих сценаріїв розвитку подій, що дозволяє планувати стратегії для запобігання загрозам і їх усунення ще до того, як вони стануть реальністю.

Кібербезпека є глобальним викликом, тому національні уряди та енергетичні компанії повинні активно співпрацювати з міжнародними організаціями та кібербезпековими агентствами для спільної боротьби з кіберзагрозами.

Спільні кібероперації: Спільні ініціативи з міжнародними партнерами дозволяють краще координувати зусилля з виявлення кіберзагроз, обміну даними та розвідки кіберзагроз.

Розвиток міжнародних стандартів і протоколів кібербезпеки: Універсальні міжнародні стандарти забезпечують більш ефективне протистояння глобальним кіберзагрозам. Такі стандарти допомагають

встановити єдині правила реагування на кіберінциденти, що важливо у разі транснаціональних атак.

Інвестиції в кібербезпеку: В умовах зростаючих кіберзагроз необхідно значно збільшити фінансування та ресурси для розвитку кіберзахисту в енергетичних системах. Безпечність енергетичних об'єктів — це не лише технічне питання, але й стратегічне для забезпечення національної безпеки.

Постійне вдосконалення кіберзахисту: Енергетичні компанії повинні постійно оновлювати свої системи безпеки, використовуючи новітні технології, такі як штучний інтелект, автоматизація та концепція "Zero Trust".

Навчання і підготовка персоналу: Людський фактор є важливим елементом кібербезпеки, тому регулярне навчання та тренування працівників з кіберзахисту є обов'язковим. Також важливо підтримувати культури обізнаності щодо кіберзагроз серед всіх співробітників.

Міжнародна співпраця: Сучасні кіберзагрози є глобальними, тому важливо посилювати співпрацю між країнами, міжнародними організаціями та компаніями, що займаються кібербезпекою для ефективного реагування на кіберзагрози.

Таким чином, кібербезпека енергетичних об'єктів є критично важливим аспектом для підтримання національної безпеки в умовах воєнного стану. Комплексний підхід до захисту, включаючи сучасні технології, підготовку персоналу і міжнародну співпрацю, дозволить забезпечити стійкість енергетичних систем до кібератак і зберегти надійність енергопостачання навіть в умовах кризових ситуацій.

Розглянемо рекомендації щодо підвищення стійкості енергетичних об'єктів до кіберзагроз під час воєнного стану. З огляду на зростаючі кіберзагрози для енергетичних об'єктів у часи воєнного стану, важливо врахувати низку рекомендацій, що дозволяють мінімізувати ризики та забезпечити безперервність функціонування енергетичних систем. Ось кілька ключових напрямків для посилення стійкості та ефективного захисту від кіберзагроз:

Удосконалення інфраструктури для забезпечення безпеки. Для мінімізації потенційних ризиків кіберзагроз, важливо вдосконалити існуючі фізичні та цифрові інфраструктури на енергетичних об'єктах.

Посилення захисту фізичних об'єктів: Оскільки кіберзагрози можуть супроводжуватися фізичними атаками (наприклад, на серверні кімнати або важливі компоненти енергетичних станцій), необхідно підвищити рівень фізичного захисту критичних інфраструктур. Це включає встановлення систем контролю доступу, охоронних сигналізацій, відеоспостереження, а також посилення захисту серверних та інших ключових зон від несанкціонованого доступу.

Модернізація старих систем: У багатьох випадках старі енергетичні системи (особливо в країнах, що переживають кризу чи воєнний стан) можуть мати значні вразливості. Оновлення застарілих технічних рішень та інтеграція сучасних цифрових технологій можуть суттєво підвищити рівень захисту. Важливо звертати увагу на інтеграцію систем моніторингу в реальному часі, систем виявлення вторгнень (IDS) та систем автоматичного реагування.

Розвиток стійких до атак мереж і технологій: Управління енергетичними мережами повинно здійснюватися з урахуванням високого рівня безпеки і стійкості до кіберзагроз.

Дистрибуція та розподіл енергетичних ресурсів: Замість централізованих енергетичних систем, які піддаються значним ризикам у разі атак, варто розвивати локальні дистрибутивні мережі та мікромережі. Така дистрибуція дозволить знизити рівень залежності від однієї точки у разі атак, а також забезпечить надійність енергопостачання для споживачів.

Розвиток систем управління через блокчейн: Застосування технології блокчейн для реєстрації та моніторингу операцій в енергетичних системах дозволяє забезпечити прозорість і захищеність даних. Блокчейн гарантує незмінність записів і захист від маніпуляцій із даними, що особливо важливо для запобігання фальсифікаціям і зловживанням у критичних енергетичних операціях.

Розглянемо розвиток національних і міжнародних партнерств у кібербезпеці. Справжня кібербезпека для енергетичних об'єктів можлива лише в рамках тісної співпраці на міжнародному рівні. Ось кілька можливих напрямків для вдосконалення такої співпраці:

Обмін даними та спільне реагування на загрози: Системи обміну інформацією про кіберзагрози між енергетичними компаніями, урядами, а також міжнародними організаціями повинні працювати цілодобово. Спільний доступ до баз даних, розвідки загроз і моделей поведінки атакуючих груп дозволить краще прогнозувати можливі кіберзагрози та швидше реагувати на них.

Визначення та імплементація міжнародних стандартів кібербезпеки: Важливим кроком є імплементація міжнародних стандартів кібербезпеки (наприклад, NIST, ISO 27001) у практику енергетичних компаній. Вони дозволяють створити єдину мову та протоколи для реагування на кіберзагрози та підвищують ефективність співпраці між країнами та організаціями.

Залучення спеціалістів і ресурсів для реагування на кібератаки: Спільні навчання, тренування та практичні симуляції, де країни і компанії можуть тестувати свої системи реагування на кіберзагрози, допоможуть виявити слабкі місця в стратегії кібербезпеки та забезпечити оперативне відновлення після атак.

Людський фактор залишається однією з найбільших вразливостей енергетичних об'єктів у випадку кіберзагроз. Тому важливо:

Регулярне навчання і підвищення кваліфікації персоналу: Працівники повинні регулярно проходити тренінги, де навчаться визначати підозрілі дії та обробляти кіберінциденти. Це включає навчання по боротьбі з фішинговими атаками, виявленню зловмисних дій у мережах та безпеки при використанні корпоративних пристроїв.

Мобільні команди з реагування на кіберінциденти: Для швидкого реагування на кіберінциденти під час воєнного стану повинні бути створені мобільні команди, які мають спеціальні навички для швидкого відновлення

енергетичних об'єктів після атак, а також для аналізу і нейтралізації загроз на місці.

Резервування енергетичних ресурсів є ключовим компонентом кібербезпеки в умовах воєнного стану. Необхідно створити альтернативні способи енергопостачання для критичних об'єктів та систем.

Мобільні та автономні джерела енергії: В умовах атаки на основні енергетичні об'єкти можуть бути розгорнуті мобільні енергетичні системи, такі як дизельні генератори або відновлювальні джерела енергії (сонячні панелі, вітрові турбіни), що забезпечать безперервне енергопостачання.

Резервні дані та інфраструктура: Важливо також передбачити створення резервних копій критичних даних та інфраструктур на окремих платформах, які не пов'язані з основними мережами енергетичних об'єктів, що дозволить відновлювати роботу систем навіть у разі виведення з ладу основних серверів і контролерів.

Таким чином, в умовах воєнного стану, кіберзагрози для енергетичних об'єктів стають одними з найсерйозніших викликів для національної безпеки. Кібернапади можуть не лише порушити роботу енергетичних систем, але й призвести до катастрофічних наслідків, таких як руйнування критичної інфраструктури, порушення енергопостачання або навіть до гуманітарних криз.

Виходячи з цього, важливо застосовувати комплексний підхід до забезпечення кібербезпеки енергетичних об'єктів, який включає використання передових технологій, таких як штучний інтелект, блокчейн та автоматизовані системи управління, а також удосконалення фізичного захисту об'єктів. Крім того, стратегічна співпраця на міжнародному рівні, ефективне навчання персоналу та розбудова резервних систем енергопостачання є важливими кроками для підвищення стійкості енергетичних систем до кіберзагроз.

Реалізація цих стратегій дозволить мінімізувати ризики та забезпечити надійне функціонування енергетичних об'єктів навіть у найскладніших умовах воєнного стану..

ВИСНОВКИ ДО РОЗДІЛУ 2:

У другому розділі роботи були визначені основні вимоги та завдання, щодо особливості функціонування енергетичних об'єктів під час воєнного стану: В умовах воєнного стану функціонування енергетичних об'єктів зазнає серйозних викликів, зокрема через вплив не лише фізичних атак, а й кіберзагроз. Збої в енергетичному постачанні можуть мати катастрофічні наслідки для держави, оскільки енергетична інфраструктура є основою для нормального функціонування економіки та життєдіяльності населення. Водночас, енергетичні об'єкти стають мішенями не тільки для військових атак, але й для кіберзлочинців, які намагаються через кібератаки викликати збій у роботі критичних систем. Проведено аналіз кіберзагроз для енергетичних об'єктів під час війни: Кіберзагрози в умовах війни набувають особливого значення, оскільки військові операції часто супроводжуються масштабними кібернападами, спрямованими на енергетичні об'єкти. До таких загроз належать атакувальні програми, фішинг, атаки на мережі SCADA, а також вплив на енергетичні системи через вразливості в інтернет-системах зв'язку. Кібератаки на енергетичні об'єкти можуть спричиняти тривалі відключення енергопостачання, порушення стабільності енергетичних мереж і навіть серйозні екологічні або економічні наслідки. Визначено, вразливості енергетичних систем, пов'язані з цифровими технологіями: Використання цифрових технологій у сучасних енергетичних системах значно підвищує ефективність їх управління, однак воно також відкриває нові вразливості, які можуть бути використані зловмисниками. Це зокрема стосується використання Інтернету речей (IoT), систем автоматизованого управління (SCADA), а також новітніх технологій зв'язку. Вразливості в цих технологіях можуть бути використані для здійснення кіберзагроз, таких як атаки на сервери, компрометація баз даних, або навіть віддалене управління важливими енергетичними процесами.

Показано кейс-стаді: кібератаки на енергетичні об'єкти під час військових конфліктів: Історія неодноразово підтверджує, що енергетичні об'єкти часто є основними цілями кібератак під час військових конфліктів. Протягом останніх років кілька країн зазнали масштабних кібератак на енергетичні інфраструктури, серед яких можна виділити атаки на енергомережі в Україні, Іраку, США та інших країнах. Ці приклади вказують на те, що кібератаки можуть не лише порушити роботу енергосистем, але й стати важливою складовою в загальній стратегії ведення війни. Обгрунтовано вплив кіберзагроз на критичну інфраструктуру під час воєнного стану: Вплив кіберзагроз на критичну інфраструктуру є значним, оскільки пошкодження енергетичних мереж може мати ланцюговий ефект, впливаючи на роботу інших важливих секторів, таких як транспортування, водопостачання та зв'язок. У разі серйозної кібератаки на енергетичні об'єкти, держави стикаються не тільки з втратами у вигляді фінансових збитків, але й з високими соціальними, гуманітарними та економічними наслідками. В умовах воєнного стану, це може призвести до порушення життєзабезпечення, паніки серед населення і затримок у відновленні нормальної діяльності держави. Таким чином, кіберзагрози для енергетичних об'єктів у часи воєнного стану є серйозною загрозою для національної безпеки, оскільки енергетична інфраструктура є критично важливою для функціонування держави. Вразливості енергетичних систем, пов'язані з цифровими технологіями, значно збільшують потенційні можливості для кібератак, які можуть не тільки порушити роботу енергетичних мереж, а й мати руйнівний ефект на всю інфраструктуру країни. Рішення щодо підвищення рівня кібербезпеки повинні включати інтеграцію передових технологій для захисту від кіберзагроз, розвиток стратегій реагування на кіберінциденти. Зважаючи на потенційні наслідки, необхідно значно посилити захист енергетичних об'єктів від кіберзагроз у умовах воєнного стану, застосовуючи комплексний підхід, що включає як технологічні, так і організаційні заходи.

РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ЕЛЕКТРОСТАНЦІЙ ЧЕРЕЗ ЦИФРОВІ ТЕХНОЛОГІЇ

3.1. Розробка системи моніторингу та захисту інформаційних технологій на енергетичних об'єктах

Цифрові технології надають потужні інструменти для підвищення рівня енергетичної безпеки електростанцій, особливо в умовах загроз з боку кібернападів. Інтеграція інноваційних цифрових рішень дозволяє не лише оптимізувати процеси управління енергетичними об'єктами, а й підвищити їх стійкість до різноманітних ризиків. Ось основні методи, що сприяють цьому.

Одним із важливих напрямків цифровізації енергетичних систем є створення та вдосконалення систем моніторингу та захисту інформаційних технологій (ІТ) на енергетичних об'єктах. Це забезпечує своєчасне виявлення потенційних загроз і аномалій у роботі електростанцій. До основних компонентів таких систем можна віднести:

Системи моніторингу реального часу: Завдяки цим системам можливий постійний моніторинг операційної діяльності енергетичних об'єктів, що дозволяє швидко реагувати на будь-які порушення або аномалії. Наприклад, на українських енергетичних об'єктах застосовуються такі рішення як "Система моніторингу мережевих інцидентів" (IDS) для виявлення та аналізу загроз в режимі реального часу.

Системи виявлення вторгнень (IDS/IPS): Вони активно застосовуються для захисту комп'ютерних мереж від несанкціонованого доступу, зокрема до критичних енергетичних систем, таких як SCADA (системи управління і контролю). Така система виявляє аномалії в мережах і може автоматично блокувати потенційні атаки.

Приклад: у 2017 році в Україні було здійснено кібератаку на енергетичну компанію "Укренерго", де спрацювала система моніторингу, що вчасно

виявила вторгнення та дозволила заблокувати частину мережі, знизивши масштаб збитків.

Розглянемо використання штучного інтелекту (AI) та машинного навчання для прогнозування та реагування на кіберзагрози. Штучний інтелект (AI) і машинне навчання активно використовуються для прогнозування та реагування на кіберзагрози. Ці технології дозволяють обробляти великі обсяги даних і виявляти приховані патерни, що можуть свідчити про кіберзагрози на енергетичних об'єктах.

Прогнозування атак: Використання алгоритмів машинного навчання дозволяє аналізувати історичні дані про атаки та визначати ймовірні сценарії розвитку нових загроз. AI може передбачити потенційні слабкі місця в інфраструктурі і рекомендувати заходи для їх усунення.

Автоматизоване реагування: AI може автоматично реагувати на кіберзагрози, активуючи відповідні механізми захисту без необхідності втручання людини. Це скорочує час реакції на атаки та зменшує ймовірність людських помилок. Приклад: компанії, що використовують AI для аналізу кіберзагроз, мають можливість виявляти нові види шкідливих програм до того, як вони заподіють значну шкоду. Наприклад, такі системи були використані для моніторингу кіберзагроз на енергетичних об'єктах в США після серії атак на енергетичні мережі в 2016 році.

Розглянемо роль блокчейн-технологій у забезпеченні безпеки даних енергетичних систем. Блокчейн є технологією, що гарантує безпеку і прозорість обробки та зберігання даних завдяки використанню дистрибутивних реєстрів. Вона має великий потенціал для забезпечення безпеки даних на енергетичних об'єктах, особливо в контексті управління енергетичними потоками та транзакціями.

Забезпечення прозорості операцій: Використання блокчейну для реєстрації всіх транзакцій і операцій на енергетичних об'єктах дає змогу зменшити ризик фальсифікації або маніпуляцій з даними. Блокчейн забезпечує

незмінність даних, що дозволяє відслідковувати кожен етап процесу і забезпечувати захист від шахрайства.

Безпека енергетичних мереж: Блокчейн може використовуватися для забезпечення безпеки даних про виробництво, споживання та розподіл енергії в реальному часі, що дозволяє запобігати втручанню сторонніх осіб у процеси енергетичних мереж. Приклад: в рамках проєктів по дистрибуції відновлювальної енергії в Європі активно застосовуються блокчейн-рішення для оптимізації енергетичних транзакцій та забезпечення прозорості в роботі енергетичних постачальників.

Інтернет речей (IoT) — це система взаємопов'язаних пристроїв, що обмінюються даними через Інтернет. IoT має важливе значення для енергетичних об'єктів, оскільки дозволяє створювати "розумні" системи для автоматичного управління та моніторингу.

Інтелектуальні датчики та пристрої: Встановлення IoT-пристроїв дозволяє постійно збирати дані про стан енергетичних систем, таких як температура, вологість, напруга та інші критичні параметри. Ці дані передаються в центральну систему моніторингу, де за допомогою аналітики можна вчасно виявляти загрози.

Управління віддаленими об'єктами: Завдяки IoT можливо здійснювати віддалене управління енергетичними об'єктами, що дає змогу оперативно реагувати на будь-які зміни в ситуації. Приклад: розумні лічильники, що використовуються в енергетичних мережах для моніторингу споживання енергії, використовують IoT для відправлення даних в центральну систему для подальшої обробки та аналізу.

3.2 Впровадження систем управління кібербезпекою на енергетичних об'єктах

Системи управління кібербезпекою (Cybersecurity Management Systems, CMS) є основою для комплексного захисту енергетичних об'єктів від

кіберзагроз. Такі системи включають в себе низку технологій і протоколів для управління безпекою, моніторингу, а також для автоматичного реагування на інциденти.

Інтеграція багаторівневого захисту: Система кібербезпеки має забезпечувати захист на всіх рівнях інфраструктури — від фізичного до цифрового. Вона включає в себе не лише технічні засоби, але й організаційні заходи щодо навчання персоналу, а також процедури реагування на інциденти.

Моніторинг та аналіз кіберзагроз: Системи для постійного моніторингу дозволяють визначати загрози на ранніх стадіях і автоматично запускати контрзаходи, такі як ізоляція атакуючих систем.

Розглянемо ризики та переваги цифровізації енергетичних систем для забезпечення безпеки. Цифровізація енергетичних систем приносить як значні переваги, так і певні ризики. Переваги включають підвищену ефективність управління, зниження людських помилок і можливість швидкого реагування на зміни. Однак, зростає ймовірність атак через нові вразливості в системах. Важливо збалансувати використання новітніх технологій із забезпеченням високого рівня кібербезпеки. Ці цифрові рішення в сукупності допомагають не лише покращити ефективність енергетичних об'єктів, але й значно підвищити їх стійкість до кіберзагроз і зменшити ризики, пов'язані з технічними неполадками або атаками на енергетичні інфраструктури.

Розглянемо моделювання та оцінка впливу цифрових технологій на енергетичну безпеку. Моделювання та оцінка впливу цифрових технологій на енергетичну безпеку дозволяють не лише зрозуміти, як ці технології можуть покращити захист енергетичних систем, але й оцінити їх ефективність у реальних умовах. Ці методи дають можливість прогнозувати й аналізувати потенційні загрози, а також визначати оптимальні стратегії для підвищення стійкості енергетичних об'єктів до кіберзагроз та інших кризових ситуацій.

Математичне моделювання енергетичних систем дає змогу передбачити поведінку систем у разі різних сценаріїв кіберзагроз та аварій. Для цього використовуються такі методи:

Динамічне моделювання: Це метод, який дозволяє досліджувати енергетичну систему в реальному часі та оцінювати її реакцію на різні види кіберзагроз, зокрема на атаки, що можуть призвести до відключення певних елементів мережі або втрати контролю над окремими підсистемами.

Системи багатокритеріальної оптимізації: Такі методи дозволяють визначати найкращі рішення для реагування на кіберзагрози, враховуючи безпеку, економічні витрати, технічні обмеження та інші фактори.

Симуляція сценаріїв атак: За допомогою симуляцій можна створити умовні сценарії, які моделюють поведінку енергетичних систем під впливом різних типів кіберзагроз, таких як DoS-атаки, відключення елементів SCADA-системи чи викрадення критичних даних. Приклад: В рамках одного з досліджень в Німеччині було розроблено математичне моделювання для прогнозування реакції енергетичних мереж на кіберзагрози. Моделювання дозволило виявити найбільш вразливі елементи в системах контролю та автоматизації.

Розглянемо оцінку ефективності впровадження цифрових технологій для забезпечення безпеки. Оцінка ефективності впровадження цифрових технологій є важливим етапом для перевірки їх здатності захистити енергетичні системи від кіберзагроз. Така оцінка включає в себе:

Аналіз зниження ризиків: Оцінка того, наскільки цифрові технології знижують ймовірність успішних атак на енергетичні об'єкти та яким чином покращують стійкість до можливих інцидентів.

Рівень безпеки даних: Оцінка ефективності засобів захисту даних, таких як криптографія, блокчейн, системи багатофакторної аутентифікації тощо.

Продуктивність і економічність: Оцінка того, наскільки інтеграція нових цифрових технологій покращує продуктивність енергетичних об'єктів, при цьому знижуючи операційні витрати на обслуговування та управління кібербезпекою. Приклад: В рамках проєктів з цифровізації енергетичних мереж в Японії були використані системи блокчейн для підвищення безпеки

розподілу енергії. Оцінка їх ефективності показала зниження операційних витрат на 20%, а також підвищення рівня захисту від маніпуляцій з даними.

3.3 Розробка алгоритмів моніторингу та аналізу кіберзагроз в реальному часі

Інтеграція алгоритмів моніторингу та аналізу кіберзагроз у реальному часі є необхідною умовою для забезпечення постійної готовності енергетичних об'єктів до потенційних атак. Важливим аспектом є використання великих даних (Big Data) для аналізу загроз.

Аналіз потоків даних: Алгоритми, що працюють із великими обсягами даних, дозволяють виявляти навіть найменші аномалії в роботі енергетичних об'єктів, що можуть свідчити про кіберзагрози. Наприклад, відхилення від норми у споживанні енергії, чи незвичні зміни в режимах роботи енергетичних установок можуть бути сигналами потенційної атаки.

Штучний інтелект та машинне навчання: Використання AI для аналізу даних з енергетичних систем дозволяє автоматично визначати патерни, які можуть свідчити про загрози в режимі реального часу. Приклад: У США на енергетичних об'єктах було впроваджено систему моніторингу на основі AI, яка здатна в реальному часі виявляти потенційні кібератаки, пов'язані з аномальним споживанням енергії, використовуючи алгоритми машинного навчання.

Розглянемо створення та аналіз тестових сценаріїв для оцінки стійкості енергетичних об'єктів. Моделювання тестових сценаріїв є важливою частиною оцінки стійкості енергетичних об'єктів до кіберзагроз. За допомогою таких тестів можна оцінити, як енергетична інфраструктура реагує на різні сценарії кіберзагроз, включаючи як відомі, так і нові типи атак.

Сценарії реальних атак: Створення тестових сценаріїв на основі реальних випадків кіберінцидентів дозволяє відтворити ситуації, схожі на ті,

що сталися в минулому. Це дає змогу протестувати готовність систем до подібних атак.

Тестування нових загроз: Створення сценаріїв для нових типів кіберзагроз дозволяє енергетичним компаніям підготуватися до ще невідомих атак. Приклад: В Україні в рамках підготовки до захисту енергетичних об'єктів від кіберзагроз були проведені навчання, на яких використовувалися різні сценарії атак на енергетичні мережі. Тестування дозволило виявити кілька слабких місць у системах, що могли б бути використані під час реальних атак.

Розглянемо оцінку впливу воєнних та кіберзагроз на роботу електростанції. Вплив воєнних і кіберзагроз на роботу електростанцій може бути катастрофічним, тому важливо оцінювати не лише технічні, але й економічні, соціальні та екологічні наслідки таких інцидентів.

Аналіз економічних наслідків: Пошкодження або виведення з ладу енергетичних об'єктів під час кіберзагрози може спричинити значні фінансові втрати, включаючи витрати на відновлення інфраструктури, штрафи за порушення контрактів або відшкодування втрат бізнес-партнерам.

Оцінка впливу на безпеку та навколишнє середовище: Виведення з ладу критичних енергетичних об'єктів може призвести до екологічних катастроф, таких як витоки палива або аварії на ядерних об'єктах. Це вимагає детального аналізу можливих наслідків кожної окремої загрози. Приклад: В Україні під час війни 2022 року атаки на енергетичні інфраструктури спричинили значні пошкодження, що негативно вплинуло на роботу електростанцій. Оцінка збитків показала, що, окрім економічних витрат, були також серйозні соціальні та екологічні наслідки.

Таким чином, цифрові технології відіграють ключову роль у підвищенні енергетичної безпеки електростанцій, надаючи інструменти для моніторингу, захисту та управління кіберзагрозами. Методи моделювання та оцінки, такі як математичне моделювання, оцінка ефективності технологій, аналіз кіберзагроз у реальному часі, а також створення тестових сценаріїв, є важливими для підвищення стійкості енергетичних систем у разі атак. Однак

цифровізація також приносить нові ризики, що потребують уважної оцінки та виваженого підходу до впровадження нових технологій в критичні інфраструктури.

Розглянемо перспективи розвитку цифрових технологій для забезпечення енергетичної безпеки. Цифровізація енергетичних систем продовжує розвиватися, відкриваючи нові можливості для підвищення рівня безпеки та ефективності управління енергетичними об'єктами. Перспективи розвитку технологій у цьому контексті зумовлені кількома ключовими напрямками:

Розвиток квантових технологій для кібербезпеки енергетичних систем. Однією з найперспективніших новітніх технологій є квантове шифрування, яке може значно покращити рівень безпеки даних в енергетичних системах. Завдяки квантовим алгоритмам забезпечується неймовірно високий рівень захисту від несанкціонованого доступу до критичних даних, що особливо важливо для енергетичних об'єктів у часи кризових ситуацій чи війни.

Квантова криптографія може бути використана для шифрування зв'язку між елементами енергетичної мережі, знижуючи ризики від перехоплення чи маніпуляцій з інформацією.

Квантові комп'ютери здатні значно підвищити ефективність алгоритмів виявлення та нейтралізації кіберзагроз, оскільки мають здатність швидко обробляти величезні обсяги даних і аналізувати складні моделі загроз. Приклад: Квантові технології активно розробляються в лабораторіях таких компаній, як IBM та Google. Вони вже досягли певних успіхів у квантовому шифруванні, що може бути застосовано для енергетичних об'єктів у майбутньому.

Автоматизація реагування на кіберзагрози за допомогою роботизованих систем. Застосування роботизованих систем для реагування на кіберзагрози стає важливим етапом розвитку цифрових технологій у забезпеченні енергетичної безпеки. Автоматичні системи можуть не лише виявляти загрози,

але й здійснювати дії, спрямовані на блокування атак і нейтралізацію шкідливих програм.

Роботизовані системи для моніторингу та реагування можуть бути розгорнуті для активного захисту кіберпростору енергетичних об'єктів. Вони автоматично виконують завдання виявлення атак, оновлення програмного забезпечення, коригування параметрів захисту без втручання людини. Такі системи також можуть використовувати алгоритми глибокого навчання для самонавчання і покращення своїх дій на основі аналізу попередніх атак. Приклад: На кількох атомних станціях в США вже тестують роботизовані системи, які можуть миттєво реагувати на спроби кібернападів, самостійно виявляючи і блокуючи загрози.

Інтеграція блокчейн-технологій в управління енергетичними мережами. Блокчейн продовжує залишатися важливим інструментом для забезпечення прозорості та безпеки даних у енергетичних мережах. В умовах цифровізації енергетичних об'єктів блокчейн може бути використаний для управління транзакціями, моніторингу розподілу енергії, а також для підвищення надійності та прозорості операцій.

Смарт-контракти на основі блокчейн можуть автоматизувати процеси купівлі-продажу енергії, знижуючи ймовірність шахрайства та маніпуляцій.

Безпека даних: Завдяки своїй дистрибутивній природі, блокчейн гарантує високу безпеку збереження та передавання даних, що важливо для захисту від кіберзагроз. Приклад: В рамках глобальних ініціатив по цифровізації енергетичних систем, таких як "Energy Web Foundation", активно використовуються блокчейн-рішення для забезпечення прозорості у розподілі енергії, а також для моніторингу енергетичних транзакцій у реальному часі.

Використання 5G для підвищення безпеки зв'язку енергетичних об'єктів. 5G технології відкривають нові можливості для швидкої і надійної передачі даних в реальному часі, що особливо важливо для безпеки енергетичних систем у кризових ситуаціях.

Мобільність та швидкість передачі даних: 5G дозволяє забезпечити високошвидкісний, стабільний зв'язок між різними елементами енергетичних мереж, що знижує ризики від затримок в обміні інформацією та дозволяє оперативно реагувати на загрози.

Підвищена безпека зв'язку: Завдяки покращеним технологіям шифрування в 5G, можливості зламу і перехоплення сигналу значно знижуються, що важливо для критичних інфраструктур. Приклад: В Китаї на деяких нових енергетичних станціях впроваджуються 5G-мережі для моніторингу та управління в реальному часі, що дозволяє значно підвищити ефективність захисту даних та мереж.

Розвиток "розумних мереж" (Smart Grids). Розумні мережі або Smart Grids є важливим напрямком у цифровізації енергетичних систем. Вони дозволяють інтегрувати відновлювальні джерела енергії, ефективно управляти енергетичними потоками та забезпечувати більш високий рівень безпеки.

Інтеграція відновлювальних джерел енергії: Розумні мережі дозволяють більш ефективно керувати енергетичними потоками, знижуючи навантаження на традиційні джерела енергії і зменшуючи ризики порушень у разі кризових ситуацій.

Миттєвий моніторинг та регулювання: Завдяки використанню IoT і AI, "розумні мережі" можуть автоматично коригувати параметри енергетичної системи в залежності від змін попиту та пропозиції, що дозволяє підтримувати стабільність і уникати аварій. Приклад: В Європі в рамках проєктів Horizon 2020 активно тестуються розумні енергетичні мережі, які можуть автоматично регулювати споживання енергії в умовах кризових ситуацій, знижуючи ризики великих відключень.

Таким чином, цифрові технології надають потужні інструменти для підвищення енергетичної безпеки електростанцій, забезпечуючи надійний захист від кіберзагроз, автоматизацію управління енергетичними потоками та інтеграцію відновлювальних джерел енергії. Серед перспективних технологій особливо варто відзначити розвиток квантових технологій для кібербезпеки,

автоматизованих систем реагування, використання 5G для забезпечення надійного зв'язку та блокчейн для забезпечення прозорості та безпеки даних. Технології штучного інтелекту та машинного навчання, а також розвиток "розумних мереж" створюють нові можливості для адаптації енергетичних систем до змін у зовнішньому середовищі та покращення стійкості до загроз. Водночас, з кожним новим кроком в цифровізації зростає потреба в комплексному підході до кібербезпеки для зменшення потенційних ризиків і забезпечення стійкості енергетичних систем у сучасних умовах.

ВИСНОВКИ ДО РОЗДІЛУ 3:

Показано, що цифрові технології відіграють ключову роль у забезпеченні енергетичної безпеки електростанцій. Вони не лише підвищують рівень захисту від кіберзагроз, а й сприяють автоматизації управління енергетичними потоками, що дозволяє ефективніше контролювати і оптимізувати використання енергоресурсів. Крім того, інтеграція відновлювальних джерел енергії за допомогою цифрових інструментів забезпечує стабільність енергетичних систем та сприяє сталому розвитку енергетичної галузі.

Цифрові технології також відкривають нові можливості для моніторингу стану обладнання в реальному часі, що дозволяє оперативно виявляти потенційні неполадки і здійснювати профілактичне обслуговування. Це, в свою чергу, знижує ризики виникнення аварій та підвищує загальну ефективність роботи енергетичних систем.

Інтеграція великих даних та аналітики дозволяє прогнозувати навантаження на енергетичні мережі, оптимізувати використання ресурсів та знижувати витрати. У свою чергу, це допомагає зменшити негативний вплив на навколишнє середовище та сприяє переходу до більш сталих і зелених форм енергетики.

Отже, застосування цифрових технологій не лише покращує безпеку та ефективність енергетичних систем, але й відіграє важливу роль у забезпеченні сталого розвитку енергетичних процесів, інтеграції відновлювальних джерел енергії та зменшенні викидів шкідливих речовин в атмосферу. Це стає важливим елементом для досягнення глобальних цілей у сфері сталого розвитку та енергетичної трансформації.

Додатково, цифрові технології сприяють розвитку нових моделей енергетичних мереж, таких як "розумні мережі" (smart grids), які забезпечують більш гнучке та ефективне управління енергетичними потоками. Ці мережі можуть автоматично адаптуватися до змін в попиті та пропозиції енергії,

оптимізуючи розподіл електричної енергії та знижуючи ймовірність перевантажень або перебоїв в постачанні. Завдяки цьому досягається більша стабільність та надійність роботи енергетичних систем.

У майбутньому інтеграція цифрових технологій дозволить ще більшою мірою персоналізувати споживання енергії. Наприклад, за допомогою інтелектуальних приладів та систем управління в будинках і підприємствах, споживачі зможуть контролювати свої енергетичні витрати та зменшувати навантаження на мережу, що сприятиме зниженню загальних енергетичних витрат і підвищенню ефективності.

Таким чином, застосування цифрових інструментів у енергетичному секторі відкриває нові горизонти для розвитку більш стабільних, ефективних та екологічно чистих енергетичних систем. Це є важливим кроком до забезпечення енергетичної незалежності, зниження викидів вуглецю та досягнення більш сталого та економічно вигідного майбутнього для всього світу. Також важливим є впровадження блокчейн-технологій для забезпечення прозорості та безпеки в управлінні енергобезпекою.

У перспективі, розвиток штучного інтелекту та машинного навчання також стане важливим фактором для вдосконалення управління енергетичними системами. Ці технології дозволять аналізувати величезні обсяги даних, отриманих від датчиків, камер та інших пристроїв, з метою прогнозування майбутніх навантажень на енергетичні мережі та виявлення потенційних проблем до того, як вони виникнуть. Це забезпечить проактивне управління енергетичними ресурсами і дозволить ще більше зменшити час реагування на неполадки, що підвищить загальну надійність енергетичної інфраструктури.

ВИСНОВКИ

Показано, що цифрові технології стали важливим елементом у забезпеченні ефективного управління енергетичними системами та підвищенні їх рівня безпеки. Цифровізація включає впровадження сучасних інформаційних технологій, таких як AI, IoT, блокчейн та машинне навчання, які дозволяють не тільки оптимізувати процеси управління енергетичними потоками, а й забезпечити захист від різних кіберзагроз. Ці інструменти сприяють інтеграції відновлювальних джерел енергії, підвищенню енергоефективності та надійності енергетичних систем.

Енергетична безпека є критично важливою складовою функціонування електростанцій і забезпечення сталого енергопостачання. Вона охоплює не тільки фізичний захист від зовнішніх загроз, а й кіберзахист інформаційних систем, що керують енергетичними потоками. У роботі визначено ключові принципи та компоненти енергетичної безпеки, зокрема надійність, доступність, стійкість до кіберзагроз та інтеграція відновлювальних джерел енергії.

У роботі детально розглянуто різні види кіберзагроз, що можуть впливати на енергетичні об'єкти, зокрема атаки на інформаційні системи управління, що можуть призвести до аварій та втрати контролю над енергетичними мережами. Особливу увагу приділено вразливостям, пов'язаним із цифровими технологіями, що використовуються для моніторингу та управління енергетичними процесами.

Аналіз міжнародного досвіду показав, що багато країн вже активно впроваджують цифрові технології для підвищення енергетичної безпеки, застосовуючи сучасні системи моніторингу та захисту від кіберзагроз, що дозволяє їм ефективно протидіяти різноманітним загрозам та мінімізувати ризики для національних енергетичних інфраструктур.

Розглянуто різноманітні методи використання цифрових технологій для підвищення безпеки енергетичних об'єктів, зокрема застосування систем

моніторингу та захисту інформаційних технологій, використання AI та машинного навчання для прогнозування та виявлення кіберзагроз, а також інтеграція Інтернету речей (IoT) для покращення управління енергетичними потоками.

З огляду на особливості воєнного стану, виявлено високий ризик виникнення кіберзагроз, що можуть серйозно вплинути на критичну інфраструктуру, зокрема на енергетичні об'єкти. Вразливості енергетичних систем, пов'язані з цифровими технологіями, значно зростають в умовах війни, що робить необхідним посилення заходів з кібербезпеки.

У роботі запропоновано методи математичного моделювання енергетичних систем з урахуванням кіберзагроз та алгоритми для моніторингу і оцінки стійкості енергетичних об'єктів в реальному часі. Важливим елементом є розробка тестових сценаріїв, які дозволяють оцінити вплив кіберзагроз та воєнних дій на роботу електростанцій, що дозволяє своєчасно виявляти слабкі місця в системах безпеки.

Цифровізація енергетичних систем має як значні переваги, так і певні ризики. Переваги включають підвищення ефективності управління, інтеграцію відновлювальних джерел енергії та зниження витрат. Однак, одночасно з цим зростає ймовірність кіберзагроз, що потребує постійного вдосконалення систем кібербезпеки та нагляду за енергетичними мережами.

Загалом, цифровізація є важливим кроком у забезпеченні енергетичної безпеки, але для досягнення оптимальних результатів необхідно враховувати потенційні ризики та постійно вдосконалювати захист від кіберзагроз, зокрема в умовах воєнних конфліктів.

З огляду на швидкий розвиток цифрових технологій, майбутнє енергетичних систем очевидно залежатиме від подальшої інтеграції новітніх технологій, таких як 5G, штучний інтелект, і технології блокчейн. Ці інструменти забезпечать більш ефективне управління енергетичними потоками, дозволять значно підвищити рівень автоматизації, а також покращать безпеку енергетичних систем, знижуючи ризики помилок людини

і зловмисних атак. Крім того, ці технології дозволять більш ефективно взаємодіяти з відновлювальними джерелами енергії, знижуючи залежність від традиційних енергетичних ресурсів і роблячи енергетичні системи більш стійкими та адаптивними до змін у попиті та пропозиції енергії.

У ході дослідження були запропоновані низка рекомендацій щодо покращення рівня енергетичної безпеки через цифрові технології, зокрема:

Впровадження комплексних систем моніторингу та захисту для виявлення та реагування на кіберзагрози в реальному часі.

Розробка та впровадження більш ефективних алгоритмів прогнозування та виявлення аномалій в енергетичних мережах, що базуються на штучному інтелекті та машинному навчанні.

Посилення кіберзахисту критичної інфраструктури в умовах воєнного стану та зростаючих кіберзагроз.

Активне використання блокчейн-технологій для забезпечення прозорості та безпеки обміну даними між енергетичними підприємствами та споживачами.

Збільшення інвестицій у дослідження та розвиток нових цифрових технологій для енергетичного сектору, особливо в частині захисту від кіберзагроз.

Таким чином, цифровізація енергетичних систем є важливою складовою забезпечення їх безпеки та ефективності. Застосування сучасних цифрових технологій дозволяє значно знижувати ризики, пов'язані з кіберзагрозами, оптимізувати використання енергетичних ресурсів і сприяти інтеграції відновлювальних джерел енергії в енергосистеми. Однак це також вимагає постійного вдосконалення систем захисту, розробки нових методів кібербезпеки та адаптації до умов, що змінюються, зокрема в умовах воєнного стану. Усі ці фактори роблять цифровізацію важливим елементом стратегічного розвитку енергетичного сектору, здатним забезпечити стабільне та безпечне функціонування енергетичних систем у майбутньому.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Воркунова О. В., Ярова Н. В., Яровий В. І. Економічна безпека підприємств морського транспорту в умовах цифровізації. Розвиток методів управління та господарювання на транспорті. Одеса, 2024. № 1(86).С. 37–52. URL: https://www.daemmt.odesa.ua/index.php/daemmt/article/view/508

2. Дергачова Г. М., Колешня Я. О. Цифрова трансформація бізнесу : сутність, ознаки, вимоги та технології. Економічний вісник Національного технічного університету України «Київський політехнічний інститут». 2020. №. 17. С. 280–290.

3. Корнієнко О. П. Морський транспорт в період четвертої індустріальної революції. Регіональна економіка та управління. 2021. № 4 (34). С. 67–71.

4. Кулішова О., Котенко В., Яковцев С. Перспективи впровадження цифрових технологій у процеси управління операційною безпекою морських портів. Таврійський науковий вісник. Серія: Економіка. 2022. № 11. С. 76–85. DOI: https://doi.org/10.32851/2708-0366/2022.11.11

5. Мурад’ян А. О., Демидюков О. В. Особливості розвитку морських портів в умовах цифрових трансформацій : закордонний досвід. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2022. Том 33(72). № 6. С. 247–252. URL: https://tech.vernadskyjournals.in.ua/journals/2022/6_2022/40.pdf

6. Пядишев В. Г. (2023). Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. Морська безпека. 2023. № 1. С. 78–86. DOI: https://doi.org/10.32782/msd/2023.1.10

7. Ярова Н. В., Воркунова О. В., Куликов Д. В. Енергоефективність підприємств портової галузі України. Розвиток методів управління та господарювання на транспорті. Одеса. 2024. № 2(87). С. 34–46. URL:https://www.daemmt.odesa.ua/index.php/daemmt/article/view/525

8. Ярова Н. В., Воркунова О. В., Куликов Д. В. Підвищення енергоефективності морських портів // Modern research in science and education. Proceedings of the 3rd International scientific and practical conference. BoScience Publisher. Chicago, USA. 2023. Pp. 1016–1019. URL: https://sci-conf.com.ua/iii-mizhnarodna-naukovopraktichna-konferentsiya-modern-research-in-science-and-education-9-11-11-2023-chikago-ssha-arhiv/

9. Ярова Н. В., Воркунова О. В., Яровий В. І. Цифровізація морської галузі. Abstracts of III International Scientific and Practical Conference. Prague, Czech Republic. 2023. Pp. 42–43. URL: https://eu-conf.com/events/scientific-opinions-on-modern-methods-of-solving-problems/

10. Ярова Н. В., Угрік І. С. Діджиталізація контейнерних перевезень : тези доп. 75-ої студ. наук.-техн. конф. ОНМУ, м. Одеса, 27–28 квітня 2022 р. Одеса, 2022. С. 220–221. URL: https://www.onmu.odessa.ua/images/university/news/75-Student_conf_spring_programm_2022_2.pdf URL: https://www.onmu.odessa.ua/images/university/news/75-Student_conf_spring_artic_2022_1.pdf

11.Яровий В. І. Інновації та цифровізація економіки. Проблеми і перспективи розвитку транспорту : матеріали XII Всеукр. наук.-практ. конф. студентів та молодих вчених : програма. Одеса : ОНМУ, 2024. URL: https://onmu.org.ua/images/university/news/XII_conf_trans_online_2024_progr.pdf

12. Adabere, Sandra & Owusu Kwateng, Kwame & Dzidzah, Esther & Kamewor, Francis. (2021). Information technologies and seaport operational efficiency. Marine Economics and Management. https://www.researchgate.net/publication/354819152_Information_technologies_and_seaport_operational_efficiency

13. Evripidis P. Kechagias, Georgios Chatzistelios, Georgios A. Papadopoulos, Panagiotis Apostolou, Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical

Infrastructure Protection, Volume 37, 2022, 100526. DOI: https://doi.org/10.1016/j.ijcip.2022.100526

14. Gavalas, Dimitris, Syriopoulos, T. & Roumpis E. Digital adoption and efciency in the maritime industry. J. shipp. trd. 7, 11 (2022). DOI: https://doi.org/10.1186/s41072-022-00111-y

15. Green Ports Fund & Financing Initiative. Asian Development Bank. 27 July 2023. URL: https://az659834. vo.msecnd.net/eventsairseasiaprod/production-adb-public/6e812c23af374512a4e05f7077b29870

16. Jovi´c, M., Tijan, E., Vidmar, D., Pucihar, A., 2022b. Factors of Digital Transformation in the Maritime Transport Sector. Sustainability, 14 (15), 9776.

17. Impact of Disruptive Technologies on Maritime Trade and Maritime Industry Blockchain, 3D Printing, e-Commerce & Battery Technology (for Harbour Craft). Singapore. URL: https://www.researchgate.net/publication/343211774_Impact_of_Disruptive_Technologies_on_Maritime_Trade_and_Maritime_Industry

18. International Convention for the prevention of Pollution from Ships, 1973 (MARPOL 1973) (Consolidated Edition, 2012). URL: https://www.imo.org/en/GoogleSearch/SearchPosts/Default.aspx?q=MARPOL%201973

19. Review of Maritime Transport 2021 – UNCTAD. Geneva. URL: https://tech.vernadskyjournals.in.ua/journals/2022/5_2022/48.pdf

20. Zeeshan Raza, Johan Woxenius, Ceren Altuntas Vural, Mikael Lind, Digital transformation of maritime logistics: Exploring trends in the liner shipping segment, Computers in Industry, Volume 145, 2023, 103811, ISSN 0166-3615. DOI: https://doi.org/10.1016/j.compind.2022.103811

21. Yarova Nina, Baryshnikova Vira, Moskalenko Dmytro & Nikiforov Vyacheslav. Development of container transportation on the danube: current trends // Challenges and problems of modern science. Proceedings of the XVII International Scientific and Practical Conference. London, United Kingdom. 2023. Pp. 12–15. URL: https://conference-w.com/