НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

28 травня 2025 року

Київ – 2025

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 05 від 29 травня 2025 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 28 травня 2025 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2025. 90 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 28, 2025. Kyiv: PIMEE NAS of Ukraine, 2025. 90 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, професор,
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

В.Ф. Залужний

КІБЕРНЕТИЧНИЙ ЗАХИСТ РОЗПОДІЛЕНИХ АВТОМАТИЗОВАНИХ СИСТЕМ ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ СИЛАМИ ТА ЗАСОБАМИ В ТЕХНОЛОГІЧНИХ ВІЙНАХ НОВОГО ПОКОЛІННЯ

Розкриті особливості функціонування розподілених автоматизованих систем організаційного управління силами і засобами в умовах ведення кібернетичної боротьби.

Визначенні кібернетичні впливи на розподілені автоматизовані системи організаційного управління силами і засобами в технологічних війнах нового покоління.

Обговорюються шляхи підвищення кібернетичного захисту розподілених автоматизованих систем організаційного управління силами і засобами для забезпечення їх живучості.

Ключові слова: розподілені автоматизовані системи, сили та засоби, живучість, штучний інтелект, кібернетична боротьба, кібернетичний захист.

Вступ

Широкомасштабне впровадження у всі сфери життя інформаційних технологій приводить до суттєвих змін у військовій справі. Війни майбутнього все більше переміщуються в цифрову площину, а кібернетичний домен стає таким же важливим полем бою, як суходіл, вода, повітря, космос, інформаційний та когнітивний простір.

Обов'язковим атрибутом сучасних високотехнологічних воєнних конфліктів є *комплексне ведення кібернетичної боротьби* або окремих її складових елементів (кібернетичної розвідки, кібернетичного захисту, кібернетичного впливу) на всіх етапах підготовки та ведення операцій (бойових дій).

Сучасні воєнні конфлікти, які спрямовані на реалізацію принципів гібридної та мережецентричної війни, передбачають використання розподілених автоматизованих систем організаційного управління (РАСОУ) для ефективного застосування на полі бою сил і засобів (СЗ).

Використання РАСОУ СЗ забезпечує *інформаційно-аналітичну перевагу* над противником за рахунок:

створення угруповання військ (сил), у тому числі формування його структури та складу, адаптованого до умов ведення сучасної збройної боротьби. Це вимагає створення єдиного інформаційного простору, єдиних баз даних, забезпечення інформаційної сумісності та надходження інформації від різноманітних автоматизованих, інформаційно-комунікаційних систем та засобів передавання даних;

наявності відповідних технічних та програмних засобів для збирання інформації, її колективного використання та організації взаємодії. Це вимагає об'єднання окремих систем розвідки, зв'язку, автоматизації на підставі єдиних ідеологічних, технологічних (програмних), технічних принципів і платформ у розвідувально-інформаційно-бойову систему;

досягнення високого ступеня взаємного узгодження дій в операціях (бойових діях) за рахунок: ясного та логічного формування замислу операції (бойових дій), що гарантує його адекватне й однакове сприйняття військами; компетентності у всіх ланках управління військами; повноти інформації; відсутності спотворення інформації в процесі її передавання; наявності системи правил узгодження дій частин і підрозділів під час підготовки та ведення операції (бойових дій);

боєздатного особового складу підготовленого теоретично, технічно і психологічно до дій в високотехнологічних операціях (бойових діях).

РАСОУ СЗ притаманні розгалужена мережа засобів зв'язку і комунікацій, використання різноманітних інформаційних технологій, насиченість комплексами засобів автоматизації та складна структура системи їх енергозабезпечення. Як наслідок, спектр об'єктів та елементів РАСОУ СЗ, що піддаються кібернетичного впливу постійно розширюється, форми та способи його нанесення противником постійно удосконалюються та урізноманітнюються.

У таких умовах, значно зростають вимоги до кібернетичного захисту РАСОУ СЗ, як складової частини комплексної системи забезпечення її живучості, що і обумовлює *актуальність* даної теми.

Основна частина

Кібернетичній боротьбі в РАСОУ СЗ притаманні певні *особливості*:

залучення до формування та реалізації кібернетичних впливів різних суб'єктів: державних військових інституцій (сил та засобів кібернетичних військ); неурядових організацій за державного спонсорування під військовим керівництвом (state-sponsored cyberattack); державних військових інституцій (сил та засобів кібернетичних військ) під виглядом неурядових організацій із повним запереченням причетності до подій держави-агресора, що надає конфлікту гібридності та унеможливлює притягнення суб'єкта до відповідальності за міжнародним гуманітарним правом;

постійне оновлення технологічної бази РАСОУ СЗ (штучний інтелект, хмарні сервіси, інтернету речей (IoT), гібридні моделі роботи органів військового управління, які збільшують ризики, пов'язані з використанням незахищених пристроїв та мереж та інші), що приводить до необхідності пошуку нових методів та механізмів їх захисту;

значні наслідки кібернетичного впливів на РАСОУ СЗ у разі відсутності стійкої та адаптованої до кібернетичних впливів системи кібернетичного захисту;

зростання кількості кібернетичних загроз як за кількістю впливів, так і за їхньою складністю;

систематичне удосконалення методів кібернетичного впливу (атаки на основі штучного інтелекту (AI-driven attacks), шкідливе програмне забезпечення з можливістю самонавчання тощо).

Дані особливості дозволяють сформувати *основні кібернетичні впливи на РАСОУ СЗ* в технологічних війнах нового покоління:

кібернетичні злами – атаки на сервери РАСОУ СЗ з метою отримання противником необхідних даних;

DDoS-атаки – перевантаження складових елементів РАСОУ СЗ для виведення з ладу систем зв'язку та комунікаційних мереж;

шкідливе програмне забезпечення – віруси, трояни та шпигунські програми, що використовуються для дезорганізації системи;

фішингові атаки – спроби отримати доступ до конфіденційної інформації шляхом введення в оману;

використання квантових технологій – зламування криптографічних алгоритмів, що використовуються в РАСОУ СЗ ;

атаки на критичну інфраструктуру РАСОУ СЗ – ураження енергетичних, транспортних та комунікаційних систем.

Зростання кількості та складності кібернетичних впливів для РАСОУ СЗ вимагає розроблення *ефективних механізмів реагування* на них, які можуть мінімізувати потенційні збитки та забезпечити необхідний рівень живучості системи.

Процес реагування на кібернетичні впливи в РАСОУ СЗ можливо забезпечити за рахунок комплексу заходів, спрямованих на ідентифікацію, аналіз, стримування, усунення та відновлення після кібернетичного впливу. Головна мета цього процесу – *мінімізувати кібернетичний вплив* на РАСОУ СЗ, *захистити* її критичні елементи та *забезпечити* безперервність та необхідну ефективність процесів управління військами та зброєю.

Для *підвищення ефективності кібернетичного захисту* РАСОУ СЗ, як складової частини комплексної системи забезпечення її живучості, доцільно розглянути використання в найближчій перспективі таких передових технологій та методів:

захист військових серверів та баз даних з використанням хмарних технологій з багаторівневим шифруванням;

використання пост-квантової криптографії для розроблення нових алгоритмів шифрування, стійких до атак квантових комп'ютерів та їх стандартизація;

інтеграція кібернетичного захисту на рівні обладнання (hardware-level security) для IoT-пристроїв;

використання штучного інтернету для моніторингу та захисту мереж IoT у реальному масштабі часу, виявлення аномалій у поведінці систем та користувачів, що дозволяє оперативно реагувати на загрози;

впровадження технології Zero Trust (модель "нульової довіри", яка передбачає перевірку кожного користувача та пристрою на кожному етапі доступу до системи) для підвищення надійності та стійкості функціонування елементів з розподіленою інфраструктурою;

автоматизація заходів кібернетичного захисту з використанням штучного інтелекту для моніторингу кібернетичних загроз, розроблення алгоритмів на основі штучного інтелекту, спроможних автоматично розпізнавати і блокувати кібернетичні атаки.

Зазначені передові технології та методи, насамперед, передбачають широке використання штучного інтелекту для автоматизації операцій з кібернетичного захисту РАСОУ СЗ та протидії загрозам "нульового дня", коли противник використовує вразливості, невідомі виробникам програмного забезпечення. Моделі машинного навчання можуть виявляти та реагувати на підозрілі дії, які можуть свідчити про атаку нульового дня.

Впровадження нових технологій та методів кібернетичного захисту РАСОУ СЗ вимагає розуміння основ традиційних принципів кібернетичної безпеки (мережева безпека, криптографія, контроль доступу та політики безпеки тощо) для побудови ефективних заходів безпеки навколо систем штучного інтелекту.

З метою *створення сучасної системи кібернетичного захисту* РАСОУ СЗ необхідно:

для розуміння можливостей та обмежень штучного інтелекту в системі кібернетичного захисту:

визначити фундаментальне розуміння концепцій машинного навчання та штучного інтелекту в РАСОУ СЗ (організація контрольованого та неконтрольоване навчання, навчання з підкріпленням, нейронні мережі та загальні алгоритми тощо);

продовжити роботу щодо розвитку в РАСОУ СЗ захищеної системи обробки та інтерпретації великих масивів даних;

для розуміння дій противника в кібернетичному домені:

систематично аналізувати варіанти супротивного машинного навчання, що забезпечить розуміння можливостей використання штучного інтелекту для ворожих атак та побудови відповідних моделей захисту від них;

систематично здійснювати заходи щодо тестування РАСОУ СЗ на проникнення: аналіз етичних методів хакерства, можливостей використання штучного інтелекту для виявлення вразливостей і моделювання кібератак, методологій, методів та способів для тестуванні на проникнення та інших заходів;

Штучний інтелект є потужним інструментом в сучасних технологіях кібернетичного захисту РАСОУ СЗ. Але дуже важливо використовувати його в поєднанні з людським досвідом та постійними науковими дослідженнями і розробками. Тому впровадження в системі кібернетичного захисту РАСОУ СЗ передових

технологій неможливе без формування якісної системи підготовки персоналу з питань кібернетичного захисту, постійного аудиту стану його підготовленості та готовності до реагування на виклики та загрози в кібернетичному домені.

Висновки

Забезпечення живучості РАСОУ СЗ ЗС можливе за умови створення ефективної системи кібернетичного захисту її елементів та підсистем.

Зростання кількості кібернетичних впливів на РАСОУ СЗ ЗС, систематичне їх удосконалення вимагає оперативного впровадження в системи кібернетичного захисту новітніх технологій та методів.

Тільки синергія між штучним інтелектом та людським інтелектом дозволяє створити ефективну систему кібернетичного захисту РАСОУ СЗ.

Удосконалення системи кібернетичного захисту РАСОУ СЗ обумовлює доцільність створення якісної системи підготовки персоналу, здатної оперативно адаптуватися до змін у ведення технологічних війн нового покоління.

І.Ю. Пилипчук

РОЗРОБКА МЕТОДІВ АВТОМАТИЗОВАНОГО СИНТЕЗУ ПОЛІТИК БЕЗПЕКИ ДЛЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ З ВИКОРИСТАННЯМ ГЕНЕТИЧНИХ АЛГОРИТМІВ

Сучасні системи управління інформаційною безпекою (СУІБ) потребують гнучких і ефективних політик безпеки для забезпечення відповідності стандартам і протидії кіберзагрозам. Ручне створення таких політик є трудомістким і схильним до помилок, що ускладнює їх адаптацію до динамічних умов. Метою дослідження є розробка методів автоматизованого синтезу політик безпеки для СУІБ з використанням генетичних алгоритмів.

Проведено аналіз теоретичних основ генетичних алгоритмів, включаючи принципи еволюційних обчислень, оптимізації та їх застосування в задачах кібербезпеки. Виявлено основні проблеми традиційних підходів до створення політик безпеки, такі як низька адаптивність до нових загроз, складність масштабування та потреба в експертному втручанні. Для вирішення цих проблем запропоновано метод, який передбачає використання генетичних алгоритмів для автоматичного генерування та оптимізації політик безпеки на основі стандартів ISO/IEC 27001 і NIST SP 800-53 [1].

Запроваджено систему автоматизованого синтезу політик, що використовує генетичні алгоритми для створення правил доступу та реагування на загрози. Розроблено алгоритм оцінки ефективності політик, який враховує критерії безпеки, продуктивності та відповідності стандартам. Для забезпечення сумісності використано стандартизовані формати політик і API для інтеграції з хмарними СУІБ. Впроваджено систему моніторингу синтезованих політик, яка відстежує їх продуктивність і генерує звіти для аудиторів. Для оптимізації створено централізовану платформу управління політиками, що уникає дублювання даних. Впроваджено систему зворотного зв’язку, яка дозволяє алгоритмам удосконалюватися на основі оцінок адміністраторів [2].

Експеримент проведено на прикладі хмарної СУІБ для обробки конфіденційних даних, де автоматизований синтез політик скоротив час їх створення на 22%. Перевагами підходу є автоматизація рутинних завдань, підвищення адаптивності політик і спрощення сертифікаційних процесів. Для забезпечення конфіденційності застосовано шифрування даних і управління доступом через IAM-політики. Впроваджено систему електронного документообігу для координації між командами безпеки та розробки. Розроблено інструменти для автоматичного тестування синтезованих політик у різних сценаріях загроз.

Додатково впроваджено механізм автоматичного резервного копіювання конфігурацій політик, що знижує ризик збоїв. Для навчання фахівців організовано тренінги з використання генетичних алгоритмів у кібербезпеці, що сприяє підвищенню їхньої кваліфікації. Впроваджено візуальний інтерфейс для управління синтезом і аналізом політик.

Для підвищення продуктивності синтезу застосовано алгоритми паралельної обробки, що зменшують час обчислень. Впроваджено базу знань із шаблонами політик безпеки, що полегшує їх адаптацію до різних систем. Для забезпечення масштабованості інтегровано хмарні платформи з підтримкою еластичних обчислень. Розроблено інструменти автоматичного аналізу ефективності політик, що дозволяють виявляти неефективні правила.

Для підтримки командної роботи створено централізовану систему управління версіями політик, що синхронізує зміни в гібридних середовищах. Впроваджено механізм автоматичного тестування політик перед розгортанням, що знижує ризик помилок. Для спрощення аудиту безпеки розроблено модуль автоматичного генерування звітів, сумісних із ISO/IEC 27001.

Додатково впроваджено систему прогнозування нових вимог до політик на основі аналізу регуляторних змін за допомогою алгоритмів машинного навчання. Для забезпечення безперебійної роботи розроблено механізм автоматичного відновлення конфігурацій політик після збоїв. Впроваджено стандартизовані шаблони для документування синтезу політик, що полегшує сертифікацію. Для інтеграції з зовнішніми системами створено API для обміну даними політик [3].

Для підвищення адаптивності СУІБ розроблено програмний модуль для автоматичного оновлення політик відповідно до нових загроз і стандартів. Впроваджено систему оцінки ефективності синтезованих політик, яка дозволяє оптимізувати їх конфігурацію. Для підтримки розробників створено інтерактивну платформу з прикладами найкращих практик використання генетичних алгоритмів, що сприяє швидкому освоєнню технологій.

Таким чином, автоматизований синтез політик безпеки з використанням генетичних алгоритмів є ефективним інструментом для підвищення гнучкості та надійності СУІБ. Реалізація запропонованих заходів, таких як автоматизоване генерування політик, моніторинг їх ефективності, електронний документообіг і тестування, сприяє створенню адаптивних і сертифікованих систем безпеки. Подальші дослідження передбачають розробку гібридних ШІ-алгоритмів для синтезу політик і інтеграцію з блокчейн-технологіями для забезпечення прозорості сертифікації. Впровадження таких рішень у навчальні програми сприятиме підготовці фахівців, здатних створювати інноваційні та безпечні IT-системи.

1. Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems (2017).
2. Brown, Tom B., et al. "Language models are few-shot learners." arXiv preprint arXiv:2005.14165 (2020).
3. Devlin, Jacob, et al. "BERT: Pre-training of deep bidirectional transformers for language understanding." arXiv preprint arXiv:1810.04805 (2018).

С.О. Романенко

ШЛЯХИ ПОКРАЩЕННЯ ПРОДУКТИВНОСТІ ХМАРНИХ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ДОПОМОГОЮ ОПТИМІЗАЦІЇ АЛГОРИТМІВ ОБРОБКИ ВЕЛИКИХ ДАНИХ

Сучасні хмарні системи управління інформаційною безпекою (СУІБ) обробляють великі обсяги даних для забезпечення кіберстійкості та відповідності стандартам, що вимагає високої продуктивності. Оптимізація алгоритмів обробки великих даних може значно підвищити ефективність таких систем, зменшуючи затримки та ресурсні витрати. Метою дослідження є розробка шляхів покращення продуктивності хмарних СУІБ шляхом оптимізації алгоритмів обробки великих даних.

Проведено аналіз теоретичних основ обробки великих даних у контексті кібербезпеки, включаючи методи паралельних обчислень, потокової обробки та машинного навчання. Виявлено основні проблеми хмарних СУІБ, такі як низька швидкість аналізу великих масивів даних, високе навантаження на обчислювальні ресурси та складність масштабування в реальному часі. Для вирішення цих проблем запропоновано підхід, який передбачає оптимізацію алгоритмів обробки даних за допомогою технологій Apache Spark, Kafka та легковагових моделей машинного навчання [1].

Запроваджено систему потокової обробки логів безпеки з використанням Apache Kafka, що забезпечує аналіз даних у реальному часі. Розроблено оптимізований алгоритм кластеризації вразливостей на основі машинного навчання, який зменшує час їх виявлення. Для підвищення продуктивності використано розподілені обчислення на базі Apache Spark, що забезпечує масштабування в хмарних середовищах. Впроваджено систему моніторингу продуктивності алгоритмів, яка відстежує затримки та генерує звіти для адміністраторів. Для спрощення управління створено централізовану платформу аналізу даних безпеки, що уникає дублювання інформації. Впроваджено систему зворотного зв'язку, яка дозволяє оптимізувати алгоритми на основі оцінок користувачів [2].

Експеримент проведено на прикладі хмарної СУІБ для моніторингу мережевих атак, де оптимізація алгоритмів скоротила час обробки даних на 13%. Перевагами підходу є підвищення швидкості аналізу, автоматизація рутинних завдань і покращення масштабованості систем. Для забезпечення конфіденційності застосовано шифрування даних і управління доступом через IAM-політики. Впроваджено систему електронного документообігу для координації між командами аналітиків, адміністраторів і аудиторів. Розроблено інструменти для автоматичного тестування продуктивності алгоритмів у хмарних середовищах.

Додатково впроваджено механізм автоматичного кешування результатів аналізу, що знижує навантаження на систему під час пікових запитів. Для навчання фахівців організовано тренінги з використання технологій обробки великих даних, що сприяє підвищенню їхньої кваліфікації. Впроваджено візуальний інтерфейс для управління алгоритмами аналізу безпеки.

Для підвищення ефективності обробки даних застосовано алгоритми стиснення логів безпеки, що зменшують обсяг передачі даних у хмарі. Впроваджено базу знань із шаблонами оптимізованих алгоритмів, що полегшує їх адаптацію до різних СУІБ. Для забезпечення масштабованості інтегровано хмарні платформи з підтримкою еластичних обчислень. Розроблено інструменти автоматичного виявлення аномалій у потоках даних, що підвищують точність аналізу безпеки.

Для підтримки командної роботи створено централізовану систему управління версіями алгоритмів, що синхронізує зміни між хмарними та локальними компонентами. Впроваджено механізм автоматичного тестування алгоритмів перед розгортанням, що знижує ризик помилок. Для спрощення аудиту безпеки розроблено модуль автоматичного генерування звітів, сумісних із ISO/IEC 27001. Організовано вебінари для адміністраторів із використання оптимізованих алгоритмів, що сприяє їх швидкому впровадженню [3].

Додатково впроваджено систему прогнозування пікових навантажень на основі аналізу історичних даних за допомогою алгоритмів машинного навчання. Для забезпечення безперебійної роботи розроблено механізм автоматичного відновлення конфігурацій алгоритмів після збоїв. Впроваджено стандартизовані шаблони для документування процесів аналізу даних, що полегшує сертифікацію. Для інтеграції з зовнішніми системами створено API для обміну аналітичними даними.

Для підвищення адаптивності СУІБ розроблено програмний модуль для автоматичного оновлення алгоритмів відповідно до нових типів загроз. Впроваджено систему оцінки ефективності алгоритмів обробки даних, яка дозволяє оптимізувати їх конфігурацію. Для підтримки аналітиків створено інтерактивну платформу з прикладами найкращих практик обробки великих даних, що сприяє швидкому освоєнню технологій.

Таким чином, оптимізація алгоритмів обробки великих даних є ефективним інструментом для підвищення продуктивності хмарних СУІБ. Реалізація запропонованих заходів, таких як потокова обробка, моніторинг продуктивності, електронний документообіг і тестування алгоритмів, сприяє створенню швидких і масштабованих систем безпеки. Подальші дослідження передбачають розробку ШІ-алгоритмів для адаптивної оптимізації обробки даних та інтеграцію з блокчейн-технологіями для забезпечення прозорості аналізу. Впровадження таких рішень у навчальні програми сприятиме підготовці фахівців, здатних створювати ефективні та безпечні хмарні системи.

1. Richard E. Bellman. Dynamic Programming. - Princeton University Press, 2010. – 392 p.
2. H. Cyber Insurance: A Hard Reset, Howden Broking, https://www.howdengroup.com (2022).
3. https://www.kaggle.com/code/akritiupadhyayks/cyber-attack-detection-with-randomforest/input?select=UNSW_NB15_training-set.csv.

В.В. Цапенко, О.В. Куликівський, С.І. Ковтун, О.В. Пономаренко

ЗАХИСТ ІНФОРМАЦІЇ В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ ДЛЯ МОНІТОРИНГУ ДОВКІЛЛЯ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

Бездротові сенсорні мережі є перспективною технологією для моніторингу стану атмосферного повітря в околі об'єктів енергетики. В роботі розглянуто проблеми забезпечення захисту інформації в таких мережах, проаналізовано основні загрози та вразливості, а також запропоновано методи та засоби захисту з урахуванням специфіки застосування.

Ключові слова: бездротові сенсорні мережі, захист інформації, моніторинг довкілля, об'єкти енергетики, кібербезпека, mesh-зв'язок, Wi-Fi .

Вступ. Для автоматизації процесів моніторингу довкілля необхідно забезпечити надійний обмін інформацією між усіма елементами системи, тобто створити єдину інтегровану мережу сенсорних і виконавчих пристроїв. У багатьох випадках використання традиційних (провідних) комунікаційних рішень є недоцільним через їх високу вартість, складність монтажу, а також неможливість ефективного використання в умовах мобільних або мініатюрних об'єктів.

Бездротові сенсорні мережі (БСМ) є інноваційною технологією, що стрімко розвивається та знаходить широке застосування у різних сферах, зокрема в системах моніторингу довкілля [1]. Завдяки здатності забезпечувати безперервний збір, передачу та опрацювання даних у реальному часі, БСМ дедалі частіше використовуються для оцінки рівня забруднення атмосферного повітря [2]. Особливо актуальним є впровадження БСМ в околі об'єктів енергетики, де зосереджені значні джерела викидів шкідливих речовин [3]. Такі системи дають змогу оперативно виявляти перевищення допустимих концентрацій забруднюючих речовин (наприклад, діоксиду сірки, оксидів азоту, твердих частинок тощо), що дозволяє своєчасно реагувати на потенційні екологічні загрози та приймати обґрунтовані рішення щодо зменшення негативного впливу на навколишнє середовище. Крім того, використання БСМ сприяє підвищенню ефективності управління екологічною безпекою, зокрема за рахунок простоти розгортання мереж, низького енергоспоживання сенсорних вузлів та можливості створення адаптивних систем контролю. У цьому контексті БСМ набувають особливої популярності завдяки своїй гнучкості, масштабованості та енергоефективності. Вони дозволяють швидко розгортати системи моніторингу навіть у складнодоступних або тимчасових локаціях, що є критичним, наприклад, у зонах стихійних лих або в районах, прилеглих до об'єктів енергетичної інфраструктури.

Водночас, відкритість бездротового середовища зв'язку робить БСМ уразливими до різноманітних загроз безпеці – зокрема, до несанкціонованого доступу, перехоплення даних, спотворення або блокування переданої інформації [1]. Це створює серйозні ризики, особливо у випадках використання БСМ для моніторингу критично важливих об'єктів. Розроблення й впровадження ефективних методів криптографічного захисту, аутентифікації пристроїв, а також протоколів безпечного обміну інформацією є важливим напрямом сучасних досліджень у сфері інформаційної безпеки БСМ.

Аналіз загроз та вразливостей бездротових сенсорних мереж при моніторингу довкілля об'єктів енергетики. Бездротові сенсорні мережі, що застосовуються для моніторингу стану атмосферного повітря (АП) навколо об'єктів енергетики (див. рис. 1), функціонують у відкритому середовищі та є вразливими до широкого спектру загроз [1].

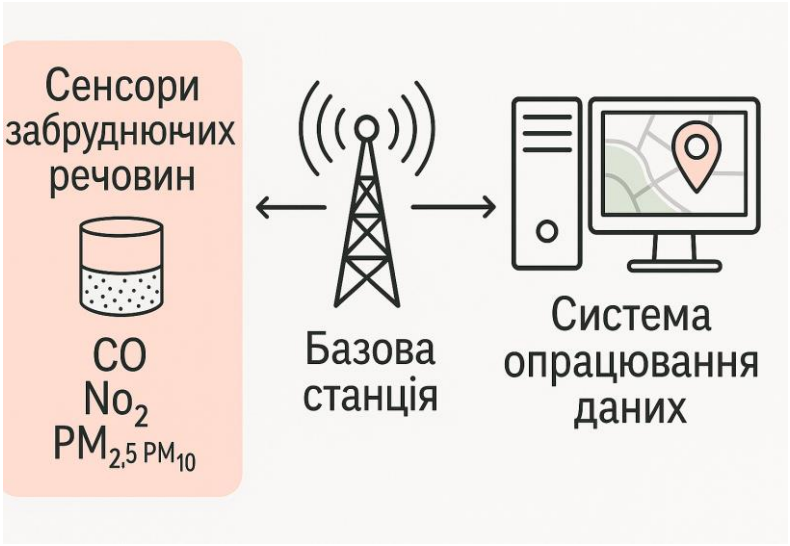


Рисунок 1 – Приклад архітектури БСМ моніторингу АП

Їх уразливість посилюється мобільністю, обмеженою обчислювальною потужністю, автономним живленням сенсорів та відсутністю централізованого захисту [4]. В таблиці 1 представлено співвідношення між основними вразливостями БСМ та відповідними засобами захисту інформації.

Таблиця 1 – Вразливості та способи захисту БСМ

Вразливості БСМ	Засоби захисту
Обмежені ресурси	Оптимізація алгоритмів захисту.
	Використання простих та ефективних методів шифрування та аутентифікації.
Бездротове середовище	Шифрування даних для забезпечення конфіденційності.
	Використання методів аутентифікації для перевірки достовірності даних.
Відсутність сталої інфраструктури	Централізоване управління безпекою для покращення моніторингу та контролю.
	Резервування даних і мережеві протоколи для забезпечення стійкості.
Високі вимоги до точності даних	Контроль цілісності даних, використання методів виявлення вторгнень (IDS).
	Використання методів корекції помилок для забезпечення точності та надійності даних.

Популярний протокол, який використовують для роботи БСМ – це стандарт IEEE 802.15.4 і специфікація ZigBee. Цей стандарт забезпечує чотири основних моделі безпеки: управління доступом, цілісність повідомлень, конфіденційність повідомлень і захист відтворення [5]. Застосування стандарту IEEE 802.15.4 є одним із основних протоколів, який широко використовується в системах моніторингу довкілля. Він підтримує базові механізми захисту, такі як шифрування даних та аутентифікацію, що дають певний рівень захисту інформації [5]. Однак ці механізми часто виявляються недостатніми для забезпечення необхідного рівня безпеки в критичних системах, де важливі не тільки конфіденційність, але й цілісність та достовірність даних. У контексті моніторингу довкілля, особливо в умовах потенційних загроз маніпулювання даними або несанкціонованого доступу до інформації, необхідно вживати додаткових заходів захисту. Такі заходи повинні забезпечувати високий рівень надійності передачі даних, їх аутентичність і цілісність, що є критично важливим для прийняття обґрунтованих рішень з охорони навколишнього середовища та реагування на екологічні загрози. Проаналізувавши найвідоміші та доступні в Україні мережі для бездротової передачі даних, можна зробити висновок, що найбільш доцільним вибором мережі буде реалізований на базі технології Wi-Fi mesh-зв’язок — за критеріями надійності, швидкості та обсягами передавання інформації [6, 7]. Mesh-зв'язок має ряд переваг у контексті захисту інформації в бездротових сенсорних мережах, особливо з точки зору підвищення надійності, стійкості до атак та забезпечення цілісності даних (Таблиця 2).

Таблиця 2 – Переваги використання mesh-зв’язку

Перевага	Опис
Підвищена стійкість до атак типу DoS	Відмова або атака на окремий вузол не призводить до зупинки мережі — трафік перенаправляється через інші маршрути.
Зменшення ризику втрати даних	Альтернативні шляхи передавання підвищують надійність передачі інформації навіть при перешкодах.
Динамічна маршрутизація для обходу скомпрометованих вузлів	Мережа автоматично виключає підозрілі вузли з маршруту, зберігаючи цілісність даних.
Відсутність "єдиної точки відмови"	Відсутність центрального вузла мінімізує ризик повного виведення мережі з ладу.
Розосереджене виявлення вторгнень (Distributed IDS)	Кожен вузол може виявляти аномальну активність, підтримуючи розподілений моніторинг безпеки.
Підвищення конфіденційності через фрагментацію трафіку	Дані передаються по різних маршрутах, що ускладнює їх повне перехоплення.
Гнучкість та адаптивність до змін середовища	Мережа автоматично адаптується до змін або відмов, забезпечуючи безперервність зв'язку.

Враховуючи ці переваги, mesh-зв'язок є ефективним рішенням для забезпечення захисту інформації в БСМ, що використовуються для моніторингу довкілля об'єктів енергетики. Реалізація системи контролю забруднення повітря на базі mesh-мережі дозволить значно підвищити надійність та стійкість системи в цілому [7].

Висновки. Захист інформації є критично важливою складовою під час розгортання та експлуатації БСМ, особливо в контексті моніторингу стану атмосферного повітря поблизу об’єктів енергетики. Незважаючи на впровадження базових механізмів безпеки, БСМ залишаються вразливими до різноманітних кіберзагроз, що створює ризики для достовірності, конфіденційності та доступності екологічної інформації. У роботі проаналізовано основні загрози та вразливості, властиві БСМ, а також окреслено ефективні методи інформаційного захисту з урахуванням обмежених ресурсів сенсорних пристроїв та обґрунтовано доцільність використання mesh-зв'язку для підвищення надійності та стійкості системи контролю забруднення повітря, а також покращений захист даних завдяки розподіленій структурі маршрутизації. Подальші дослідження та розробки необхідні для створення ефективних методів захисту, які враховують обмежені ресурси сенсорних вузлів, особливості бездротового зв'язку та специфічні вимоги до точності та надійності даних у системах моніторингу довкілля.

1. Жуковський, П. С. (2021). Аналіз уразливостей бездротових сенсорних мереж. Сучасний захист інформації, (4), 59-63.
2. Жураковський, Б. Ю., Пархомей, І. Р., & Дружинін, В. А. (2018). Обробка інформації в сенсорних мережах. Адаптивні системи автоматичного управління, (1), 42-57.
3. Мокін, В. Б., Собко, Б. Ю., Дратований, М. В., Крижановський, Є. М., & Горячев, Г. В. (2017). Створення інформаційної системи моніторингу забруднення атмосферного повітря міста на основі технології «Інтернет речей». Вісник Вінницького політехнічного інституту, (3), 49-58.
4. Щелконогов, О. О. (2012). Забезпечення захисту бездротової системи контролю розкриття апаратури. Львів, Видавництво Львівської політехніки, 192-197.
5. Туранська, О. С., & Лисенко, О. І. (2017). Захист інформації у безпроводових сенсорних мережах. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ».
6. Мостовий, В. В., Понедільник, О. В., & Пастушок, І. М. (2018). Захист безпровідних сенсорних мереж від атак. Збірник тез доповідей VII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, 2, 130-130.
7. Kovtun, S., Ponomarenko, O., & Nazarenko, O. (2023). Quality of the information flow management at stochastic energy consumption conditions. System Research in Energy, (3 (74)), 78-84.

Н.В. Заїка, І.В. Мартинюк, М.Ю. Комаров, О.М. Джигун

УДОСКОНАЛЕННЯ МЕТОДУ МОНІТОРИНГУ З ВИЯВЛЕННЯМ КРИТИЧНИХ ЗБОЇВ У РОБОТІ ВЕБ-РЕСУРСІВ ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ

Наразі ІТ-інфраструктури бізнесу та особливо державних установ є одними з головних споживачів інформаційних технологій. Вони належать до критичних систем, адже їхні збої можуть призводити до серйозних фінансових і репутаційних втрат. Сучасний розвиток ІТ зосереджений на інтеграції різних програмних рішень в єдину інфраструктуру та на оновленні систем під потреби інноваційного управління. При цьому ІТ-інфраструктури повинні забезпечувати стабільну роботу критичних систем і можливість їх реінжинірингу в реальному часі, з мінімальними витратами та без втрати ключових показників: надійності, безпеки, масштабованості, ефективності, керованості й гарантії якості обробки даних [1—3].

Важливим компонентом забезпечення стійкої роботи ІТ-інфраструктури є система моніторингу, яка дозволяє виявляти й оперативно реагувати на технічні проблеми. Одним із популярних інструментів у цій сфері є Zabbix — система моніторингу з відкритим кодом, яка надає повний спектр функцій для спостереження за станом мереж, серверів, додатків і сервісів. Zabbix виступає як ІТ-сервіс, що дозволяє автоматизовано відстежувати працездатність інфраструктури, зменшуючи час простою і підвищуючи загальну ефективність та безпеку систем [4]. Водночас, науково-методичні засади інформаційного управління саме у сфері критичних ІТ-сервісів і процесів, включаючи моніторинг за допомогою таких систем як Zabbix, потребують подальшого розвитку та глибоких досліджень.

У цьому контексті розробка та впровадження ефективних засобів моніторингу та кіберзахисту набуває особливої актуальності. Одним із ключових підходів є організація постійного моніторингу стану інформаційних ресурсів критичних об’єктів. Для цього використовуються такі методи, як:

• Моніторинг доступності, зокрема перевірка статус-кодів HTTP для виявлення недоступних або нестабільних веб-ресурсів;

• Аналіз логів веб-сервера, що дозволяє виявляти підозрілу активність, наприклад, повторні спроби авторизації або несанкціоновані запити;

• Моніторинг продуктивності, з акцентом на швидкість завантаження сторінок та реагування системи;

• Інтеграція спеціалізованих сервісів моніторингу, таких як Zabbix чи Prometheus, які забезпечують автоматичне відстеження показників систем у реальному часі, сповіщення про відхилення від норми та підтримку високої доступності сервісів.

Система Zabbix, зокрема, дозволяє централізовано контролювати як апаратні, так і програмні компоненти інфраструктури, що робить її ефективним інструментом для забезпечення ІТ-послуг на рівні критичних об’єктів. Вона забезпечує збір і візуалізацію даних, історію подій та можливість гнучкого налаштування політик сповіщення, що є важливим у системах раннього реагування.

У межах підвищення рівня кіберзахисту веб-ресурсів запропоновано метод розширеного моніторингу, який дозволяє не лише відстежувати доступність і продуктивність веб-сайту, а й виявляти внутрішні помилки вебресурсу. Такий підхід сприяє своєчасному виявленню критичних збоїв, які потенційно можуть бути використані зловмисниками або призвести до дестабілізації роботи ресурсу.

Подальші шляхи та рекомендації з підвищення ефективності управління критичною інформаційною інфраструктурою пов’язано із розробкою адаптивної архітектури під задачі [5—6].

На етапі проектування важливо враховувати гнучкість та масштабованість ІТ-інфраструктури. Застосування принципів архітектури з низьким рівнем зв'язності дозволяє легко адаптувати систему до змін або оновлень, що особливо актуально для інфраструктур, які обслуговують критичні сервіси (наприклад, енергетика, транспорт, охорона здоров’я).

Підвищення оперативності та достовірності обміну інформацією в ієрархічній системі управління [7]. Це може бути досягнуто через централізовану платформу моніторингу, доповнену захищеними каналами зв’язку, резервними вузлами та відмовостійкими протоколами передачі інформації.

Zabbix може виступати базовим рівнем, який через API може бути підключений до зовнішніх систем (наприклад, графічних платформ, SIEM, систем керування інцидентами). Інформація, зібрана моніторинговими засобами (наприклад, зі скриптами), повинна не лише фіксувати проблеми, але й ініціювати автоматизовані сценарії реагування (наприклад, перезапуск сервісів, блокування доступу та повідомлення технічної групи або керівництва). Це значно скорочує час реагування і знижує ризик ескалації інциденту.

Critical Security Controls — це набір кращих практик і рекомендацій, розроблених Центром безпеки Інтернету (Center for Internet Security, CIS), що мають на меті покращення кібербезпеки організацій шляхом ефективного управління ризиками та запобігання найбільш поширеним кіберзагрозам. Концепція CIS Controls складається з набору конкретних заходів і методів, які допомагають організаціям зміцнити свою кіберзахищеність, знижуючи ймовірність успішної кібератаки. Загалом це 18 основних категорій заходів, які покривають різні аспекти кібербезпеки [8].

Впровадження концепції CIS Controls забезпечує системний підхід до побудови захисту організацій: здійснюється ідентифікація активів, управління вразливостями, контроль привілейованого доступу, безперервний моніторинг, захист даних, а також підвищення обізнаності персоналу щодо актуальних кіберзагроз.

Впровадження CIS Controls як системного підходу до безпеки дозволяє організаціям:

- ідентифікувати активи і вразливості;
- визначати пріоритети захисту;
- застосовувати контроль доступу;
- реалізовувати безперервний моніторинг;
- забезпечувати навчання персоналу;
- стандартизувати заходи кіберзахисту.

Для оцінювання стану мережевої безпеки застосовують сканери вразливостей, зокрема Nessus і OpenVAS [9]. Вони дозволяють швидко виявляти вразливості, проводити аутентифіковані/неаутентифіковані перевірки та адаптувати захисні заходи до реальних умов.

Висновки

Забезпечення надійної роботи веб-ресурсів та компонентів критичної інформаційної інфраструктури вимагає впровадження ефективних систем моніторингу, зокрема шляхом інтеграції платформи Zabbix з автоматизованими засобами тестування. Такий підхід дає змогу своєчасно виявляти критичні помилки та здійснювати проактивне реагування на загрози.

Застосування контрольних списків (Checklists) у сфері кібербезпеки дозволяє систематизувати процеси перевірки, оцінювання ризиків, відповідності політикам безпеки, а також підвищити ефективність моніторингу стану захищеності інформаційних систем.

Формування архітектури критичної інформаційної інфраструктури має ґрунтуватися на методах математичного моделювання, штучного інтелекту та системного аналізу. Це дозволяє розробляти оптимальні структури із врахуванням специфіки завдань, мінімізуючи при цьому складність застосовуваного математичного апарату.

Одним із ключових напрямів удосконалення кіберзахисту є підвищення оперативності передачі критичної інформації та забезпечення її достовірності. Це досягається шляхом використання єдиної системи проектування та оптимізації структури критичної інформаційної інфраструктури.

1. Комаров. М.Ю., Гончар С.Ф., Дімітрієва Д.О. Дослідження проблеми кіберживучості об’єктів критичної інформаційної інфраструктури. Nuclear and Radiation Safety. 2021. С. 59-65.
2. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць ХНУПС. 2016. № 4. С. 168-172.
3. Мурасов Р.К., Курцеітов Т.Л., Мельник Ю.В. Імовірнісний метод прогнозування надзвичайних подій на потенційно небезпечних об’єктів критичної інфраструктури. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. Т.2, №44, С.60-64.
4. Zabbix. URL: www.Zabbix.com (дата звернення 01.05.2025).
5. Поночовний Ю.Л., Харченко В.С. Методологія забезпечення гарантоздатності інформаційно-керуючих систем з використанням багатоцільових стратегій обслуговування. Radioelectronic and Computer Systems. 2020. № 3. С. 43–58.
6. Singer, P. W., Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. 2014. 306 с.
7. Теорія мотивації захисту. URL https://open.ncl.ac.uk/theories/10/protection-motivation-theory (дата звернення 01.05.2025).
8. Critical Security Controls (CIS Controls). URL: www.cisecurity.org (дата звернення 01.05.2025).
9. OpenVAS. URL:www.openvas.org (дата звернення 01.05.2025).

O.M. Dzhyhun

ELECTRIC POWER INDUSTY OF UKRAINE DURING MILITARY AGGRESSION.

The current energy situation in Ukraine, shaped by various external factors, requires not only adaptation, but also a strategic rethinking of the functioning of enterprises in the industry. The opening of the possibility of exporting electricity to EU countries opens up new prospects for the Ukrainian energy sector.

Ukraine's energy sector has been at war since 2014. At the same time, the Ukrainian energy sector has faced a list of new threatening challenges, such as nuclear terrorism with the seizure of the Zaporizhzhia NPP, numerous damages to critical infrastructure - electricity and gas networks, and a more critical decrease in the level of payments in the energy system. But despite the hostilities throughout the country, there is a decision to continue synchronizing Ukraine's energy system with the energy system of Continental Europe.

The challenges that Ukraine has faced in connection with full-scale military operations on the territory of our country are particularly tangible and serious for the energy sector. This applies to both the prompt restoration of infrastructure facilities from the destruction caused by military actions, and ensuring the passage of the autumn-winter heating period of 2022/2023, which is expected to be the most difficult for the entire European continent, as well as the strategic restoration and renewal of the energy sector in the context of Ukraine's acquisition of the status of a candidate for accession to the EU. It is expected that it is not possible to find the optimal answer to every challenge and not the first time. However, it is important to correctly identify and record strategic priorities, as well as their financial and economic capabilities and sources, so that the development of energy regulatory regulation is as predictable and transparent as possible for all energy market participants.

Since the beginning of the full-scale invasion in Ukraine, 42% of the generating capacities of the power system have been destroyed and occupied. The largest occupied facility is the Zaporizhzhia NPP (6 GW), and the most significant losses have been suffered by heat generation, in the structure of which 87% of coal-fired CHP plants are irretrievably lost. 2.3 thousand MW of hydropower capacity has been destroyed and damaged [1-2]. The non-use of nuclear energy as a weapon and means of terrorist attacks is regulated by the Geneva Convention, so the enemy's main target was thermal power plants and hydroelectric facilities.

Unfortunately, the «green» generation suffered damage. 3.9 thousand MW of wind and solar power plants were destroyed and occupied. Renewable energy sources, wind farms are less damaged than solar power plants, and the latter are more vulnerable to small arms fire and missiles (due to the large area of construction and the fragility of photovoltaic modules). The capacity of «green» generation was also destroyed. Of the 6.23 GW of industrial solar power plants put into operation, 3.72 GW (60% of solar power plants) are located in the temporarily occupied territories, 1.12 GW in the frontline regions on the TOT are damaged. In total, they can supply up to 2.2 GWh to the power grid during peak hours, and up to 502 MWh during the day in winter.

In Ukraine, the total installed capacity of wind farms is 1.9 GW. Large wind farms in Ukraine are concentrated in Zaporizhia, Mykolaiv, Odessa and Lviv regions. Due to the military aggression of Russia, more than 2/3 of wind turbines have been stopped. Currently, 1162.5 MW of installed capacity is not working, 372.5 MW remain in operation, which are concentrated mainly in the Odessa and Lviv regions. According to the Ukrainian Wind Energy Association, 71% of generation is located in the temporarily occupied territories

Thus, in the Kharkiv region, all ground-based solar power plants (28.4 MW of installed capacity) and most industrial rooftop solar power plants (6.3 MW damaged and destroyed, and only 1.0 continues to operate) have been destroyed, and up to 1.2 GW of solar power plants are located in TOT (temporarily occupied territories).

If we analyze the damage zones territorially, the greatest losses were suffered by the generating capacities of the regions close to the combat zone, which before the shelling of the power system were energy surplus, but now have an electricity deficit. There is also destruction of large generating facilities in the deep rear, in particular, in the Carpathian region and Podillia.

The shelling of the energy system led to damage to the hydropower sector. Thus, out of the 6.64 GW of hydroelectric and PSPP capacities, 351 MW were destroyed, and the supply to the network is at the level of 2.17 GWh, provided that the river water level is high. Currently, this indicator is at 1.2 GWh due to the autumn low water period (lowest river levels) and dry (low water) summer.

Elements of the main power grids and substations of NPC Ukrenergo are undergoing constant destruction. Today, the power system operates 7,880 MW of installed nuclear generation capacity (Southern Ukrainian, Rivne and Khmelnytskyi NPPs). The largest in Europe and one of the 10 largest nuclear power plants in the world, Zaporizhia NPP (6 GW of installed capacity), is under temporary occupation, although its energy supply is carried out by overhead lines from controlled territories.

Ukraine's energy sector needs strategic rethinking and adaptation to new conditions, which includes adaptation to European standards, investment in innovative technologies, active participation in international projects, and development of renewable energy. Due to the devastating damage to 22.58 GW of installed thermal generating capacity (the vast majority of which is coal-fired) on TOT, the consumption of hard coal as a source of electricity generation sharply decreased. The energy industry has a significant number of critical assets that need to be managed effectively, including scheduling and timely maintenance and repairs to reduce unplanned downtime and increase equipment availability. The upheaval caused by the war in Ukraine showed how automation of asset management processes helps to quickly respond to accidents and ensure the stability of the energy system.

In the energy sector, a number of regulatory changes have been introduced since February 24, 2022, designed to stabilize the industry and address critical issues.

Main scenarios for the development of the energy system in the coming years [3].:

1. If there is no military factor (without shelling of energy system elements),

in the next 5-7 years Ukraine will have a deficit of electricity in summer and winter, which imports will not be able to cover.

2. Optimistic, in which investors return to the energy sector

3. Continued destruction of Ukrenergo NPP substations and open switchgear of NPPs by massive strikes: electricity shortages will increase, albeit temporarily

After the war, reconstruction and modernization will become integral parts of the energy sector, and in this context, innovation, effective management, technological renewal, and active work in the field of renewable energy sources become key factors [4]. Realizing the global nature of energy security, ensuring the competitiveness of Ukrainian energy companies, it is advisable to introduce innovations in this area by developing strategic approaches. One of the key aspects of responding to this situation is investing in research and development to create and implement new technologies and methods aimed at increasing productivity and ensuring competitiveness in the market.

In the energy sector of Ukraine, after the period of war realities, it is important to focus on building our own competitive advantages to ensure sustainability and further development. The energy sector of Ukraine is a significant component of the national economy, characterized by a number of competitive advantages that determine its potential importance at the regional and global levels. First of all, it is worth noting the advantageous geographical location of the country, which ensures its unique position. Ukraine has all the necessary resources in its bowels to meet its own energy needs and has the potential to export them to other countries. This opens up prospects for the development of transport infrastructure and promotes the creation of strategic alliances in the energy sector, contributing to the expansion of sales markets for enterprises.

1. Н. Гутаревич Енергетика під час війни в Україні: які зміни в регулівнні https://jurliga.ligazakon.net/aktualno/12602_energetika-pd-chas-vyni-v-ukran-yak-zmni-v-regulyuvann.
2. Енергетика під час війни: як системи управління активами надають ефективні рішення для енергетики https://www.epravda.com.ua/publications/2024/01/29/709143/.
3. Ігнатьєв С. Енергетична система України: стан на кінець 2024 року та сценарії на 2025. https://oil-gas.com.ua/statti/enerhetychna_systema_ukrainy_stan_na_kinets_2024_roku_ta_stsenarii_na_2025.
4. С. Нєсвєтова, К. Сорока Стратегічні підходи забезпечення конкурентних переваг підприємств енергетичної галузі України. https://ir.kneu.edu.ua/server/api/core/bitstreams/78b0e23a-7bc7-42a1-a5f2-e0ca1a6047de/content.

Г.П. Костенко

ВТОРИННІ БАТАРЕЇ ЕЛЕКТРОТРАНСПОРТУ ЯК АКТИВИ ІЗ ДИНАМІЧНИМИ РИЗИКАМИ: ПІДХІД ДО МОДЕЛЮВАННЯ І УПРАВЛІННЯ У СИСТЕМАХ ПРИЙНЯТТЯ РІШЕНЬ

Стрімке зростання кількості літій-іонних батарей, що вивільняються після завершення терміну служби в електротранспорті, породжує як нові можливості, так і нові загрози для енергетичної системи. З одного боку, вторинні батареї (second-lifebatteries, SLB) є джерелом гнучкості, балансу та резерву. З іншого — вони несуть підвищені ризики, пов'язані з деградацією, невизначеністю технічного стану та потенційними аномаліями в роботі. У контексті зростання ролі децентралізованих джерел енергії, поширення мікромереж і розвитку цифрових інфраструктур, SLB мають розглядатися як активи із динамічним ризиком, що вимагає включення до систем постійного моніторингу та автоматизованого прийняття рішень.

Поведінка SLB у другому життєвому циклі є значно менш передбачуваною порівняно з новими акумуляторами. Це зумовлено множинністю змінних, які не завжди можливо відтворити або верифікувати з технічної документації. Наприклад, ступінь деградації елементів у межах одного модуля може суттєво відрізнятись, залежно від температурного режиму експлуатації, типу транспортного засобу, профілю навантаження або попередніх відмов, які не були зафіксовані. Це породжує асиметричні ризики — тобто ймовірність відмови одного з компонентів у «загалом справному» блоці зростає з часом експоненційно.

Крім того, SLB часто інтегруються в низьковольтні та середньовольтні системи, що мають неоднорідні топології, слабкий зворотній зв'язок і високий ступінь залежності від локальних умов. У таких умовах навіть короткочасні відхилення параметрів батареї можуть призводити до каскадних збоїв в мікромережі або до втрати функції резервування. Це особливо критично в умовах енергетичної дестабілізації — наприклад, під час пікових навантажень, бойових дій або аварійних відключень централізованого живлення.

З погляду інформаційної безпеки, SLB з цифровими модулями управління (BMS, CAN-шини, хмарні сервіси) перетворюються на елементи кіберфізичної системи, які можна потенційно атакувати або використовувати як точку доступу. Наявність різнорідного програмного забезпечення, відсутність уніфікованих стандартів безпеки для SLB і обмежена підтримка з боку виробників посилюють ризики втручання в ланцюг керування енергосистемою через батарейні блоки.

Окремо варто згадати ризики пов'язані з недоступністю чи втратою даних про попередній життєвий цикл батареї. У багатьох випадках оператор отримує модуль без повної історії навантажень або технічного обслуговування. Це суттєво ускладнює класифікацію ризиків і вимагає запровадження адаптивних систем діагностики, які можуть діяти в умовах неповної або суперечливої інформації.

Таким чином, SLB — це активи з високою динамікою технічного та інформаційного стану, і їх використання можливе лише за умови постійного спостереження, аналізу контексту, а також швидкої адаптації логіки управління до змін параметрів. Успішна інтеграція SLB в енергетичні системи нового покоління неможлива без врахування цих ризиків і переходу від концепції «пасивного використання» до моделі «розумного активу», який взаємодіє з мережею як учасник динамічного енергетичного середовища.

З огляду на високий ступінь невизначеності технічного стану вторинних батарей, ефективне управління пов'язаними з ними ризиками потребує поєднання декількох моделей у рамках єдиної системи прийняття рішень [1-5]. Запропонований раніше підхід до моделювання повторного використання SLB включає низку взаємопов'язаних моделей — від оцінки деградації до просторової оптимізації [2,5]. Однак окремий інтерес становить здатність цих моделей виявляти, оцінювати та знижувати ризики, що виникають при інтеграції SLB в енергосистему.

Кожна модель виконує специфічну функцію в системі управління ризиками. Так, модель деградації дозволяє ідентифікувати критичні параметри, які можуть вказувати на наближення відмови. Модель залишкового ресурсу (RUL) переводить ризик у часову площину, надаючи можливість проактивного планування. Економічна модель, своєю чергою, враховує можливі втрати внаслідок технічних збоїв. Просторова модель враховує зовнішні ризики — географічні, інфраструктурні, контекстуальні. Оптимізаційна модель дозволяє уникати концентрації ризиків у вразливих точках системи, тоді як модель планування заміни забезпечує своєчасне виведення батарей з експлуатації до моменту їх критичного зносу.

Узагальнення функцій кожної моделі в контексті ризик-менеджменту наведено в табл. 1.

Таблиця 1 - Моделі як інструменти управління ризиками використання вторинних батарей електротранспорту в енергетичних системах

Назва моделі	Ризики, на які впливає модель	Функція в управлінні ризиком
Модель деградації	Втрата функціональності через деградацію, приховані дефекти	Оцінка технічного стану; виявлення аномалій
Модель залишкового ресурсу (RUL)	Непередбачуваний вихід з ладу, короткий залишковий строк служби	Прогнозування безпечного періоду експлуатації

Прродовження таблиці 1

Модель економічної доцільності	Неефективне використання ресурсів, збитки від невдалих інвестицій	Врахування можливих втрат у процесі ухвалення рішень
Оптимізаційна модель розподілу	Накопичення деградованих батарей у критичних вузлах системи	Зменшення системного ризику через оптимальний розподіл
Просторова модель	Фізична вразливість інфраструктури, географічні загрози	Урахування локальних умов у стратегії впровадження
Модель планування заміни	Раптова відмова без резерву для заміни, аварійна ситуація	Своєчасне виведення з експлуатації до критичної точки

Особливість SLB полягає в тому, що їх параметри змінюються не лише поступово (через природну деградацію), а й різко — у відповідь на зовнішні чинники, некоректне управління або критичні стани енергосистеми. Це створює додаткове навантаження на операторів, знижує передбачуваність резервів і вимагає нових методів технічного аналізу. Крім того, SLB як елемент складної енергетичної архітектури, що взаємодіє з мережею в реальному часі, може стати вразливою точкою для кіберзагроз. У зв'язку з цим виникає необхідність у побудові підходу, що поєднує фізичний моніторинг, аналіз ризиків, прогнозування відмов і автоматизовану реакцію на зміни стану.

Запропонований підхід включає кілька рівнів. На базовому рівні формується цифровий профіль батареї — на основі історичних даних, індексу деградації та інформації з BMS (BatteryManagementSystem). Індекс деградації, який враховує календарне, циклічне та стохастичне старіння, дозволяє не лише оцінювати залишковий ресурс, а й виявляти потенційно критичні зони наперед. Цей індекс інтегрується в модель моніторингу, яка відстежує зміни ключових параметрів (SOH, внутрішній опір, температура, швидкість заряду/розряду) в режимі реального часу.

На другому рівні реалізується динамічна модель ризику — з використанням байєсівського аналізу або нечіткої логіки для оцінки ймовірності відмови залежно від зміни кількох факторів одночасно. На третьому рівні функціонує механізм виявлення аномалій — як за пороговими сценаріями (перевищення температури, падіння напруги, різкі коливання ємності), так і за допомогою методів штучного інтелекту (наприклад, рекурентні нейромережі для ідентифікації відхилень від нормальної динаміки).

Реалізація цих функцій передбачає інтеграцію SLB до SCADA або EMS-рішень на рівні локальних і регіональних систем управління. У разі виявлення критичних змін або ризику відмови, система може автоматично виводити батарею з режиму активної роботи, переключати її на інший режим (наприклад, обмеження потужності) або видавати сигнал на рівень диспетчерського втручання. У перспективі — реалізація «адаптивних сценаріїв експлуатації» SLB з урахуванням ризику в реальному часі.

Очікуваним результатом впровадження такого підходу є підвищення технічної надійності енергосистем з участю SLB, зменшення кількості аварійних ситуацій, стабілізація резервного живлення в мікромережах, а також зниження вразливості до кіберінцидентів через розмежування зон відповідальності й запровадження адаптивної логіки реагування. У довгостроковій перспективі це може лягти в основу стандартів безпечного використання SLB в критичній інфраструктурі.

Вторинні батареї мають розглядатися не лише як ресурс повторної цінності, а як складна динамічна одиниця, що потребує спеціалізованих підходів до прогнозування, діагностики та безпечної інтеграції. Інтеграція моделей моніторингу, оцінки ризику та реагування в автоматизовані системи управління створює можливості для використання SLB навіть у тих застосуваннях, де раніше це вважалося неприйнятним через підвищену відповідальність і вимоги до надійності. Це відкриває новий напрям в управлінні активами енергосистеми — динамічний, цифрово контрольований, адаптивний до змін середовища та поведінки самих активів.

Таким чином, ієрархія моделей формуєбагаторівневу систему управління, щоохоплює не лишетехнічний, а й економічний та просторовийвимірризику. Така структура дозволяєформуватикомплексні правила реагування на зміну стану SLB, враховуючи не лишевнутрішніпараметри батарей, а й контекст їхексплуатації. Це, у свою чергу, є передумовою для створенняадаптивних, кібербезпечних систем моніторингу і управління, здатнихефективноінтегрувати SLB у складніенергетичніархітектури та підвищуватистійкістьсистеми в умовахневизначеності та зростаючихзагроз.

1. Kostenko, G., & Zaporozhets, A. (2024). World experience of legislative regulation for lithium-ion electric vehicle batteries considering their second-life application in power sector. System Research in Energy, 2(77), 97–114. https://doi.org/10.15407/srenergy2024.02.097.
2. Костенко, Г., &Запорожець, А. (2024). Інтегральний показник деградації вторинних батарей електромобілів в системах зберігання енергії: урахування календарного та циклічного старіння. Системні дослідження в енергетиці, (2а (78), 31-33. Вилучено із https://systemre.org/index.php/journal/article/view/848.

3. Kostenko, G. (2024). Accounting Calendar and Cyclic Ageing Factors In Diagnostic And Prognostic Models Of Second-Life EV Batteries Application In Energy Storage Systems. System Research in Energy, 3(79), 21–34. https://doi.org/10.15407/srenergy2024.03.021.
4. Kostenko, G., & Zaporozhets, A. (2024). Transition from Electric Vehicles to Energy Storage: Review on Targeted Lithium-Ion Battery Diagnostics. Energies, 17(20), 5132. https://doi.org/10.3390/en17205132.
5. Костенко, Г. (2025). Кластерний підхід до використання вторинних батарей електротранспорту для надійного та сталого резервного живлення в енергосистемах. Системні дослідження в енергетиці, (1 (81), 40-60. https://doi.org/10.15407/srenergy2025.01.040.

С.Є. Саух

ОЦІНЮВАННЯ РЕЗИЛЬЄНТНОСТІ ОБ'ЄДНАНОЇ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ, ЯКА ФУНКЦІОНУЄ В УМОВАХ ТЕРОРИСТИЧНИХ АТАК

Трирічне функціонування Об'єднаної енергосистеми України (ОЕС України) в умовах російських масованих ракетно-дронових атак є предметом постійної уваги дослідників, які періодично оприлюднюють аналітичні звіти з оцінками поточного стану енергосистеми. Такі аналітичні дослідження не дозволяють сформувати уявлення про перспективи функціонування енергосистеми та оцінити її резильєнтність на майбутніх періодах тривалістю рік та більше.

Мета представленого дослідження полягає у розробці математичної моделі ОЕС України, придатної для короткострокового прогнозування її розвитку в умовах систематичних масованих ракетно-дронових атак. Модель призначена для оцінювання резильєнтностіОЕС України за різних сценарних умов її захисту, руйнування та відновлення з урахуванням наявних резервних механізмів та ресурсів.

Розглянемо рівняння динаміки енергетичних об'єктів, придатних для використання. Множина F_t генеруючих енергоблоків доступних для використання на поточний період часу t визначається множиною F_{t-1} генеруючих енергоблоків, які були доступними для використання в попередній період часу $t-1$, а також множинами раніше пошкоджених генеруючих енергоблоків $dF_{t-TL,LD}$, $dF_{t-TM,MD}$ та $dF_{t-TS,SD}$, довготривалий, середній та короткотривалий ремонти яких тривалістю TL, TM, TS, відповідно, були завершені на початок поточного періоду t, за винятком множин генеруючих енергоблоків $dF_{t,LD}$, $dF_{t,MD}$, $dF_{t,SD}$, які були уражені в період часу t та отримали, відповідно, великі, середні та дрібні пошкодження, тобто маємо динамічне рівняння

$$F_t = \left(F_{t-1} \cup dF_{t-TL,LD} \cup dF_{t-TM,MD} \cup dF_{t-TS,SD}\right) \setminus \left(dF_{t,LD} \cup dF_{t,MD} \cup dF_{t,SD}\right).$$

Для систем зберігання енергії та генеруючих установок, що використовують відновлювані джерела енергії, маємо рівняння, відповідно,

$$S_t = \left(S_{t-1} \cup dS_{t-TL,LD} \cup dS_{t-TM,MD} \cup dS_{t-TS,SD}\right) \setminus \left(dS_{t,LD} \cup dS_{t,MD} \cup dS_{t,SD}\right),$$

$$R_t = \left(R_{t-1} \cup dR_{t-TL,LD} \cup dR_{t-TM,MD} \cup dR_{t-TS,SD}\right) \setminus \left(dR_{t,LD} \cup dR_{t,MD} \cup dR_{t,SD}\right).$$

До пошкоджених енергоблоків АЕС, ТЕС, ГЕС, систем зберігання енергії таких типових для ОЕС України, як ГАЕС, а також генеруючих установок, що використовують відновлювані джерела енергії будемо відносити як ті, що були уражені безпосередньо, так і ті, що втратили можливість підключення до енергосистеми через руйнування трансформаторних підстанцій та/або інших критично важливих мережевих об'єктів.

Множини $dX_{t,LD}, dX_{t,MD}, dX_{t,SD}$ енергетичних об'єктів типу $X \in \{F, S, R\}$, уражених в період часу t, визначаються відповідно до:

1) стратегічних цілей, обраних агресором при плануванні ударів разом з типом застосованої зброї та її кількості;
2) ефективності роботи системи протиповітряної оборони;
3) наявності захисних споруд та рівня захисту, який вони здатні забезпечувати.

Для енергетичних об'єктів однакового типу $\forall X \in \{F, S, R\}$ результат дії перерахованих вище факторів впливу можна представити у вигляді характеристики наслідків ураження цих об'єктів (рис. 1). Така характеристика відображає кількість уражених об'єктів $|dX_{t,LD}|, |dX_{t,MD}|, |dX_{t,SD}|$, кластеризованих за масштабністю їх руйнувань у три групи, відповідно: великі, середні та дрібні руйнування.

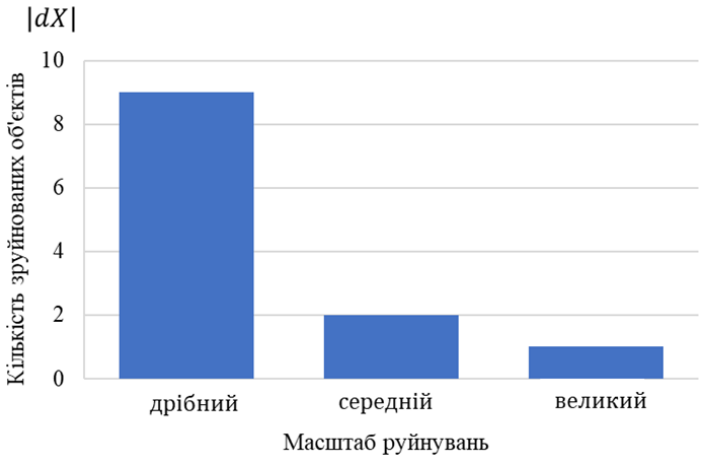


Рисунок 1 – Характеристика наслідків ушкодження об'єктів типу X

Енергетичні об’єкти типу $\forall X \in \{F, S, R\}$, які зазнали різних за масштабами руйнувань, для свого відновлення потребують виконання ремонтних робіт різної тривалості, відповідно, TL, TM, TS. Характеристика середньої тривалості таких робіт може бути представлена у вигляді діаграми (рис. 2).

Отже, користуючись такими характеристиками, а також наведеними вище рівняннями, можна визначити множини F_t, R_t, S_t, різного типу генеруючих енергоблоків, систем зберігання енергії та генеруючих установок, що використовують відновлювані джерела енергії, доступні для навантаження в ОЕС України на поточний період часу t.

За наявності необхідних запасів устаткування та матеріалів вважаємо прийнятними терміни відновлення енергогенеруючих та енергопередавальних об’єктів, в залежності від ступеня їх пошкодження, представлені в таблиці 1.

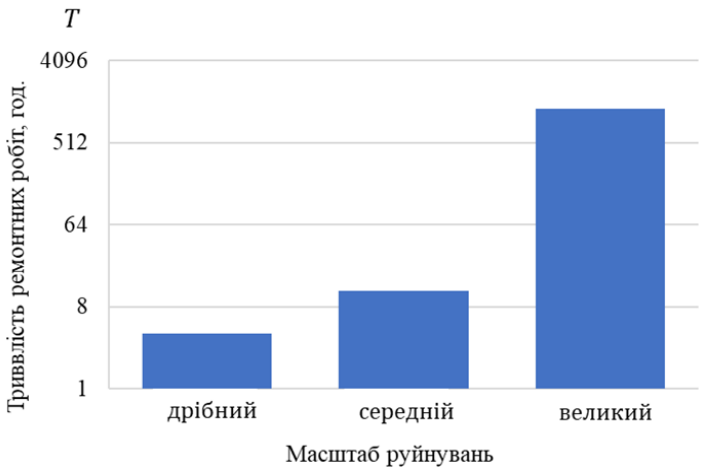


Рисунок 2 – Характеристика тривалості ремонтних робіт на пошкоджених енергетичних об’єктах типу X

Таблиця 1 – Орієнтовні терміни відновлення обладнання ОЕС України

Об’єкт/характер пошкоджень	ТЕС та ТЕЦ	Підстанції
Легкі пошкодження (без необхідності заміни обладнання)	1 тиждень	1-1,5 тижні
Середні пошкодження (заміна обладнання, запаси наявні)	1 місяць	1 місяць
Важкі пошкодження (за наявності обладнання та матеріалів)	6 місяців	1 місяць

Мінливість складу придатних до експлуатації енергетичних об’єктів є характерною ознакою ОЕС України, що знаходиться під руйнівним впливом систематичних масштабних терористичних атак та функціонує завдяки проведенню ремонтно-відновлювальних робіт та будівництва захисних споруд. Для дослідження резильєнтностіОЕС України необхідно використовувати кластерну модель режимів навантаження енергетичних об’єктів [1]. Від відомих моделей режимів навантаження електроенергетичних систем [2-7] кластерна модель відрізняється наявністю рівнянь динаміки кількісного складу придатних до експлуатації енергетичних об’єктів, а також описом режимів навантаження не окремих енергетичних об’єктів, а їх однотипових множин, що суттєво зменшує велику розмірність задач прогнозування таких режимів на періоді тривалістю до одного року з погодинною деталізацією.

Рівень задоволення попиту на електроенергію необхідно оцінювати динамічним коефіцієнтом

$$\mathbb{R}_{t,\Delta T} = \sum_{t-\Delta T}^{t} (l_t - \Delta l_t) \Big/ \sum_{t-\Delta T}^{t} l_t, \qquad t > \Delta T,$$

значення якого характеризує резильєнтність енергосистеми, тобто її готовність виконувати свою функцію для будь-якого t на відрізку часу $[t, t-\Delta T]$ тривалістю ΔT. Тут $l_t -$ обсяг попиту на електроенергію, $\Delta l_t -$обсяг розвантаження споживачів електроенергії.

Математична модель ОЕС України забезпечує короткострокове прогнозування режимів навантаження енергетичних об’єктів та розвантаження споживачів в умовах систематичних масштабних ракетно-дронових атак. Модель дозволяє оцінити резильєнтністьОЕС України за наступних сценарних умов:

1. очікуваних стратегій атак - їх періодичності, масштабності та цілеспрямованості;
2. динаміки ефективності роботи систем ППО щодо захисту енергетичних об’єктів;
3. запланованих графіків введення в експлуатацію захисних споруд різного рівня захисту;

4. динаміки ефективності застосування резервних механізмів та достатності ресурсів для виконання ремонтних робіт.

Для кожного типу енергетичних об’єктів зазначені сценарні умови відображаються у вигляді характеристик наслідків їх ушкодження (рис. 1) та тривалості ремонтних робіт (рис. 2).

Крім того, запропонована модель ОЕС України є інструментом аналізу її резильєнтності в умовах:

5. руйнівного впливу ракетно-дронових атак на транскордонні з’єднання національної електроенергетичної системи;

6. реалізації планів з будівництва нових транскордонних з’єднань;

7. ризиків прийняття окремими країнами-сусідами політичних рішень щодо обмежень обсягів експорту-імпорту електроенергії.

1. Саух, С. Є., & Борисенко, А. В. (2025). Моделювання електроенергетичної системи України та оцінювання її резильєнтності в умовах систематичних терористичних атак. Технічна електродинаміка, 2025(2), 57–70.
2. Knueven B., Ostrowski J., Watson J. “On Mixed-Integer Programming Formulations for the Unit Commitment Problem”, INFORMS Journal on Computing, vol. 32(4), 2020, pp. 855–1186.
3. Panos E., Lehtilä A. “Dispatching and unit commitment features in TIMES”, Energy Technology Systems Analysis Programme Report, Aug. 2016, pp. 51. https://iea-etsap.org/projects/TIMES_Dispatching_Documentation.pdf.
4. Montero L., Bello A., Reneses J. “A Review on the Unit Commitment Problem: Approaches, Techniques, and Resolution Methods”. – Energies. – 2022, 15 (4), 40p. https://doi.org/10.3390/en15041296.
5. Saukh S. "MILP formulation of the UC-problem with boundary conditions on the autonomous forecasting horizon," IOP Conf. Series: Earth and Environmental Science, 1254 (2023) 012034, 10p. – https://iopscience.iop.org/article/10.1088/1755-1315/1254/1/012034.
6. Palmintier B. S. Incorporating Operational Flexibility Into Electric Generation Planning. Impacts and Methods for System Design and Policy Analysis, Ph.D. thesis, Massachusetts Institute of Technology, 2013, 273p. http://hdl.handle.net/1721.1/79147.
7. Palmintier B.S., Webster, M.D. “Heterogeneous Unit Clustering for Efficient Operational Flexibility Modeling”. IEEE Transactions on Power Systems. vol. 29, no. 3, pp. 1089-1098, May 2014, doi: 10.1109/TPWRS.2013.2293127.

М.Ю. Комаров, С.Ф. Гончар

ОГЛЯД МЕТОДІВ ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кібератаки на об'єкти критичної інфраструктури під час російської агресії проти України, наряду зі збройними атаками, мають надзвичайно високий руйнівний вплив.

З початком повномасштабного вторгнення в Україну особливо зросла кількість політично вмотивованих кібератак, а також атак, які є складовими частинами комплексних атак, що включають у себе політичні, інформаційні, технічні та військові заходи.

Так, за даними Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, в 2024 році було опрацьовано 4315 кіберінцидентів. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз [1].

Таким чином, враховуючи вищенаведену інформацію, можна констатувати, що питання кіберстійкості об'єктів критичної інфраструктури взагалі та їх кіберрезильєнтності зокрема набуває надзвичайно високої актуальності.

Оцінювання кіберрезильєнтності включає різні методи, які допомагають аналізувати ризики, вразливості та здатність системи відновлюватися після кіберінцидентів. Ось кілька популярних підходів:

1. **Cyber Resilience Review (CRR)** – методика, яка оцінює здатність організації підтримувати критичні функції під час кіберзагроз.
2. **Cyber Risk Index (CRI)** – індекс, що вимірює рівень ризику для організації, враховуючи її вразливості та потенційні загрози.
3. **Framework for Improving Critical Infrastructure Cybersecurity (NIST)** – стандарт, який допомагає організаціям оцінювати та покращувати свою кіберстійкість.
4. **Failure Mode and Effects Analysis (FMEA)** – аналіз можливих збоїв та їх впливу на систему.

Cyber Resilience Review (CRR)

Методика Cyber Resilience Review (CRR) — це інструмент для оцінки операційної стійкості та практик кібербезпеки організації. CRR базується на моделі CERT® Resilience Management Model (CERT-RMM), розробленій в Інституті програмної інженерії Університету Карнегі-Меллона [2].

Огляд кіберстійкості (CRR) – це оцінка на основі співбесіди для оцінки операційної стійкості та практик кібербезпеки організації.

Завдяки CRR організація отримує та розвиває розуміння своєї здатності управляти кіберризиками під час звичайної діяльності та під час операційного стресу і кризи. Переваги включають:

- покращення обізнаності всієї організації щодо необхідності ефективного управління кібербезпекою;
- огляд сил і засобів, найбільш важливих для забезпечення безперервності надання критично важливих послуг у часи операційного стресу і кризи;
- каталізатор діалогу між учасниками з різних функціональних областей в організації;
- підсумковий звіт з використанням визнаних стандартів для відображення відносної зрілості процесів організаційної стійкості в кожній з 10 сфер.

Основні аспекти методики:

1) Інтерв'ю на основі оцінки: CRR проводиться у формі інтерв'ю, щоб оцінити здатність організації управляти кіберризиками як у звичайних умовах, так і під час криз.

2) 10 доменів оцінки: Методика охоплює такі ключові домени, як управління активами, управління конфігураціями, управління вразливостями, управління інцидентами, управління ризиками, навчання та обізнаність тощо.

3) Результати оцінки: Організація отримує звіт, який показує зрілість процесів стійкості в кожному домені, а також рекомендації для покращення.

4) Переваги: CRR сприяє підвищенню обізнаності про кібербезпеку, забезпечує діалог між різними функціональними підрозділами організації та допомагає забезпечити безперервність критичних послуг.

Cyber Risk Index (CRI)

Cyber Risk Index (CRI) — це методологія оцінки кіберризиків, яка допомагає організаціям визначити рівень загроз та вразливостей у їхній цифровій інфраструктурі.

Індекс кіберризиків – це онлайн платформа оцінювання рівня кіберризиків організації, розроблена компанією Trend Micro у тандемі з Ponemon Institute для дослідження кіберризиків та визначення ключових сфер для покращення кібербезпеки.

CRI вимірює розрив між поточним станом безпеки організації та ймовірністю атак. Як і раніше, остання версія CRI надає глобальний погляд на організації в Північній Америці, Європі, Азіатсько-Тихоокеанському регіоні та Латинській/Південній Америці.

Основою комплексного індексу CRI складає опитування IT-фахівців у різних частинах світу з метою вимірювання рівня готовності компаній реагувати на кібератаки. Індекс складається з двох складових частин:

1) Рівня готовності – відображає готовність організації до захисту від кібератак;
2) Середовища загроз – відображає стан ландшафту загроз на момент обчислення CRI.

Таблиця 1 – Індекс кіберризику

Регіон / Індекс	**Північна Америка**	**Європа**	**АСЕАН**	**Латинська Америка**	**Загальний**
Готовність	5,29	5,39	5,47	5,22	5,34
Загроза	5,39	5,27	5,42	5,25	5,33
Загальний індекс	-0,10	0,12	0,05	-0,03	0,01

Framework for Improving Critical Infrastructure Cybersecurity (NIST)

Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) — це добровільна методика управління ризиками кібербезпеки, розроблена Національним інститутом стандартів і технологій США (NIST). Вона спрямована на захист критично важливих об'єктів інфраструктури та інших секторів, важливих для економіки та національної безпеки.

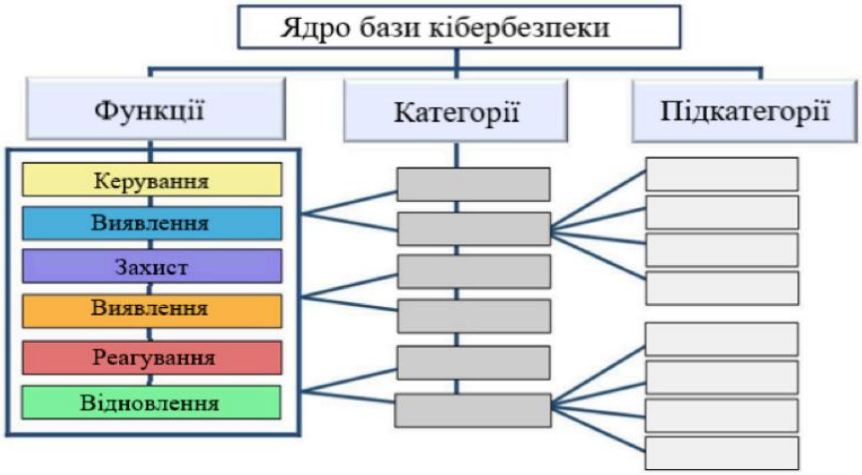


Рисунок 1 – Структура ядра CSF

Failure Mode and Effects Analysis (FMEA)

Метод FMEA (Failure Mode and Effects Analysis) — це систематичний підхід до аналізу потенційних відмов у процесах, продуктах або системах, а також оцінки їх наслідків. Цей метод широко використовується для підвищення якості, зниження ризиків і забезпечення безпеки в різних галузях, таких як автомобільна промисловість, охорона здоров'я, виробництво тощо.

Приклад застосування FMEA для аналізу стану кібербезпеки наведений нижче.

Таблиця 2 – Приклад застосування FMEA

Елемент	**Можливий режим відмови**	**Наслідки відмови**	**Причини відмови**	**Існуючі заходи контролю**	**Серйозність (S)**	**Ймовірність (O)**	**Виявлення (D)**	**RPN (S × O × D)**	**Рекомендовані дії**
Захист паролів	Використання слабких паролів	Неавторизований доступ до системи	Відсутність політики складності паролів	Мінімальна перевірка складності паролів	8	6	5	240	Впровадити політику складних паролів, двофакторну автентифікацію
Оновлення ПЗ	Відсутність оновлень	Уразливість до відомих атак	Невчасне оновлення систем	Ручне оновлення	9	5	4	180	Автоматизувати оновлення програмного забезпечення
Захист даних	Витік конфіденційних даних	Репутаційні та фінансові втрати	Недостатній контроль доступу	Базові заходи безпеки	10	4	6	240	Впровадити шифрування даних, обмежити доступ до конфіденційної інформації

Цей приклад демонструє, як FMEA може бути використаний для виявлення та усунення слабких місць у кібербезпеці.

Індекс RPN визначається як добуток бальних оцінок тяжкості S, частоти виникнення O та вірогідності виявлення D:

$$I_{RPN} = S \times O \times D \quad (1)$$

Розрахований показник дозволяє провести порівняння різних режимів в рамках одного аналізу. Також індекс RPN придатний для оцінки ефективності корегувальних дій ERPN, яка здійснюється наступним чином

$$E_{RPN} = \frac{I_{RPNi} - I_{RPNr}}{I_{RPNi}} \quad (2)$$

де: IRPNi – значення індексу RPN до впровадження корегувальних дій;

IRPNr – переглянуте значення індексу RPN після реалізації запланованих заходів.

Отримане значення дозволяє зробити висновок про зміну ризику виникнення відмови та ефективності впровадження корегувальних заходів.

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.
2. Cyber resilience review (CRR). Method Description and Self-Assessment User Guide. https://www.cisa.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf.

А.В. Ониськова

КІБЕРБУЛІНГ – ЯК УБЕЗПЕЧИТИ ДІТЕЙ ВІД ЙОГО НЕГАТИВНИХ НАСЛІДКІВ

Кожна людина, яка живе в соціумі, може зіткнутись із фізичним чи психологічним насильством щодо себе. Особливо це твердження є актуальним у стосунках між дітьми шкільного віку та молоді.

Цькування у шкільному середовищі мало місце завжди. Це не те, що виникло миттєво й нізвідки. Однак, в теперішній час цькування (булінг) отримало розповсюдження як у всьому світі, так і в Україні. Ця проблема набула такого масштабу, що про неї почали відкрито говорити і виникла необхідність протидіяти булінгу на законодавчому рівні та встановити відповідальність за такі діяння [1].

Особливу увагу слід приділити кібербулінгу. Спілкування людей у мережі Інтернет зазвичай знеособлене, що може викликати оманливе почуття безкарності та суттєво полегшує застосування психологічного насильства, тому звертаємо увагу на те, що зі зростанням темпів використання цифрових технологій діти все частіше піддаються саме цьому виду цькування.

Фактом сьогодення є те, що найактивнішими користувачами мережі Інтернет є підлітки. Особливостями підліткового віку є стрімкі зміни у психо-фізичному стані, що можуть призводити до проявів агресивної поведінки як у реальному, так і у віртуальному просторі. З кожним роком кількість юних користувачів збільшується. Інтернет у сьогоденні став невід'ємною частиною життя сучасних дітей, їхнім найближчим оточенням, джерелом знань про навколишній світ, а також низки негативних явищ, із якими можуть зіштовхнутися підлітки під час користування мережею Інтернет.

Що таке кібербулінг? Кібербулінг – це булінг із застосуванням цифрових технологій. Він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах. Це форма агресії, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований.

Приклади включають: поширення брехні про когось або розміщення фотографій, які компрометують когось, у соціальних мережах; надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями; видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені [2].

Отже, кібербулінг – це напади з метою завдання психологічної шкоди, які здійснюються через електронну пошту (і-мейл), миттєві повідомлення, розгортаються в чатах, на веб-сайтах, в соціальних мережах; діють через текстові повідомлення або через зображення (фото, відео); до кібербулінгу відносять також терор за допомогою мобільного телефонного зв'язку.

Висновок такий, що кібербулінг – це умисні дії, що скоюються однією особою або групою осіб відносно іншої особи, посередництвом електронних засобів комунікації, з метою завдання шкоди, що можуть здійснюватися напряму, або анонімно і можуть призвести до низки негативних наслідків в результаті створення ситуації напруження, тиску, залякування, переслідування [3].

Ознаки того, що підліток став жертвою кіберцькування: раптова зміна поведінкового й емоційного стану дитини після користування нею соціальних мереж (це може бути агресивність, підозрілість і відверта замкнутість); деструктивні стосунки батьків з дитиною (особливо загострюються під час обговорення реального життя підлітка); істеричні прояви характеру (несподівані безпричинні сльози, крик); погіршення здоров'я через безсоння та занепокоєння дитини; невдалі спроби суїциду; дитина необмежено користується інтернетом, надаючи перевагу віртуальному світу; різке погіршення навчального процесу в школі (дитина неохоче йде на навчання, суперечить вчителям і батькам).

Батьки мають пояснювати своїм дітям, що: спілкування з незнайомцями в інтернеті може нести небезпеку, тому краще спілкуватися зі знайомими у реальному житті людьми; доцільно також закрити від незнайомців свою сторінку в соціальних мережах та список друзів; не варто писати назву навчального закладу, де навчається дитина; не слід надсилати незнайомцям з інтернету і в приватні повідомлення свою адресу та номер телефону [4].

Якщо дитина стала жертвою булінгу, то: поговоріть з дитиною, дайте їй зрозуміти, що ви не звинувачуєте її в ситуації, що склалася, готові її вислухати і допомогти; запитайте, яка саме допомога може знадобитися дитині, запропонуйте свій варіант вирішення ситуації; поясніть дитині, до кого вона ще може звернутися за допомогою у разі цькування (психолог, соціальний педагог, класний керівник, адміністрація школи/гімназії, поліція); підтримайте дитину в налагодженні стосунків з однолітками та підготуйте її до того, що вирішення проблеми булінгу може потребувати певного часу; будьте підтримкою для дитини [5]!

Жодна дитина не може бути об'єктом незаконного посягання на її честь і гідність.

Профілактики кібербулінгу передбачає навчання користувачів мережі Інтернет основним правилам безпеки і коректної поведінки по відношенню до інших користувачів спільноти.

1. Наказ МОН від 28.12.2019 № 1646 Деякі питання реагування на випадки булінгу (цькування) та застосування заходів виховного впливу в закладах освіти. https://zakon.rada.gov.ua/laws/show/z0111-20#top.
2. Кібербулінг – що це та як це зупинити? https://www.unicef.org/ukraine/cyberbulling.
3. Міхеєва О.Ю. Корнієнко М.М. Кібербулінг як соціально-педагогічна проблема, Young Scientis, №11(63), November 2018, с.247-251.
4. Кібербулінг: що це, яким він буває та як від нього захистити свою дитину. https://www.telegraf.in.ua/kremenchug/10082081-kberbulng-scho-ce-yakim-vn-buvaye-ta-yak-vd-nogo-zahistiti-svoyu-ditinu.html.
5. Що таке булінг та кібербулінг. Їхні види і шляхи вирішення. https://vseosvita.ua/library/so-take-buling-ta-kiberbuling-ihni-vidi-i-slahi-virisenna-485112.html.

С.М. Дяченко, О.С. Терещенко, Д.В. Строгонов

ВПЛИВ УЛЬТРАЗВУКОВИХ КОЛИВАНЬ, ПРИКЛАДЕНИХ ДО МЕТАЛЕВОГО ДРОТУ НА ПРОЦЕС ОТРИМАННЯ СФЕРИЧНИХ ПОРОШКІВ МЕТОДОМ ПЛАЗМО-ДУГОВОГО РОЗПИЛЕННЯ

На тлі безперервно зростаючого споживання порошкових матеріалів гранулометричного складу 45-105 мкм у технологіях 3D-друку з використанням енергії електронного променю (EBM) та лазера (SLM, SLS, DLMS) з'являється потреба використання нових підходів до розпилення [1].

Плазмо-дугове розпилення як один з найактуальніших методів отримання високоякісних сферичних порошків використовує енергію прямої або дотичної плазмової дуги для отримання розплаву металу на торці заготовки, зрив краплі під дією тиску плазмової дуги та диспергування крапель розплавленого металу з подальшим твердінням та кристалізацією отриманих частинок при їх прольоті у реакторі в середовищі інертного газу. Одним із перспективних підходів до отримання металевих порошків є введення високочастотних (зазвичай 20–40 кГц) ультразвукових коливань у металеві розплави, що дозволяє отримати металевий порошок високої чистоти та вузького розподілу часток за розмірами. Метод відрізняється тим, що розплавлений метал контактує безпосередньо з поверхнею, що вібрує з ультразвуковою частотою. Коливання створюють поверхневі хвилі та кавітуючи збурення, які розбивають розплав на краплі. Краплі охолоджуються в газовому середовищі (аргон, азот, повітря) та твердіють у вигляді порошку [2, 3].

Автори планують провести роботи дещо по іншій схемі, а саме – виконати розпилення металевого дроту за допомогою енергії плазмової дуги з одночасним накладанням на дріт в твердому стані ультразвукових коливань. Такий підхід має сприяти отриманню більш дрібних вихідних крапель розплаву та звузити розподіл частинок за розмірами.

Крім того, відомо, що прикладання ультразвуку сприяє покращенню механічних властивостей металу дроту до моменту розплавлення, очищенню його поверхні та модифікації мікроструктури, попередньому нагріву дроту, що в кінцевому результаті повинно дозволити контролювати параметри отриманих частинок.

Ультразвукові коливання, які прикладаються до металевого дроту в холодному (твердому) стані, суттєво впливають на його мікроструктуру без досягнення температур плавлення. Такий вплив реалізується через високочастотні механічні вібрації, що породжують циклічні мікродеформації. В результаті цього процесу внутрішня структура металу зазнає значних змін, що може позитивно впливати на його механічні властивості, наприклад, зміну розподілу та щільності дислокацій, утворення субграней і навіть зернове уточнення [4] .

Фізичні механізми впливу ультразвуку на дріт можуть бути такими:

Акустична стимуляція внутрішніх дислокацій. При контактному впливі ультразвукових коливань у металевому дроті з'являються високочастотні циклічні навантаження. Такі цикли можуть «розблокувати» дислокації, які до цього були зафіксовані на перешкодах (наприклад, вторинних фазах, включеннях або попередніх накопиченнях дислокацій). Внаслідок цього дислокації починають рухатися, реорганізовуватися та скупчуватися в певних регіонах, що може вести до їхнього з'єднання в міжгранні сітки чи формування субструктур.

Феномен акустичної пластифікації (acoustoplasticity). При механічному впливі ультразвукових коливань спостерігається явище акустичної пластифікації. Це означає, що ефективне значення критичного напруження для початку пластичних деформацій (коли дислокації починають рухатися) знижується завдяки додатковій енергії, внесеній коливаннями. В результаті навіть без макроскопічного деформування можуть виникати локальні мікропластичні деформації, що сприяють реорганізації внутрішньої структури.

Генерація мікростресів і їхній вплив. Контактний ультразвук забезпечує періодичне навантаження, завдяки якому у матеріалі виникають мікростреси. Ці мікростреси сприяють переналаштуванню внутрішньої мікроструктури.

Утворення субграней. Поступова організація дислокацій може призводити до формування дислокаційних сіток, що згодом перетворюються на субграні або навіть нові зернові межі.

Зернова структура. У деяких випадках можливе зернове уточнення, коли початкове зерно розділяється на менші ділянки через накопичення і реорганізацію дислокацій. [5]

Для проведення дослідних робіт було розроблено та виготовлено обладнання для введення ультразвукових імпульсів з частотою 20 кГц в металевий дріт з подальшим розплавленням його з використанням плазмотрону. Зовнішній вигляд обладнання показано на рис.1.

Ультразвукова коливальна система складається з п'єзоелектричного перетворювача та механічних резонаторів - бустера та хвилеводу (сонотроду). Дріт для атомізації проходить між робочим торцем сонотроду та поверхнею спеціальної опори що притискається до сонотроду. Опора може бути як резонансна (в сенсі коливального процесу), так і нерезонансна. На рис.2 показано результат моделювання методом скінченого елементу (МСЕ) взаємодії частини коливальної системи (бустер та сонотрод) з резонансною опорою [6]. Задача розраховується при умові дії зосередженої сили з частотою 20 кГц, яка прикладається нормально до входу бустера.

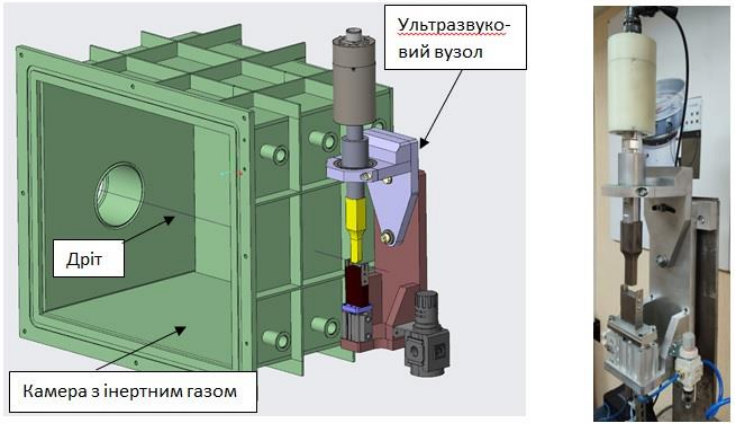


Рисунок 1 – Схема експериментальної установки та фото вузла кріплення ультразвукової коливальної системи

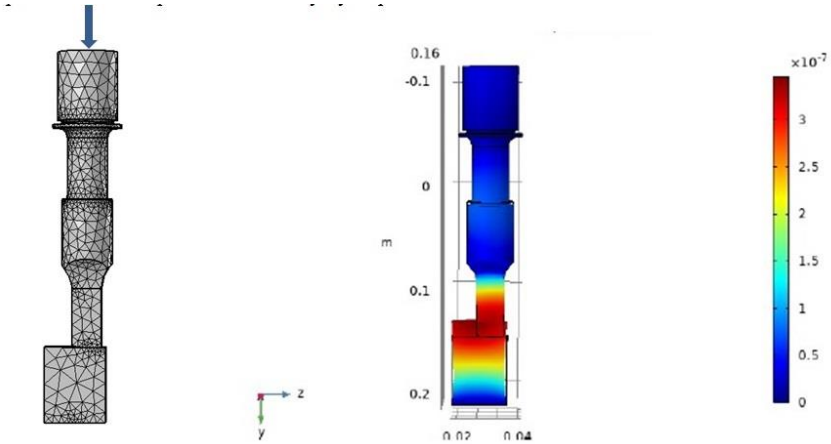


Рисунок 2 – Епюри коливального процесу: бустер та сонотрод в контакті з активною опорою

Робоча поверхня сонотроду має радіусну фаску, яка дозволяє змінювати кут введення коливань в дріт. На рис.3 показана схема вузла кріплення коливальної системи та фрагмент з наклоним розташуванням коливальної системи.

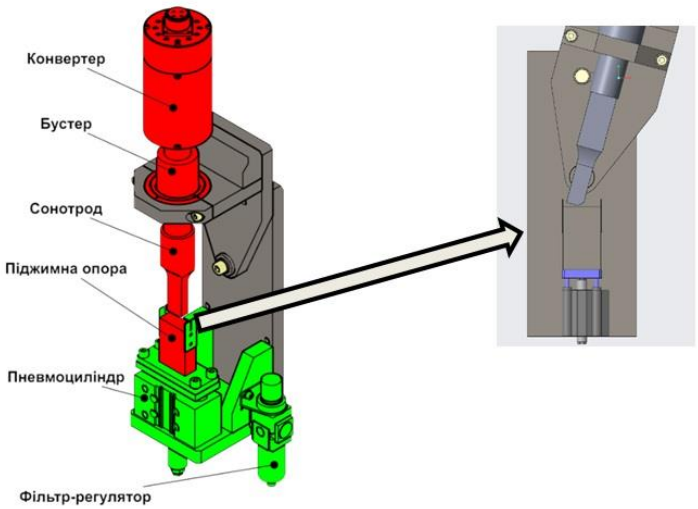


Рисунок 3 – Вузол кріплення ультразвукової коливальної системи з можливістю кутового введення ультразвукових коливань в дріт

Аналіз наукових публікацій показав, що питанню з розпилення металевого дроту з ультразвуковим збуренням до моменту розплавлення в плазмотроні приділялось недостатньо уваги та не є досконало вивченим. Заплановані авторами роботи на цій дослідній установці можуть допомогти зрозуміти широкий спектр актуальних наукових і прикладних питань у галузях порошкової металургії, матеріалознавства, плазмових технологій та нанотехнологій, а саме:

1. Контроль розміру та морфології частинок

Як ультразвук впливає на середній діаметр крапель, їх гранулометричний розподіл і сферичність?

Чи можливо стабільно отримувати нано- або субмікронні порошки?

2. Енергетична ефективність процесу

Як ультразвукові коливання впливають на температуру розплаву, час плавлення дроту та загальну витрату енергії?

Чи може ультразвук зменшити необхідну теплову потужність плазмотрона?

3. Гомогенізація складу та контроль фазового стану

Чи покращує ультразвук розчинення легуючих елементів у дроті до розплаву?

Як коливання впливають на структурну однорідність сплаву?

4. Запобігання агломерації частинок

Чи знижує ультразвук ефект формування сателітів у польоті?

Вплив ультразвуку на диспергування вихідних крапель у дрібніші ще до або в момент розпилення.

5. Взаємодія фаз "твердий — рідкий — плазма"

Механізм впливу ультразвуку на границю розділу фаз "твердий дріт ↔ рідкий метал ↔ плазма".

6. Параметрична оптимізація процесу

Які комбінації частоти, амплітуди ультразвуку, швидкості подачі дроту та струму плазмотрона забезпечують максимальну якість порошку?

Встановлення оптимальних режимів атомізації для різних металів (Al, Cu, Ti, Fe).

7. Аналітика домішок та оксидів

Як змінюється кількість оксидних включень, якщо застосовувати ультразвук?

Можливість зменшення газовмісних дефектів у частинках порошку.

8. Розробка нових матеріалів

Можливість синтезу композиційних порошків: порошковий дріт або композиційний дріт + ультразвук.

Формування металокерамічних частинок або порошків з функціональними включеннями (TiC, Al2O3, B4C).

9. Тестування моделей

Валідація моделей теплопереносу, фазових переходів і гідродинаміки розплаву під впливом ультразвуку.

Розробка числових моделей розпаду крапель у присутності УЗ-коливань.

1. Shanthar R., Chen K., Abeykoon C. (2023) Powder-Based Additive Manufacturing: A Critical Review of Materials, Methods, Opportunities, and Challenges. Advanced Engineering Materials. 25(I). 19. https://doi.org/10.1002/adem.202300375.
2. Novel Cold Crucible Ultrasonic Atomization Powder Production Method for 3D Printing / Ł. Żrodowski et al. Materials. 2021. Vol. 14, no. 10. P. 2541. URL: https://doi.org/10.3390/ma14102541.
3. Arc character and droplet transfer of pulsed ultrasonic wave-assisted GMAW / C. Fan et al. The International Journal of Advanced Manufacturing Technology. 2017. Vol. 95, no. 5-8. P. 2219–2226. URL: https://doi.org/10.1007/s00170-017-1414-7.
4. Dubovyy, O. M., Karpechenko, A. A., Bobrov, M. M., Zhdanov, O. O., Makrukha, T. O., & Nedelko, Y. E. (2017b). Formation of Polygonization Nanoscale Substructure and Its Impact on the Physical and Mechanical Properties of Metals, Alloys, and Sprayed Coatings. METALLOFIZIKA I NOVEISHIE TEKHNOLOGII, 39(2), 209–243. https://doi.org/10.15407/mfint.39.02.0209.
5. Balasubramani, N., StJohn, D., Dargusch, M., & Wang, G. (2019). Ultrasonic Processing for Structure Refinement: An Overview of Mechanisms and Application of the Interdependence Theory. Materials, 12(19), 3187. https://doi.org/10.3390/ma12193187.

Г.П. Дубинський, В.Ю. Зубок

ЕЛЕКТРОЕНЕРГЕТИКА В ЛАНЦЮЖКУ ПОСТАЧАННЯ РЕЗИЛЬЄНТНИХ ЦИФРОВИХ ПОСЛУГ

Резильєнтність – здатність готуватися та планувати, сприймати, відновлюватися та успішніше адаптуватися до несприятливих подій. Це найбільш широке, мультидисциплінарне визначення [1], в фокусі якого знаходиться складна система. Ця система має певну динамічну властивість, яка закладена в її організацію (функціональну схему) та яка послуговує основою здатності подолання негативних впливів, що витікають з ризиків.

Резильєнтність ланцюжків постачання (supplychains, надалі – ЛП) визначена важливим фактором [2–4]. Ланцюжок постачання цифрової послуги(надалі *цифровий ЛП*) — це сукупність організаційних, технічних і інформаційних компонентів, які забезпечують створення, надання, підтримку та оновлення цифрової послуги для кінцевого користувача. Його можна описати як мультидисциплінарну систему, яка включає не лише традиційних постачальників ресурсів і технологій, а й логіку програмного забезпечення, дані, цифрову інфраструктуру та підтримку безперервної доступності. В табл. 1 представлено найтиповіші ключові елементи цифрового ЛП.

Таблиця 1 – Ключові елементи цифрового ЛП

№	Елемент	Складові	Функції
1.	Хмарні провайдери та ЦОДи	IaaS-провайдери (AWS, Azure, Google Cloud) Центри обробки даних, хостинг-провайдери	Фізична інфраструктура, обчислювальні ресурси, стійкість до збоїв.
2.	Платформи доставки	Content Delivery Networks (Akamai, Cloudflare) DNS-провайдери Системи кешування (GGC), аналітика трафіку (Cloudflare)	Забезпечують оптимізовану доставку контенту, мінімізацію затримок, захист від DDoS.
3.	Оператори мереж електронних комунікацій	Backbone-оператори (транзитний рівень, Tier-1/Tier-2) Національні або регіональні оператори інтернету	Забезпечують інтернет-зв’язок між дата-центрами, провайдерами, мережами обміну трафіку, транснаціональні переходи.
4.	Провайдери останньої милі	Локальні інтернет-провайдери, мобільні оператори, кабельні мережі FTTH, xDSL, 4G/5G, Wi-Fi mesh	Забезпечують доступ кінцевого користувача до цифрової послуги.
5.	Домашні/корпоративні мережі	Маршрутизатори, Wi-Fi точки доступу, проксі/брандмауери Внутрішні LAN-сегменти, IoT-шлюзи	Впливають на якість, затримку, безпеку та конфіденційність передачі даних.
6.	Кінцеві пристрої споживача	Комп’ютерна техніка, мобільні пристрої, розумні пристрої, IoT Операційні системи, браузери, застосунки, інтерфейси	Є точкою взаємодії з цифровою послугою

Електроенергетика визнана найбільш критичним ресурсом для функціонування інформаційних та операційних технологій [5]. Це підтверджує наявність залежності від електричної енергії кожного з розглянутих елементів цифрового ЛП.

Математично ЛП часто моделюється як орієнтований граф, мережа потоків, або система динамічних рівнянь. Обирати формальне представлення ланцюга постачання залежно від того, які саме аспекти резильєнтності будее обрано для аналізу (структурну стійкість, адаптивність, час відновлення тощо). Два перших варіанта пов’язані з дослідженням топології. Надалі під топологією розуміється взаємне розташування елементів системи (вершин та дуг графа, пристроїв в мережі масового обслуговування тощо).

Графова модель ЛП може бути представлена як орієнтовний зважений граф, що складається з вершин та дуг. Вершинам та дугам ставляться у відповідність певні сутності. Наприклад:

Вершини (nodes, VV) — постачальники, склади, виробники, дистриб'ютори, споживачі.

Дуги (edges, EE) — потоки товарів, інформації або фінансів.Кожна дуга має вагу: вартість, час доставки, ймовірність збоїв тощо.

ТодіЛП може бути позначений як

$$G = (V, E, w)$$

де $w : E \to \mathbb{R}$ – функція ваг (наприклад, ризики, обсяги).

На такій моделі природно проводити аналіз з використанням графових методів та теорії складних мереж. Відомі метричні характеристики, такі як ступінь вузла, навантаженість, центральність, кластеризація

дозволяють знаходити спільні точки відмови, досліджувати стійкість до видалення вузлів (nodefailure), моделювати каскадні ефекти.

Схематичне подання цифрового ЛП можна представити наступним чином:

[Хмара/ЦОД] → [CDN/DNS] → [Backbone-оператор] →

→ [Нац. оператор] → [Провайдер останньої милі] →

→ [Домашня мережа] → → [Кінцевий пристрій] →

→ [Інтерфейс послуги / ідентифікація / оплата].

Слід зазначити, що сама по собі цифрова послуга може бути декомпонована на складові (наприклад, доступ до державного електронного реєстру передбачає використання цифрової довірчої послуги), і в кожної складової може виникнути власний ЛП. В результаті аналізу та декомпозиціїмережевих архітектур, типів електронних комунікацій, систем передачі даних, топологій, задіяних у наданні найбільш чутливих інформаційних потреб населення та бізнесу будуть отримані множини споживачів, цифрових послуг, засобівдоступу,операторів електронних комунікацій різних рівнів, провайдерів інфраструктур цифрових послугі т.і.

1. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. DOI: 10.1007/s10669-013-9485-y.
2. International Organization for Standardization. (2022). ISO 28000:2022.Security and resilience — Security management systems — Requirement. Retrieved from: https://www.iso.org/standard/79612.html.
3. ДСТУ ISO/TS 22318:2023 Безпека та стабільність. Системи управління неперервністю бізнесу. Настанови щодо управління неперервністю ланцюга постачання (ISO/TS 22318:2021, IDT). Retrievedfrom: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106505.
4. NIST IR 7622. (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. Retrieved from https://csrc.nist.gov/pubs/ir/7622/final.
5. NIST SP 800-82 Rev. 3. (2023) Guide to Operational Technology (OT) Security. Retrieved from: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

О.А. Владимирський, В.М. Зварич, Ю.І. Гижко, В.О. Артемчук, І.А. Владимирський, С.А. Недосєка

ДЕЯКІ ПИТАННЯ ОЦІНКИ РЕЗИЛЬЄНТНОСТІ ЕЛЕМЕНТІВ ЕНЕРГЕТИЧНОГО ОБЛАДНАННЯ ПРИ ВПРОВАДЖЕННІ БЕЗДРОТОВИХ СИСТЕМ ДІАГНОСТИКИ

Електроенергетичні системи розглядаються як кіберфізичні комплекси, в яких операції програмуються, координуються й контролюються через інформаційно-комунікаційну інфраструктуру. Мережеві компоненти енергосистем є вразливими до кібератак, що обумовлює необхідність розробки методів мінімізації кібернетичних ризиків.

Оцінка стійкості систем після аварійних подій базується на концепції зниження втрат і прискореного відновлення працездатності до проектного рівня. Ключовим критерієм є здатність енергосистеми адаптуватися до змінених умов експлуатації з мінімальними невідповідностями функціональних показників.

Універсальна діагностична платформа для всіх компонентів теплоелектростанцій технічно не здійсненна, тому на етапі проєктування формуються критерії критичності для ідентифікації пріоритетних об’єктів контролю. Елементи, від яких залежить підтримка безперервності технологічних процесів, відносяться до першої черги моніторингу.

Локалізація дефектів трубопроводів водо- та теплопостачання відбувається з використанням методів неруйнівного контролю. Поширені причини пошкоджень — знос матеріалів і корозійні процеси. Регулярне виявлення витоків є необхідним завданням для забезпечення надійності інфраструктури [1].

Метод вібродіагностики належить до класу високочутливих методів неруйнівного контролю й застосовується для аналізу динамічних характеристик механічних вузлів. Еталонними виробниками обладнання для вібродіагностики є Brüel & Kjær, PCB Piezotronics, SPM Instrument, Derricktron, Bently Nevada, Timken, а також виробники електротехнічного обладнання — Siemens і ABB.

У контексті мобільних діагностичних систем мобільні вузли збору та передавання даних повинні забезпечувати оперативність оцінки технічного стану основного й допоміжного обладнання. Бездротові канали передачі даних забезпечують гнучкість розгортання та можливість оперативного масштабування систем [2].

Архітектура бездротової інформаційно-вимірювальної системи вібродіагностики містить:

- апаратні модулі для реєстрації вібраційних сигналів та їх оцифрування;
- комунікаційні модулі для передачі даних у центральний обчислювальний вузол;
- програмні компоненти для керування процесом збору даних, статистичної обробки та алгоритмів класифікації технічного стану за заданими критеріями [3, 4].

Визначення пріоритетності елементів моніторингу реалізується через ризико-орієнтований підхід, що дозволяє сконцентрувати обчислювальні ресурси й мережеву пропускну здатність на найбільш критичних об’єктах із високим рівнем потенційних наслідків при відмові [5].

У статті представлено методологію оцінки резильєнтності елементів енергосистем із використанням бездротових систем діагностики, включно з алгоритмами пріоритизації, структурою ІВС вібродіагностики та класифікацією виявлених аномалій.

У якості бездротових систем та прикладів їхнього застосування розглядаються:

- сучасні стандартні системи широкого застосування, це серія стандартів IEEE 802.11 (Wi-Fi), стандарт IEEE 802.15.1 (Bluetooth), а також рішення за стандартом 802.15.4 (ZigBee, WirelessHART, MiWi), LPWAN;
- існуючи спеціалізовані системи реєстрації діагностичних даних, такі як британська система Enigma3hyQ виробництва Ovarro Connecting Technologies, що використовує 3G та 2G зв’язок, американська система PermaNET Trunc Main (TM) GPS компанії FCS моніторингу трубопроводів, що використовує GPS синхронізацію реєстрації даних за часом та ін.;
- система кореляційної радіо синхронізації розподілених у просторі вимірювань, створену в ІПМЕ ім.. Г.Є.Пухова НАН України.

Серед визначальних характеристик при виборі бездротової системи є задовільні для конкретних завдань діагностування пропускна здатність, точність часової синхронізації вимірювань, дальність дії, завадовий захист, часова стабільність, кліматична стійкість, мобільність, енергоспоживання, екологічність, вартість, надійність. Аналізуються можливі причини відмов, пошкоджень систем, їхні наслідки. В ході цього аналізу зіставляються часові терміни відновлення функцій системи, що припустимі, з фактичними прогнозованими термінами.

Робота виконується в рамках проєкту НФДУ 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень системи тепло- та водопостачання з урахуванням зношення та мілітарних впливів».

1. Владимирський О.А., Владимирський І.А. Просторовий і частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів// Електрон. моделювання, 2021, 43, № 4, с.22 —36. https://doi.org/10.15407/emodel.43.04.022.
2. Wu W.-S., Kuo K.C., Lin Yu-H., Tsai Y.-C. Non-contact magnetic cantilever-type piezoelectric energy harvester for rotational mechanism. Microelectronic Engineering. 2018, vol. 191, pp.16-19. https://doi.org/10.1016/j.mee.2018.01.026.

3. 3. Babak V.P., Babak S.V., Myslovych M.V., Zaporozhets A.O., Zvaritch V.M. Diagnostic Systems for Energy Equipments Part of the Studies in Systems, Decision and Control book series (SSDC, volume 281) - Erfurt: Springer Nature, (Switzerland), 2020. - 133 p. https://doi.org/10.1007/978-3-030-44443-3.
4. Гижко Ю. і Зварич В. 2024. Особливості побудови компонентів багаторівневих експертних систем вібродіагностики вузлів електротехнічного обладнання з урахуванням використання бездротових блоків зв'язку. Технічна електродинаміка. 5 (Сер 2024), 094. DOI: https://doi.org/10.15407/techned2024.05.094.
5. Ganin A., Massaro E., Gutfraind A., Steen N., Keisler J., A. Kott A., Mangoubi R., Linkov I., Operational resilience: concepts, design and analysis Scientific Reports| 6,19540 ; (2016). URL: https://doi.org/10.1038/srep19540.

О.А. Владимирський, І.А. Владимирський, В.О. Артемчук, І.П. Криворучко, Д.М. Семенюк

РЕЄСТРАТОРИ АКУСТИЧНИХ СИГНАЛІВ ДІАГНОСТИЧНОЇ СИСТЕМИ ТРУБОПРОВІДІВ «РАСТР-2В»

ВСТУП.

В Україні близько 35% водопровідних та 44% теплових мереж перебувають в аварійному стані [1, 2]. Це призводить до значних втрат води та тепла, вимагає оперативного виявлення та усунення витоків для забезпечення сталого тепло- та водопостачання населення. Значний загальний знос підземних мереж трубопроводів та міліарні впливи ускладнюють пошук витоків через:

- розгалуженість мереж та зношеність запірної арматури, що ускладнює ізоляцію окремих ділянок і підвищує ризик аварійних ситуацій;
- зниження тиску в системах, що ускладнює використання традиційних акустичних методів діагностики, оскільки зменшується інтенсивність акустичних сигналів витоків;
- необхідність підвищеної оперативності, коли час на проведення діагностичних робіт обмежений через військові дії та пов'язані з ними ризики;
- наявність потужних завад, як акустичних, так і електромагнітних, що утруднює точне визначення місць пошкоджень та ін..

Оскільки наявні умови діагностування є ширшими ніж діагностичні можливості сучасних течешукачів, ці прилади потребують розвитку та адаптації. Для цього створено дослідну систему РАСТР-2В з більш широкими, ніж звичайні прилади, технічними можливостями за частотним та динамічним діапазонами реєстрованих сигналів, завадовим захистом, кількістю синхронізованих вимірювальних станцій та каналів, з додатковим активним зондуванням трубопроводів [3].

ПРИЗНАЧЕННЯ.

Система РАСТР-2В призначена для визначення координат витоків підземних трубопроводів у складних умовах. Багатоканальний реєстратор є складовою частиною системи. Його призначенням є здійснення запису сигналів з вібродатчиків, що встановлюються на трубопроводі, рис.1,2. До складу системи РАСТР-2В входить 3 реєстратори. Їхнім спільним режимом роботи є контрольований за якістю, синхронізований за часом запис вібросигналів з вібродатчиків завданою тривалістю. Відповідне програмне забезпечення (ПЗ) встановлене на РС-сумісні комп'ютери, що входять до складу реєстраторів. ПЗ працює під управлінням ОС Windows.

ОПИС АПАРАТНОЇ ЧАСТИНИ.

Застосування трьох, рознесених у просторі на десятки метрів реєстраторів, порівняно зі звичайними течешукачами з двома станціями, дозволяє ефективно використовувати додаткові методи діагностування та вимірювати важливі характеристики поширення сигналів по трубах. Синхронна реєстрація трьох вібросигналів кожним з реєстраторів дозволяє враховувати суттєву просторову нерівномірність коливань стінки трубопроводу в алгоритмах параметричної кореляційної обробки акустичних даних [4].

Для коректного застосування кореляційних методів потрібна синхронізація записів вібросигналів з точністю не гірше 0,1 мс. Для цього використовується загальний для всіх реєстраторів радіосигнал синхронізації у вигляді генерованого системою білого шуму. Перед обробкою записів з трьох реєстраторів здійснюється їхня програмна синхронізація. Для цього обчислюються взаємні кореляційні функції (ВКФ) прийнятих реєстраторами радіосигналів і за цими ВКФ визначаються часові поправки до сигналів з датчиків з внесенням до них відповідних часових корегувань.

Реєстратор побудовано на базі комп'ютера у форматі нетбук, рис.1, та містить вхідні фільтри, блоки регулювання посилення (АРП), багаторозрядні АЦП. Вбудований контролер пересилає прийняті з датчиків сигнали у мобільний комп'ютер за допомогою USB інтерфейсу. Передбачена можливість програмного управління коефіцієнтами посилення кожного з вхідних каналів, у тому числі безпосередньо у вібродатчиках. Здійснюється оперативний звуковий контроль будь-якого з вхідних каналів. Конструктивно автономний реєстратор виконано у вигляді кейсу, рис.1. Окремим пристроєм, створеним на базі переносної радіостанції, є цифровий генератор синхросигналу у вигляді рівномірного за спектром шуму у діапазоні 100...4000 Гц. Передбачена робота системи в пасивному та в активному режимах. Тому в системі використовується генератор тестових сигналів для зондування трубопроводу та акустичний випромінювач. Випромінювач зображений на рис.2, середнє фото, пристрій на трубопроводі червоного коліру.

ОСНОВНІ РЕЖИМИ РОБОТИ.

Режими обробки записів вібросигналів з метою ретельного подолання завад та виявлення витоків у програмне забезпечення реєстраторів (ПЗ) не входять, бо вирішення цих задач потребує більших можливостей екрану, обчислювальних ресурсів комп'ютера та більш зручних умов. Тому ця робота, як і при звичайному застосуванню кореляційних течешукачів, виконується в автомобільній лабораторії. Функцією ПЗ є якісна реєстрація вихідних даних, яка відбувається біля трубопроводів, рис.1.

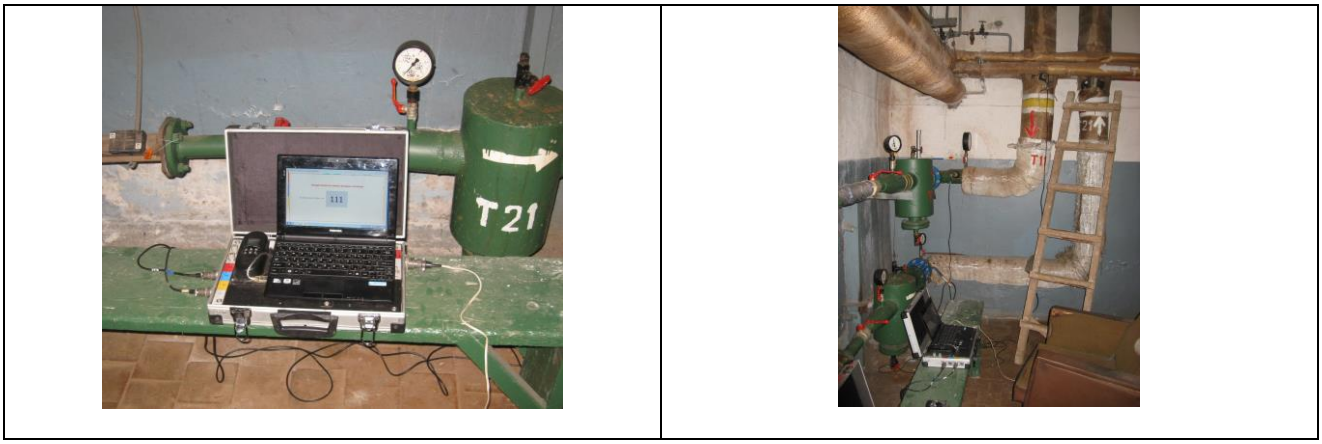


Рисунок 1 – Реєстратор системи РАСТР-2В під час випробувань у бойлері

Рисунок 2 – Датчики реєстратора та акустичний випромінювач системи РАСТР-2В
на трубопроводі теплової мережі

Основними функціями ПЗ, рис.3, є:

- чотирьох канальний осцилограф для візуального контролю форми вібросигналів та синхросигналу;
- запис вібросигналів окремими файлами, у розширенні імені яких прописується ідентифікатор реєстратора, який використовується у подальшій груповій обробці даних, яка відбувається в автомобільній лабораторії;
- управління посиленням сигналів через ручний чи автоматичний режими;
- обчислення та спостереження поточних спектрів сигналів;
- контроль рівнів сигналів;
- управління тривалістю записів сигналів.

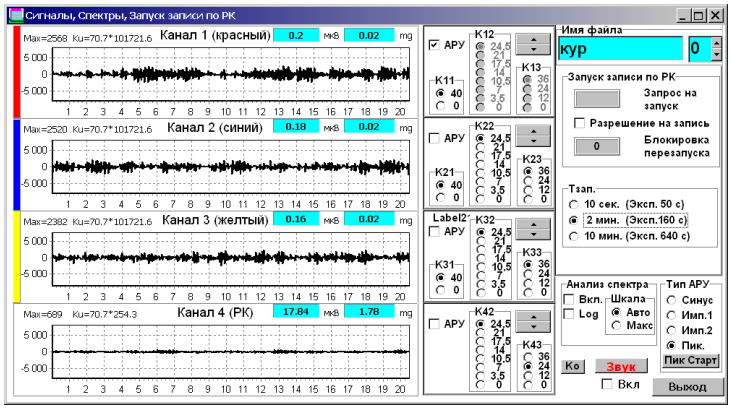


Рисунок 3 – Формат ПЗ з контролю та запису сигналів

Ці та інші функції ПЗ реєстраторів забезпечують витребувану якість реєстрації акустичних даних у мінливих зовнішніх акустичних умовах. Наприклад, передбачено три види алгоритмів роботи АРП в залежності від інтенсивності та виду нестаціонарних завад. Бо адаптація до завад АРП сприяє підвищенню чутливості системи РАСТР-2В до сигналів витоків.

Автори висловлюють щиру подяку Національному фонду досліджень України за грантову підтримку, завдяки якій була виконана дана розробка в рамках проєкту №2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів».

1. Центральне водопостачання України: скільки мереж перебуває аварійному стані. URL: https://ru.slovoidilo.ua/2021/06/11/infografika/obshhestvo/centralnoe-vodosnab zhenie-ukrainy-skolko-setej-naxoditsya-avarijnom-sostoyanii (дата звернення: 9.05.2025).
2. Фандоріна О. В аварійному і ветхому стані перебуває 44% тепломереж України. Українські новини. URL: https://ukranews.com/ua/news/726665-teplomerezhi-ukra yiny-perebuvayut-v-avarijnomu-stani (дата звернення: 9.05.2025).
3. Vladimirsky A.A., Vladimirsky I.A. Correlation parametric method for determining the velocity of acoustic wave propagation in a pipeline. *Electronic Modeling*, 2024, 46(6).P.55-63. URL:https://doi.org/10.15407/emodel.46.06.055 (дата звернення: 9.05.2025).
4. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання.* 2021. Т.43, №3. С.3-16.
URL: https://doi.org/10.15407/emodel.43.03.003 (дата звернення: 9.05.2025).

С.Б. Бурченко, І.І.Сватовський

НАПРЯМКИ РОЗВИТКУ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ УПРАВЛІННЯ ОБ'ЄКТАМИ ЕНЕРГЕТИКИ ВІД КІБЕРЗАГРОЗ

Взаємопов'язаний характер сучасної критичної інфраструктури, до якої відносятся і енергетичні мережі, означає, що порушення в одному секторі промисловості може мати опосередкований вплив на інші. Ця взаємозалежність посилює потенційний вплив кібератак і вимагає комплексного підходу до захисту енергетичної інфраструктури. Кібератаки на енергетичний сектор можуть мати далекосяжні наслідки по причиніїх впливуна роботу інших критично важливих сфер. Якщо функціонування енергомереж буде порушено, то це може призвести до порушення роботи інших мереж критичної інфраструктури.

За таких умов організації повинні дедалі більше застосовувати спільні підходи до кібербезпеки, зокрема, в інтеграції своїх інформаційних технологій (IT), операційних технологій (OT) та Інтернету речей (IoT). Дотримання стандартів і кращих практик кібербезпеки відіграють вирішальну роль у цьому, що підтверджується увагою до спільних питань безпеки у кіберпросторі та регуляторних актів, таких як серія стандартів ISO/IEC 27000, IEC 62443 та Директива Європейського Союзу NIS2. Інтеграція IT, OT та Інтернету речей в енергетичних системах, таких як розумні мережі - SmartGrid, підвищує ефективність та швидкість реагування, але також може створити нові види їх вразливостей. Розуміння взаємозалежностей всередині та між секторами інфраструктури має вирішальне значення для підвищення їх стійкості до дії зовнішніх і внутрішніх загроз кібербезпеки.

Конвергенція OT/IT має як численні переваги, але також і свої ризики, які наражають промислові системи на нові загрози кібербезпеки. Стандарт ISO/IEC 27001:2022 надає сукупність вимог до корпоративного управліннящодо стратегій управління ризиками та здатностісті проактивного виявлення, оцінки та зменшення потенційних загроз. Стандарт спрямовує зусилля компаній на управління інцидентами безпеки для забезпечення оперативного реагування на кібератаки. У середовищах OT для цього повинні слугувати такі засоби, як системи виявлення та запобігання вторгнень (IDS/IPS), які можуть контролювати дотримання правил безпеки і в мережевих IT системах і в системах управління OT.

Для впровадження стратегій управління вразливостями OT є критично важливим виявлення та пом'якшення потенційних ризиків безпеки, перш ніж зловмисники ними скористаються. Це включає проведення регулярних оцінок ризиків, актуалізації програмного забезпечення та постійного моніторингу аномальної активності в мережах управління об'ктами енергетики, який повинний сприяти оперативному реагуванню на кіберзагрози.

При цьому основні технології та методи, що використовуються в кібербезпеці критичної інфраструктури як IT, так і OT, повинні включати такі з них: 1. сегментація мереж - ізоляція критично важливих систем від менш захищених і менш важливих для обмеження поширення шкідливого програмного забезпечення та несанкціонованого доступу; 2. забезпечення конфіденційності сигналів управління мережами і важливого трафіку –застосуванням алгоритмів надійного шифрування даних як під час їх передачі, так і при зберіганні в базах даних; 3. безперервний моніторинг - впровадження рішень IDS/IPS для виявлення загроз у режимі реального часу, що дозволяє оперативно реагувати на потенційні інциденти; 4. управління доступом – застосуванням механізмів багатофакторної а автентифікація (MFA), щоб гарантувати, що лише уповноважений персонал матиме доступ до критично важливих систем.

Оскільки кіберзагрози продовжують розвиватися, майбутнє захисту енергетичної інфраструктури залежатиме від того, наскільки ефективно буде забезпечена адаптація до появи цих нових ризиків. Новітні технології, такі як штучний інтелект (ШІ) та машинне навчання (МН), відіграватимуть дедалі більшу роль у виявленні вразливостей та потенційних атак на мережі, а також на реалізацію відповідних контрзаходів щодо протидії ним. Системи на базі ШІ можуть аналізувати величезні обсяги даних для виявлення закономірностей, які можуть вказувати на потенційні загрози, тоді як застосування алгоритмів МН може з часом покращувати точність прогнозів оцінок безпекової ситуації. Крім того, технологія блокчейн також може підвищити безпеку та прозорість транзакцій між об'єктами енергетичної інфраструктури.

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. https://www.iso.org/standard/27001.
2. ISA/IEC 62443 Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
3. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

А.О. Кримська

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ В ЕНЕРГЕТИЧНІЙ ГАЛУЗІ

Вступ. Використання штучного інтелекту (ШІ) з метою підвищення ефективності захисту від кіберзагроз в енергетичній галузі активно розглядалося протягом останніх років. Чимало дослідників зосереджувалиувагу на цій темі, виокремлюючи різноманітні підходи до її реалізації. Наприклад, A. Bécueetal. досліджували виклики та можливості, що виникали на перетині ШІ, кіберзагроз. Автори наголошувалина здатностіінтелектуальних систем адаптивно реагувати на складні й динамічні кіберризики в енергетичних інфраструктурах [1]. Зокрема F. Bertoneetal. звернули увагу на ефективність технологій ШІ в запобіганні кібератакам на розумні мережі. Алгоритми машинного навчання демонстрували високу точність виявлення аномалій у реальному часі, що підвищувало рівень безпеки систем розподілу енергії. Особливу увагу автори приділили моделюванню атак на основі історичних даних, що уможливлювало формування превентивних сценаріїв реагування. Дослідники підкреслили важливість постійного оновлення навчальних вибірок для збереження релевантності моделей в умовах змінних загроз [2]. Науковці A. J. deAzambujaetal. надали огляд рішень кібербезпеки на основі ШІ, акцентуючи на захисті критичної інфраструктури. Так, застосування глибокого навчання допомагає виявляти нові вектори атак та автоматизувати процеси реагування. Такі підходи сприяють мінімізації людського фактора в управлінні кіберзахистомі забезпечували адаптивність систем безпеки. Вчені також наголосили на необхідності міждисциплінарної взаємодії для розроблення ефективних рішень [3]. АвториJ. Goveaetal. зосередилися на впровадженні інтелектуальних моделей у захист енергетичних об’єктів. Інтеграція ШІ підвищувала стійкість систем до складних атак, зокрема спрямованих на SCADA-компоненти. Дослідники висвітлювали роль когнітивного аналізу в прогнозуванні загроз і швидкій ідентифікації вразливостей. У дослідженні було підкреслено важливість адаптивних механізмів навчання для підтримки актуальності захисних моделей [4]. Натомість A. B. Igeetal. аналізували ефективність захисних стратегій у сфері відновлюваної енергетики. Учені наголосили, що інтелектуальні підходи сприяли виявленню вразливостей ще на етапі проєктування інфраструктури, створюючи умови для проактивного реагування. Вони також розглянули можливість використання адаптивних ШІ-рішень для динамічного оновлення політик безпеки відповідно до рівня загроз і зазначили, що такий підхід здатен забезпечити безперервність функціонування систем навіть під час кібератак [5].

Огляд новітніх кіберзагроз і ролі ШІ взміцненні захисних механізмів представив F. Jimmy. У дослідженні було вказано, що моделі ШІ не лише виявляли загрози, а й прогнозували поведінку зловмисників, дозволяючи будувати гнучкі системи реагування. Вчений звернув увагу на здатність ШІ до самонавчання, що підвищувало ефективність у боротьбі з раніше невідомими атаками, а також підкресливважливість інтеграції таких рішень у державну кіберполітику [6]. АвториM. Ozkan-Okayetal. здійснили комплексне дослідження ефективності ШІ та машинного навчання у сфері кібербезпеки, за результатами якого було встановлено, що застосування цих технологій забезпечувало скорочення часу реагування на інциденти й підвищення рівня автономності систем безпеки [7]. Практичні аспекти захисту систем енергомоніторингу в УкраїнірозглянулиO. Ponomarenko & A. Krymska. Вони запропонуваливикористання ШІ для обробки даних у режимі реального часу та виявлення аномалій, що давало змогу швидше ідентифікувати потенційні порушення. Автори акцентували на важливості адаптивних моделей аналізу, які здатні ефективно працювати в умовах нестабільного інформаційного середовища. У дослідженні підкреслено, що впровадження таких рішень підвищує стійкість енергетичних об’єктів до складних атак [8]. Можливості ШІ у виявленні та запобіганні кіберзагрозам окреслено в праціM. Rizvi. У дослідженні зазначено, що інтелектуальні системи можуть не лише автоматизувати виявлення загроз, а й оптимізувати процеси прийняття рішень у сфері безпеки. Особливу увагу було приділено використанню нейромережевих алгоритмів для побудови гнучких моделей реагування. Також було визначеноздатність таких рішень до самоадаптації у відповідь на зміну характеру атак [9]. Зокрема H. Szczepaniuk& E. K. Szczepaniuk дослідили застосування алгоритмів ШІ в енергетичному секторі на прикладі реальних кейсів. Інтеграція ШІ забезпечувала зростання точності моніторингу та прогнозування потенційних загроз, сприяючи оперативному реагуванню на кіберінциденти. Такі технології зменшували навантаження на персонал, підвищували автономність систем безпеки та сприяли створенню масштабованих інтелектуальних рішень для захисту критичної інфраструктури [10].

Мета дослідження. Обґрунтувати можливості та окреслити умови ефективного застосування технологій ШІ для забезпечення кібербезпеки в енергетичній галузі в умовах цифровізації.

Результати дослідження. У сучасних умовах цифровізації та стрімкого розвитку інформаційних технологій енергетична галузь дедалі більше інтегрується з кіберпростором. Це створює нові можливості для автоматизації, моніторингу та управління енергосистемами, проте водночас підвищує їхню вразливість до кіберзагроз. З огляду на стратегічну важливість енергетичної інфраструктури для національної безпеки, питання кіберзахисту набуває актуальності. У цьому контексті зростає інтерес до застосування технологій ШІ, які демонструють високу ефективність у виявленні, аналізі та нейтралізації кіберзагроз. Енергетичні компанії, які впроваджують системи ШІ для захисту своїх мереж, отримують змогу проактивно реагувати на потенційні атаки, мінімізуючи наслідки або повністю їм запобігаючи. Однією з головних переваг ШІ є здатність обробляти великі обсяги даних у режимі реального часу. У рамках кібербезпеки це означає виявлення аномалій у

функціонуванні мереж, відстеження нетипової поведінки користувачів або пристроїв, а також ідентифікацію підозрілих шаблонів трафіку. Наприклад, за допомогою алгоритмів машинного навчання можна автоматично класифікувати види атак, прогнозувати їхні можливі наслідки та пропонувати відповідні контрзаходи. Такі системи вже довели свою ефективність у виявленні DDoS-атак і фішингових кампаній. Застосування нейронних мереж у поєднанні з методами поведінкового аналізу дає змогу формувати адаптивні системи захисту, які здатні навчатися на основі нових загроз і вдосконалювати власні моделі. ШІ виступає не лише як інструмент реагування, а й як засіб превентивногозахисту. Впровадження ШІ також сприяє оптимізації роботи центрів моніторингу безпеки (SOC), адже передбачає зменшення навантаження на аналітиків, автоматизацію рутинних процесів, що дає змогу зосередитися на більш складних і критичних аспектах. Водночас ефективність застосування ШІ у сфері кібербезпеки енергетики залежить від якості навчальних даних, обсягу історичної інформації про інциденти, а також від загальної цифрової зрілості компанії.

Важливим аспектом також є безпека самих алгоритмів ШІ, оскільки вони можуть бути об'єктом атак (наприклад, підкидання некоректних даних для «обману» моделі). У зв'язку з цим постає необхідність у створенні надійних процедур валідації моделей, перевірки результатів їхньої роботи, а також розробки стандартів етичного та безпечного застосування ШІ в критично важливих інфраструктурах. Окремо варто підкреслити, що ефективність протидії кіберзагрозам із застосуванням ШІ в енергетичній галузі значною мірою залежить від міжгалузевої співпраці, обміну знаннями між державними органами, операторами енергосистем іпостачальниками технологій. Формування єдиної кіберекосистеми, уякій ШІ відіграватиме роль ключового інструменту аналізу та управління ризиками, є необхідною умовою сталого розвитку сектору. Важливу роль у цьому також відіграє міжнародна співпраця, зокрема участь у глобальних ініціативах з обміну інформацією про кіберзагрози, формування стандартів безпеки та проведення спільних навчань. Окрім того, впровадження ШІ в системи енергетичної безпеки потребує інвестицій у людський капітал –підготовка фахівців, які володіють як знаннями у сфері енергетики, так і навичками роботи з сучасними інструментами ШІ, є критичним чинником успіху. Розвиток міждисциплінарних освітніх програм, центрів досліджень і лабораторій ШІ на базі енергетичних установ та університетів є важливою частиною стратегії цифрової трансформації галузі.

Висновки. Таким чином, використання технологій штучного інтелекту в боротьбі з кіберзагрозами в енергетичній галузі відкриває нові можливості для забезпечення сталості, надійності та безпеки енергопостачання. Успішна інтеграція ШІ потребує комплексного підходу, що охоплює як технологічні, так і організаційні, правові та етичні аспекти. У майбутньому можна очікувати подальшого вдосконалення інтелектуальних систем безпеки, їхньої інтеграції з технологіями інтернету речей, блокчейну та квантових обчислень, що дасть змогу створити більш стійку до кіберзагроз енергетичну інфраструктуру. У перспективі саме штучний інтелект може стати ключовим елементом комплексної системи кіберзахисту в енергетиці, здатної не лише реагувати на атаки, а й передбачати їх і запобігати їм.

1. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review, 54(5),* 3849-3886. https://link.springer.com/article/10.1007/s10462-020-09942-2.
2. Bertone, F., Lubrano, F., & Goga, K. (2020). Artificial intelligence techniques to prevent cyber attacks on smart grids. *Annals of Disaster Risk Sciences: ADRS, 3(1).* https://hrcak.srce.hr/249381.
3. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics, 12(8).* https://www.mdpi.com/2079-9292/12/8/1920.
4. Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems, 12(5).*https://www.mdpi.com/2079-8954/12/5/165.
5. Ige, A. B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *International Journal of Science and Research Archive, 12(1),* 2978-2995. https://www.researchgate.net/profile/Oluwatosin-Ilori-3/publication/383377711_Analyzing_defense_strategies_against_cyber_risks_in_the_energy_sector_Enhancing_the_security_of_renewable_energy_sources/links/66c9fca8920e05672e4d0a1c/Analyzing-defense-strategies-against-cyber-risks-in-the-energy-sector-Enhancing-the-security-of-renewable-energy-sources.pdf.
6. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library, 1,* 564-74. https://pdfs.semanticscholar.org/ee4c/c97d11f7c827fc1a8a059e584d739ad87cf8.pdf.
7. Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEe Access, 12,* 12229-12256. https://ieeexplore.ieee.org/abstract/document/10403908/.
8. Ponomarenko, O., & Krymska, A. (2024, May 29). Strategies for ensuring data security in energy monitoring systems in Ukraine. Institute of Modeling Problems in Power Engineering named after G. Ye. Pukhov. Scientific and Practical Conference "Cybersecurity of Energy Sector", Kyiv, Ukraine, 94–97. https://ipme.kiev.ua/wp-content/uploads/2024/06/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8-%D0%91%D0%95-2024.pdf.
9. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science, 10(5),* 055-060. https://www.academia.edu/download/102883869/IJAERS_08_may_2023.pdf.
10. Szczepaniuk, H., & Szczepaniuk, E. K. (2022). Applications of artificial intelligence algorithms in the energy sector. *Energies, 16(1).* https://www.mdpi.com/1996-1073/16/1/347.

ADVANCING STRESS TESTING METHODOLOGIES FOR HIGH-IMPACT LOW-PROBABILITY EVENTS

Abstract.

The AGILE project introduction. The increasing frequency of disruptive natural, technological, and hybrid disasters calls for new ways to manage systemic risks. Particularly, High-Impact Low-Probability (HILP) events pose critical challenges for infrastructure resilience, where traditional risk management tools often fall short. The AGILE project (stands for "AGnostic risk management for high Impact Low probability Events")is the Horizon Europe project funded by the European Commission and United Kingdom Research and Innovations (UKRI). The AGILE Consortium (Agile, n.d.) is shaping a practical approach to disaster risk management through building a new kind of stress-testing method and to design agnostic, flexible tools that can be adapted to different sectors for stress-testing and managing such complex risks. The AGILE framework is depicted at fig.1.

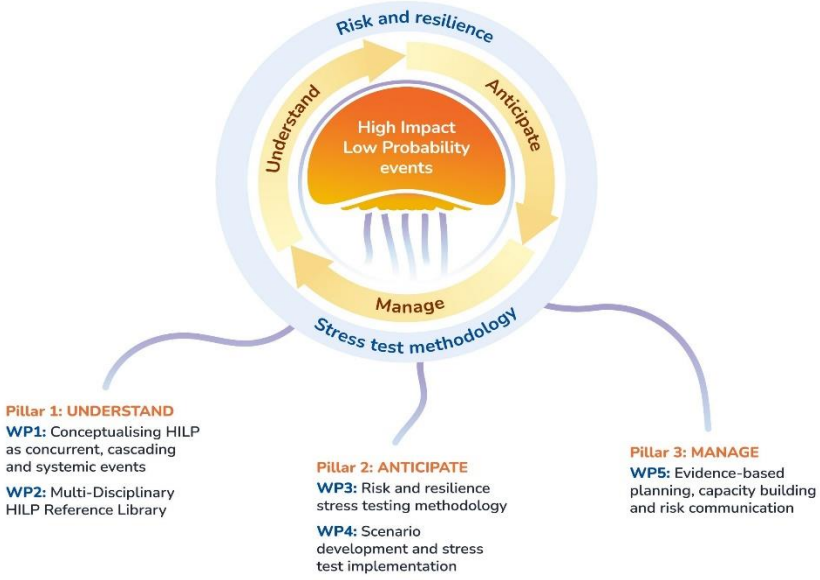


Figure1 – The AGILE Project Concept

Within AGILE consortium, Ukraine is represented by Pukhov Institute for Modelling in Energy Engineering (PIMEE), National Academy of Sciences of Ukraine entity. Amid ongoing war and hybrid threats, Ukraine offers a unique environment to test the adaptability and relevance of stress-testing frameworks in real-world high-risk settings.

Tiered approach to resilience stress testing. In the context of disaster risk reduction, the assessment of the resilience of critical infrastructure through stress testing is studied. The Agile project uses a multi-level approach to stress testing, depicted in Fig. 2 (Linkov et al., 2022).

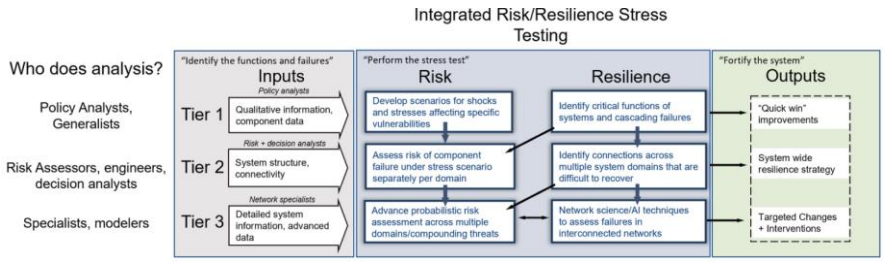


Figure2 – Tiered approach to integrated risk and resilience stress testing for critical infrastructure

According to this approach, Tier 1 is a screening level assessment that identifies critical system functions and analyzes changes in system connectivity in response to shocks and stressors. Tier 2 uses simplified system models to understand and quantify the connections between different domains and their impact on critical system functions. Tier 3 uses advanced modeling techniques (e.g., network science and artificial intelligence) to further assess changes in interconnected networks in response to random and targeted threats and attack scenarios (Linkov et al., 2018).

Ukrainian case study description. PIMEE's case study is dedicated to the digital resilience of Ukraine. It contains an in-depth analysis of the current situation and best practices for maintaining, restoring and developing digital infrastructure and digital services in the context of kinetic and cyber impacts that continue to be brought by russian military aggression. It highlights technological, organizational and human challenges and threats. Stress testing will focus on the cascading effects of the power industry on communication and information systems (CIS), which play a crucial role in sustainable life of anybusiness, all types of electronic communications, mass media, public information services etc. Through its national case study, PIMEE provides a testbed to explore how European methodologies can be transferred and customized to Eastern European infrastructures under persistent crisis conditions. AGILE's core methodology starts from structured risk assessment frameworks with multilevel stress test levels (ST-1 to ST-3). PIMEE works to adapt these tools to the constraints and realities of Ukraine's infrastructure, where uncertainty, resource scarcity, and external attacks are constant factors. For example, in Ukraine, national energy system and electronic communications often operate under partial damage. Instead of assuming that critical infrastructure will always remain fully functional, PIMEE focuses on how these systems behave and adapt when parts of them are damaged or disrupted. Our goal is to understand how services can be maintained even partially during crises, and how quickly they can recover. This perspective is crucial for refining stress test parameters and calibration against HILP scenarios that are no longer hypothetical.

Preparations to the Tiers 1 and 2 testing. The essential part of tiered stress testing is a system description. Stress test partners describe the system to be tested by answering three questions as follows.

Q1. To whom or what do we aim to enhance resilience and preparedness for HILPs?

A1. We aim to enhance the resilience of electronic communications, digital services, and supply chains of digital services to subscribers in response to cascading failures originating from disruptions in the energy system caused by HILP events

Q2. What is the heuristic definition of the system?

A2. The system can be heuristically defined as an interconnected network of energy-dependent digital infrastructure, including telecommunications networks, cloud computing services, data centers, and digital service providers, which collectively ensure the continuity of digital services to end-users. This system operates within a broader socio-technical and regulatory environment that influences its resilience to cascading failures from energy disruptions.

Q3. The primary objectives of this system's functioning.

A3: the primary objectives are:

– Ensuring continuity of critical digital services (e.g., emergency communications, financial transactions, public services) despite energy disruptions.

– Implementing redundancy and failover mechanisms to mitigate cascading effects.

– Enhancing coordination between energy providers, digital service operators, and regulatory bodies to improve crisis response.

– Developing adaptive recovery strategies that enable rapid restoration of services following disruptions.

– Strengthening cyber-physical resilience by integrating energy management solutions and backup power infrastructures.

Further work and activities. An essential component of PIMEE's work is facilitating local stakeholder dialogue through workshops and scenario sessions. These aim to bridge the methodological innovations of AGILE with the daily operational logic of Ukrainian infrastructure actors (Palma‐Oliveira et al., 2017). PIMEE's approach involves early engagement of operators and decision-makers to co-define hypothetic HILP scenarios and validate stress-test results. The results of the stress testing conducted by the Ukrainian PIMEE team within the AGILE project will be included in the overall data set and methodological framework of the project, which forms the basis for strategic recommendations in the field of risk management of HILP events. These results will contribute to strengthening the capacities of stakeholders in risk management at the local, national and European levels, and will serve to adapt European approaches to the conditions of countries that are in a state of possible risks.

As stated in the Grant Agreement (Grant Agreement №101121356, Section 1, pp. 8–9), *"The project will ultimately improve the strategic and operational risk management capacities and capabilities of DRM (Disaster Risk Management) stakeholders on local, regional and national level and thus strengthen the societal resilience to new and emerging risks in Europe and beyond."*

1. Agile – Consortium(n.d.) Available: https://www.project-agile.eu/consortium/ (Accessed on 12.05.2025).
2. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction, 82*, 103323. https://doi.org/10.1016/j.ijdrr.2022.103323.
3. Linkov, I., Fox-Lent, C., Read, L., Allen, C. R., Arnott, J. C., Bellini, E.,& Woods, D. (2018). Tiered approach to resilience assessment. Risk Analysis, 38(9), 1772-1780.https://doi.org/10.1111/risa.12991.
4. Palma-Oliveira, J. M., Trump, B. D., Wood, M. D., & Linkov, I. (2017). Community-driven hypothesis testing: A solution for the tragedy of the anticommons. Risk Analysis, 38(3), 620-634.

А.А. Симонов, О.М. Дибач

ПРОБЛЕМИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ ТА КЕРУЮЧИХ СИСТЕМ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ

Актуальність забезпечення кіберзахисту інформаційних та керуючих систем (ІКС) атомних електростанцій (АЕС) продовжує дедалі збільшуватися, оскільки відбувається планова модифікація ІКС АЕС, із відповідним зростанням складності цифрових систем, збільшенням взаємозв'язків між ІКС і різними блоками АЕС, а також активністю зловмисників, здатних використати слабкі місця як у самій інфраструктурі, так і в організаційних процесах.

Серед головних викликів, які не повною мірою враховані чинними стандартами, зокрема IEC 62645:2019 [1], варто відзначити низку специфічних аспектів управління ризиками кіберзахисту.

Перш за все, серйозною проблемою є складність визначення ймовірності виникнення малоймовірних, але потенційно критичних подій, таких як порушення нормального виконання функцій безпеки, яке ініційоване кібератакою. В контексті об'єктів атомної енергетики, навіть одиничний такий інцидент може мати серйозні наслідки для ядерної та радіаційної безпеки. Наразі відсутні емпіричні статистичні дані щодо таких інцидентів, що відповідно обмежує можливість їх врахування під час оцінки ризиків [2].

Також однією з ключових проблем є обмежене врахування агрегованих ризиків, пов'язаних із використанням однакових ІКС у різних блоках АЕС або на різних майданчиках АЕС. Потенційна виявлена вразливість в одній такій ІКС може бути використана для компрометації інших аналогічних ІКС. Відсутність специфічних механізмів оцінки таких ситуацій може призводити до недооцінки потенціалу масштабного поширення кіберзагроз, оскільки кібератака може мати значно ширший вплив, ніж передбачалося під час оцінки ризиків. У таких випадках критичним є врахування не лише індивідуального ризику для окремої ІКС, а й кумулятивного ефекту, спричиненого широким застосуванням однотипних рішень. Додатково ускладнює оцінку агрегованих ризиків використання у складі ІКС заздалегідь розроблених загальнопромислових цифрових компонентів. Враховуючи обмежений доступ до повного складу апаратного та програмного забезпечення таких виробів, немає можливості повноцінно ідентифікувати та оцінити всі вразливості цих компонентів або потенційні вектори атак, які можуть задіяти ці компоненти, що значно ускладнює проведення оцінювання ризиків [3].

Крім того, надзвичайно складним є аналіз ризиків, пов'язаних із міжсистемними взаємозв'язками, особливо коли мова йде про непрямі функціональні залежності. Кібератаки, спрямовані на менш критичні функції, можуть через ланцюг взаємозв'язків мати негативний вплив на основні функції систем безпеки. Така складність взаємодій і взаємозв'язків наразі не відображена в існуючих інструментах аналізу ризиків, що знижує точність оцінювання та ефективність реагування на кіберзагрози [2].

Управління ризиками додатково ускладнюється невизначеністю в оцінці характеристик потенційного зловмисника. Зазвичай, аналіз ґрунтується на неповних даних та експертних оцінках, які не завжди можуть забезпечити достатню точність для прийняття обґрунтованих рішень. Відсутність достовірної інформації про мотивацію, ресурси, рівень технічної підготовки та інші параметри потенційного зловмисника знижує ефективність і достовірність оцінки ризиків [4].

Окремої уваги потребує питання відсутності уніфікованого процесу управління ризиками, який би враховував технічні, організаційні та регуляторні аспекти. Наявні відмінності у підходах до управління ризиками, що застосовуються у різних країнах, створюють додаткові труднощі. Зокрема, складно інтегрувати сталі практики та дієві підходи до оцінки ризиків, коли діючі регуляторні вимоги значно відрізняються. Різні організації та країни пропонують альтернативні рішення щодо оцінювання ризиків ІКС АЕС і часткового вирішення вищезазначених викликів:

– FCSRM/SCSRM (Facility and System Computer Security Risk Management) – розроблений Міжнародним агентством з атомної енергії підхід, який передбачає двоступеневу модель оцінювання ризиків кіберзахисту: на рівні всього об'єкта (FCSRM) та окремих систем (SCSRM). Він забезпечує комплексний розгляд як стратегічних, так і тактичних ризиків, пов'язаних з чутливими цифровими активами [5].

– HAZCADS (Hazards and Consequences Analysis for Digital Systems) – методика, розроблена EPRI (Electric Power Research Institute), що використовує системно-теоретичний аналіз процесів для виявлення небезпечних керуючих дій і розробки відповідних заходів кіберзахисту [6].

– CIE (Cyber-Informed Engineering) – стратегія Міністерства енергетики США, яка передбачає включення міркувань кібербезпеки в процес проєктування систем АЕС на ранніх стадіях життєвого циклу [7].

– EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité (фр.) – Expression of Needs and Identification of Security Objectives) – методика, яка використовується у Франції, орієнтована на формалізований аналіз потреб і визначення цілей безпеки. Вона дозволяє структурувати процес управління ризиками і включає інструменти для складання документації та підвищення обізнаності користувачів [8].

– HTRA (Harmonized Threat Risk Assessment) – канадський підхід, що базується на модульному і масштабованому фреймворку для стратегічного й тактичного аналізу. Він містить набір шаблонів і таблиць для спрощення оцінки ризиків [9].

Висновки

Ефективне управління ризиками кіберзахисту ІКС АЕС є критично важливим через ускладнення цифрових архітектур, зростання взаємозв'язків між системами та посилення кіберзагроз.

Існуючі стандарти не повною мірою враховують специфічні аспекти стосовно ризиків кіберзахисту, зокрема: агреговані ризики, міжсистемні залежності, відсутність повної інформації про цифрові компоненти та невизначеність щодо потенційних зловмисників.

Для підвищення ефективності управління ризиками ІКС на АЕС України важливо подолати вищезгадані виклики, розробити національні методичні рекомендації (з урахуванням міжнародних підходів/методик) щодо оцінювання та управління ризиками кіберзахисту, які охоплюватимуть технічні, організаційні та регуляторні аспекти.

1. International Electrotechnical Commission. (2019). *Nuclear power plants – Instrumentation and control systems – Cybersecurity requirements* (IEC 62645:2019). Geneva: IEC.
2. National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments* (NIST SP 800-30 Rev. 1). Gaithersburg, MD: U.S. Department of Commerce.
3. International Electrotechnical Commission. (2024). *Nuclear facilities – Instrumentation, control and electrical power systems – Cybersecurity risk management approaches* (IEC TR 63486:2024). Geneva: IEC.
4. International Atomic Energy Agency. (2021). *Computer Security for Nuclear Security* (IAEA Nuclear Security Series No. 42-G). Vienna: IAEA.
5. International Atomic Energy Agency. (2018). *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* (IAEA Nuclear Security Series No. 33-T). Vienna: IAEA.
6. Electric Power Research Institute. (2021). *Hazards and Consequences Analysis for Digital Systems (HAZCADS)*. Palo Alto, CA: EPRI.
7. U.S. Department of Energy. (2022). *National Cyber-Informed Engineering Strategy*. Washington, DC: DOE.
8. Agence nationale de la sécurité des systèmes d'information. (2020). *EBIOS Risk Manager – Expression des besoins et identification des objectifs de sécurité*. Paris: ANSSI.
9. Canadian Centre for Cyber Security. (2022). *Harmonized Threat Risk Assessment (HTRA) methodology*. Ottawa: CCCS.

С.Ф. Гончар, М.Ю. Комаров

ПІДХІД ДО ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ ІЗ ЗАСТОСУВАННЯМ АНАЛІЗУ РИЗИКІВ

На сьогоднішній день не можна гарантувати повну захищеність будь-якої інформаційної системи, у тому числі об'єкта критичної інформаційної інфраструктури (далі – системи) [1]. Якщо раніше метою було забезпечення кібербезпеки системи, то поступово вона трансформується у забезпечення кіберрезильєнтності. Як зазначається в [2] кібербезпека зосереджена на зміцненні системи, щоб запобігти зменшенню її функціональності, увага приділяється ступеню зменшення функціональності, а кіберрезильєнтність зосереджена на відновленні функціональності системи. Відновлення може бути повним або частковим, та передбачає адаптацію системи, яка підвищить її стійкість до майбутніх деструктивних дій або, в деяких випадках, покращить її функціональність. При цьому, на перший план виходять задачі мінімізації часу відновлення функціональності системи, забезпечуючи захист життєво важливих її компонентів, тобто, забезпечення кіберрезильєнтності інформаційних систем об'єктів критичної інформаційної інфраструктури, як стану критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз [3].

Враховуючи викладене вище актуальною задачею являється оцінювання кіберрезильєнтності систем, що дасть змогу оцінити кіберрезильєнтність, порівняти з допустимим значенням, зробити висновок про її достатність чи необхідність підвищення тощо.

Дослідження показують різні підходи до оцінювання кіберрезильєнтності. Так, у [4] описується підхід до оцінювання кіберрезильєнтності, зосереджений на здатності системи протистояти чітко визначеним і передбачуваним загрозам, тобто уникненні деструктивних дій, що є частиною традиційного процесу управління ризиками. У цьому випадку оцінюється ймовірність відмови компонентів системи у відповідь на різні сценарії загроз з метою зміцнення системи, щоб уникнути кібервторгнення. Однак, як зазначають автори [2, 4], це не зовсім кіберрезильєнтність, оскільки ключовим поняттям кіберрезильєнтності є прийняття кібервторгнення в систему, як ймовірної події, в результаті чого знижується функціональність системи. При цьому, основна увага приділяється здатності системи відновлюватися та адаптуватися, а не просто чинити опір кібератакам. Як зазначають автори [2, 4], кіберрезильєнтність характеризує те, що відбувається після кібератаки та вимагає готовності як до відомих, так і до невідомих кіберзагроз.

Підхід до оцінювання кіберрезильєнтності, який включає аналіз ризиків, як центральний компонент, розглянуто у [5]. При цьому, аналіз ризиків залежить від характеристики загроз, вразливостей і наслідків деструктивних дій для визначення очікуваної втрати критичної функціональності системи. У профілі функціональності системи ризик у системі інтерпретується як загальне зниження критичної функціональності, а кіберрезильєнтність системи пов'язана з нахилом кривої поглинання та формою кривої відновлення, рис. 1, що вказує на часовий вплив деструктивної дії на систему. Пунктирна лінія свідчить про те, що високорезильєнтні системи можуть адаптуватися таким чином, що функціональність системи може покращитися відносно початкової функціональності, підвищуючи кіберрезильєнтність системи до майбутніх деструктивних дій.

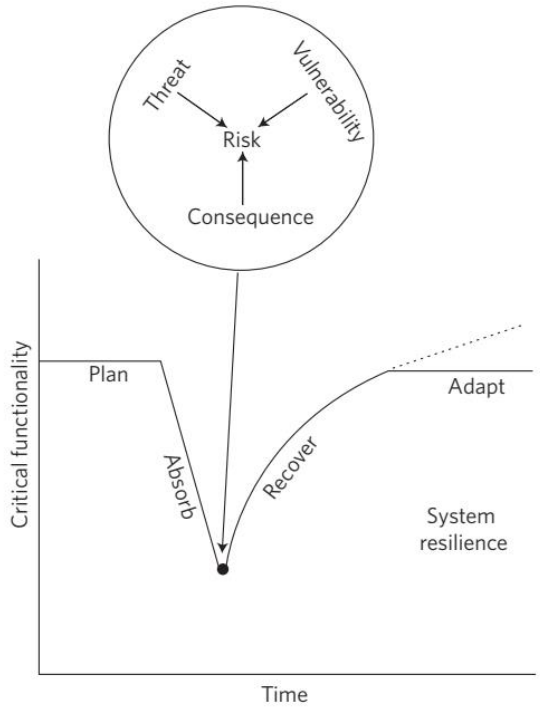


Рисунок 1 – Аналіз ризиків в структурі резильєнтності [5]

Аналіз ризиків кількісно визначає ймовірність того, що система досягне найнижчої точки критичного функціонального профілю. Управління ризиками допомагає системі підготуватися та спланувати несприятливі події, тоді як кіберрезильєнтність інтегрує здатність системи поглинати деструктивні дії та відновлюватися після них, а потім адаптуватися (рис. 1). Кіберрезильєнтність не є заміною управління ризиками, а являється додатковим атрибутом, який використовує стратегії адаптації та пом'якшення для покращення традиційного управління ризиками.

Схематичні зображення змін у критичних функціях з часом, рис. 2, показують взаємодію ризику та стійкості в роботі системи під час деструктивної дії. Розмір початкового збурення відображає загальний ризик для системи, тоді як форма кривої відновлення визначається кіберрезильєнтністю системи. Площа під кривою вказує на загальну функціональність системи. Системи, які стикаються з високими ризиками з високою стійкістю, працюють краще, ніж ті, які стикаються з подібними ризиками, але з низькою стійкістю. Системи з низьким ризиком, але також низькою стійкістю можуть працювати так само, або, можливо, гірше, ніж системи з високим ризиком і високою стійкістю.

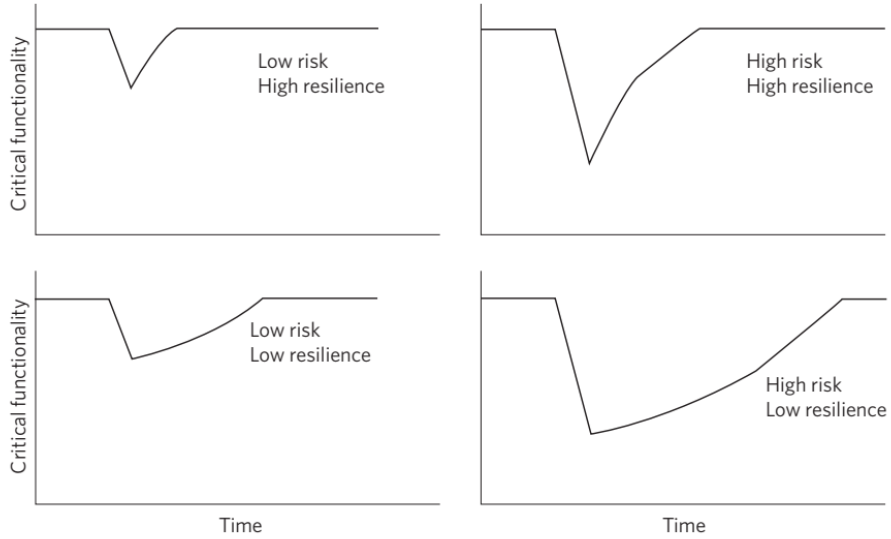


Рисунок 2 – Схематичні зображення взаємодії ризику та резильєнтності [5]

1. Гончар С.Ф. Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2019. – Т.30(69). Ч.1. – №4. – С. 40-44.
2. Kott, A. and Linkov, I., 2021. To Improve Cyber Resilience, Measure It. IEEE Computer, 54(2), Feb.2021, pp.80-85.
3. Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : автореф. дис. ... докт. техн. наук : спец. 05.13.21. Київ, 2020. 38 с.
4. A. Kott and I. Linkov, eds., Cyber Resilience of Systems and Networks. Cham, Switzerland: Springer, 2019.
5. Linkov, I., T. Bridges and others, 2014. Changing the resilience paradigm, Nature Climate Change, 4(6), June 2014, pp.407-409.

M.V. Prazian

CYBERSECURITY AND RESILIENCE: INTEGRATING HUMAN FACTORS INTO CRITICAL SYSTEMS

Human errors [1] account for approximately 90% of cyber breaches, underscoring their significant impact on organizational security. These mistakes stem from cognitive biases, heuristics, attitudes, and a lack of training among end users, which create vulnerabilities that malicious actors can exploit. The ongoing war in Ukraine has provided numerous lessons regarding human errors. Human factors are often out of focus; however,[2] industrial accident data reveal that 60%-90% of incidents arise from human error. Researchers cite several high-profile disasters from the late 20th century, including the 1979 Three-Mile Island nuclear accident in the USA, the 1984 Bhopal disaster in India, the 1986 Chernobyl catastrophe in Ukraine, and the 1988 Piper Alpha explosion and fire in the North Sea.The human and organizational elements [3]that contributed to the Challenger and Titanic incidents stem from failures in organizational leadership.

Technical failure issues often lead to significant, albeit less severe, problems. Regarding severity, approximately 40% were linked to organizational factors, 40% to human factors, and 20% to technical factors. For near-miss events, the severity percentages shifted to 22% for organizational technical characteristics, while human factors accounted for 55% [4]. How organizations handle errors and accidents depends on their culture. Ron Westrum [5] defines three general categories of safety culture: pathological (power-oriented), bureaucratic (rule-oriented), and generative (performance-oriented). Pathological organizations are characterized by significant amounts of fear and threat; they seek out the 'responsible' for the problem and punish them accordingly. Accidents seldom result from the actions of a single individual or group; instead, they arise from a complex interaction of various contributing factors [6]. Thus, 'human errors' should be explored further to identify better operational tools that prevent catastrophic failures [7]. A complex error-prone system promotes open discussions about mistakes, leading to a shift from blameless reporting to learning and analysis. This approach represents one of the modern organizational strategies [8]. Integrating human factors into operational resilience modeling for critical infrastructure [9] involves considering frameworks, dynamic models, and human error occurrence and propagation analyses. This study adopts a time- and process-centered approach to maintenance, decision-making, and policy, viewed through the lens of human performance. The resilience of critical systems due to human-machine interfaces has become more achievable and nuanced through the integration of the prepare, absorb, recover, and adapt phases [10].

Two primary gaps include the diverse dynamics of human-systems modeling across various infrastructures and countries, along with the challenges associated with developing modeling frameworks and collecting data. Exploring the human factors taxonomy [11], along with critical systems such as ISO 9241-210:2019, Ergonomics of human-system interaction — Part 210[12], and NIST-like standards, appears to be a beneficial approach for applying these concepts to underdeveloped critical systems. The "Lessons Learned" approach has a long and mature history[13] and is recommended for maintaining and enhancing critical system resilience and recovery. As part of a formal approach, it incorporates human factors, data, metrics, models, and human-machine systems for various critical infrastructure scenarios. The 'Lessons Learned' method consists of two phases: Analysis and Implementation. For example, human-centered guidance, as outlined in NASA's Human System Integration (HSI) [14] and the FAA's dynamic regulatory system [15], can serve as valuable tools within the systems engineering framework.

Conclusions: To err is human. Thus, 'human errors' are not always dramatic but can have severe repercussions. Minimizing mistakes should start at the organizational culture level and involve implementing systematic measures to enhance preventability, reducing uncertainty regarding basic, complex, and intelligent failures. Unequal development across different critical infrastructure components indicates both gaps and opportunities. The latter can arise from transmitting and adapting the best ongoing and prospective tools for lagging sectors. Integrating human factors into critical systems should include a comprehensive suite of psychological safety measures, operational tools, and standards. The levels of adaptation and development of human factors vary across critical systems, including digital, energy, transportation, aviation, industry, food, buildings, healthcare, finance, and education. This variation is supported by the 'Lessons Learned' approach, ISO standards, and NIST guidelines.

1. Calvin Nobles, Anuradha Rangarajan, & Darrell Burrell. (2025). Human Factors Engineering- as-a-Service in Cybersecurity. IGI Global Scientific Publishing, 29. https://doi.org/DOI: 10.4018/979-8-3693-6437-6.ch014.
2. Yalçın, E., Ciftcioglu, G., & Güzel, B. (2024). Human reliability analysis methods. Pamukkale University Journal of Engineering Sciences, 30, 282–292. https://doi.org/10.5505/pajes.2023.33958.
3. Ferguson, N. (2021). Doom: The Politics of Catastrophe. Penguin Press. https://www.amazon.com/Doom-PoliticsCatastrophe-Niall-Ferguson/dp/0593297377.
4. Battles, J. (2001). Disaster Prevention: Lessons Learned from the Titanic. Proceedings (Baylor University. Medical Center), 14, 150–153. https://doi.org/10.1080/08998280.2001.11927752.
5. Westrum Ron. (2014). The study of information flow: A personal journey. Safety Science, 67, 58–63. https://doi.org/DOI: 10.1016/j.ssci.2014.01.009.
6. Perrow Charles. (2011). Normal Accidents: Living with High-Risk Technologies (Updated Edition). Princeton University Press. https://doi.org/10.2307/j.ctt7srgf.

7. Nicole Forsgren, Jez Humble, & Gene Kim. (2018). Accelerate: The Science of Lean Software and DevOps: Building and Scaling High-Performing Technology Organizations (Illustrated edition). IT Revolution Press.
8. Edmondson Amy. (2023). Right Kind of Wrong: Why Learning to Fail Can Teach Us to Thrive. Penguin. https://www.amazon.com/Right-Kind-Wrong-Learning-Thrive-ebook/dp/B0BW3DDXY6.
9. Magoua, J., Wang, F., Li, N., & Fang, D. (2023). Incorporating the human factor in modeling the operational resilience of interdependent infrastructure systems. Automation in Construction, 149, 104789. https://doi.org/10.1016/j.autcon.2023.104789.
10. B.D.Trump, K. Poinsatte-Jones, M. Elran, C. Allen, B. Srdjevic, M. Merad, D. M. Vasovic, & J. M. Palma-Oliveira. (2017). Social Resilience and Critical Infrastructure Systems. Resilience and Risk, 289. https://doi.org/10.1007/978-94-024-1123-2_9.
11. Stroeve, S., Kirwan, B., Turan, O., Kurt, R. E., van Doorn, B., Save, L., Jonk, P., Navas de Maya, B., Kilner, A., Verhoeven, R., Farag, Y. B. A., Demiral, A., Bettignies-Thiebaux, B., de Wolff, L., de Vries, V., Ahn, S. I., & Pozzi, S. (2023). SHIELD Human Factors Taxonomy and Database for Learning from Aviation and Maritime Safety Occurrences. Safety, 9(1), 14. https://doi.org/10.3390/safety9010014.
12. ISO/IEC. (2010). ISO 9241-210:2010(en), Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems. https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en.
13. JALLC. (2022). The NATO Lessons Learned Handbook (Fourth Edition). NATO, Joint Analysis and Lessons Learned Centre. https://www.jallc.nato.int/organization/products/books-guides.
14. Jennifer Rochlis Zumbado. (2015, November 1). Human Systems Integration (HSI) Practitioner's Guide. Lyndon B. Johnson Space Center, Houston, Texas 77058. https://ntrs.nasa.gov/citations/20150022283.
15. FAA. (2019). Dynamic Regulatory System (Advisory Circulars (AC) AC 00-74). AIR-626B: Avionics Navigation & Flight Deck. https://drs.faa.gov/browse/excelExternalWindow/A4D589578F6CE6B1862583EF004C31A7.0001?modalOpened=true.

USING THE ARTIFICIAL INTELLECTUAL TO REMOTE SENSING AND SPATIAL INFORMATION PROCESSING FOR A PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE FACILITIES

Abstract: Methods for creating intelligent information systems for remote sensing and processing of spatial information from a large area in the energy sector, which adapt to a complex radio frequency environment based on the technology of the cognitive minimization method in a distributed sensor system based on a neurocomputer with a deep learning function, which is reconfigured in real time, depending on the complexity of the input information, are considered. A distributed system created according to this principle allows for remote capture of information about a spatial object on the ground, interference, and provides the possibility of real-time reconfiguration of the receiving path, reducing the impact of interference by using dynamic algorithms for digital signal processing that change during operation. Typical machine learning models, such as regression models and tree-based algorithms, are used for training. It is shown that they have a good compromise between prediction accuracy, ease of implementation, training, and explanation. We adapt a more general definition of anomaly. [1]

Keywords: Smart-Handled Radar, LPI (Low Probability of Intercept) Radar, CFAR (Constant False Alarm Rate), IoT (internet of things), artificial Intelligence, Deep learning, Signal processor, Signal-to-Noise Ratio (SNR), adaptive antenna arrays with time modulation.

1. Introduction

Intelligent remote sensing systems for capturing and processing spatial information from a large area in the energy sector require greater mobility, stealth, and sensitivity to ensure the reception of desired signals and the effective reduction of unwanted ones, in which the sensor part or antenna systems play a crucial role. The correct combination of antenna characteristics and signal processing allows for effective operation in the spatial, frequency, and time domains.

The main goal of intelligent information collection networks supported by a sensor network is the reliability of obtaining reliable information in real time. Research into new sensor network technologies is aimed at developing intelligent antennas with low loss, adaptive beamforming. Such intelligent antenna technology must take into account the complexity of information collection sensors. In addition, antenna devices associated with sensor networks are capable of receiving the external electromagnetic environment, thereby correctly reconfiguring the radiation characteristics of the generated field.

Design of a sensor system for collecting and processing spatial information for the needs of the energy industry.

The innovative idea of using time as an additional degree of freedom to control the antenna pattern is taken as a basis. In fact, multi-antenna methods are considered for using spatial diversity, multiplexing and beamforming, achieving a high level of reliability and throughput. The concept of time-modulated arrays (TMA) of multi-antenna devices significantly simplifies the equipment. TMAs are electromagnetic systems with a radiation pattern that is controlled by applying periodic pulses of variable width to individual elements. The nonlinear nature of the antenna array operation leads to the appearance of radiation patterns at harmonic frequencies of such periodic pulses. Among the latter, the formation of a harmonic radiation pattern of TMA is of particular importance due to the attractive compromise between performance and equipment complexity. From this point of view, TMAs are sensors capable of converting the spatial diversity of a communication channel into frequency diversity.

TMAs, in their simplest configuration, are antenna arrays whose radiated power patterns are controlled by periodically turning on and off the excitation of individual elements of the array. The hardware implementation of TMAs is greatly simplified, since they can be implemented using switches, rather than the complex multiplication of weighting factors, as in conventional arrays.

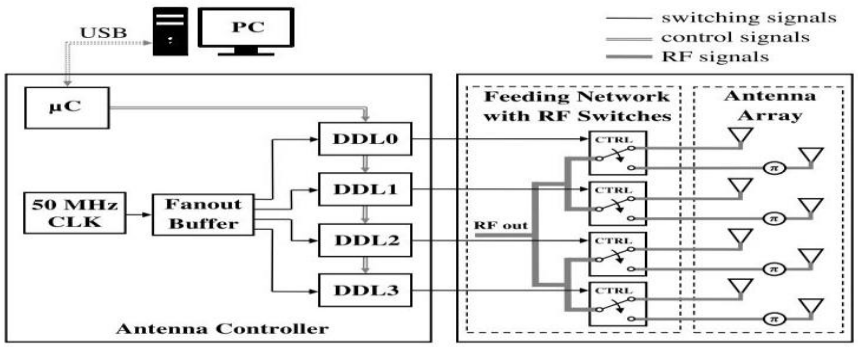


Figure 1 – TMA system including antenna array with switches, antenna controllers and adaptive algorithm implementation node

The spectrum of the time-modulated signal at the output of each time-modulated element E can also be obtained from:

$$Yn = Sn * Mn \quad (1)$$

where (*) denotes the convolution operator,

and Sn and Mn are sets of Fourier series coefficients of the received signal.

The first term in equation (1) is the diffraction factor at the fundamental mode frequency (q =0; q=0) fc fc, which shows that we can tune the magnitude of the excitations exclusively by using the normalized pulse durations ξnξn, and the second term in equation (1) shows the existence of side-lobe radiation (SB) at frequencies $fc + qf$, 0fc+qf0 (harmonics) on the other hand. By varying ξnξn and/or n on, we can also control the radiation pattern at each side-lobe harmonic, in this case having the possibility to tune the magnitude and phase of the excitations simultaneously. SR can either be minimized or, as explained in the following sections, used to advantage.

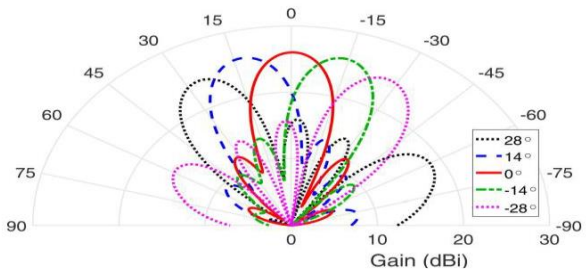


Figure 2 – TMA configuration showing the four parts of the radiation pattern,
the direction of the desired and unwanted transmitter

Applying periodic pulses to different antennas results in the conversion of spatial diversity into frequency diversity, and thus, a single RF input stage is sufficient to utilize such spatial diversity. Adaptation occurs both in the transmit and receive paths. This occurs after measuring one of three parameters:

1. Signal-to-noise and interference ratio (SINR);
2. Bit error rate (BER);
3. RSSI (Received Signal Strength Indicator) input signal level.

Then we select the signal parameters required for the receiver. To ensure maximum quality, the SNR (signal-to-noise ratio) level should be as high as possible, and the BER should be as low as possible.

Adaptation during RF scanning is ensured by:

- switching to optimal frequencies;
- changing the radiation power;
- switching of used antennas;
- automatic connection establishment (i.e. receiving the reflected signal);
- network organization capability;
- QoS measures the state of the sensing and receiving channels.

Cognitive radar networks (CRNs) extend the capabilities of autonomous cognitive radar in the field by providing the ability to observe targets from multiple perspectives to reduce the effect of stealth; allocate resources in space and time; obtain the best tracking performance; and obtain more information from the scene. Recognition problems in CRNs are often viewed through the lens of iterative learning tasks - the network implements one or more cognitive processes, where each process first observes the environment, then selects operating parameters (from discrete or continuous options) using the observation history and previous rewards, and then the cycle repeats. In addition, cognitive radar networks are often implemented with flexible architectures and wide-bandwidth external interfaces, which allows the addition of electronic auxiliary measures, such as passive signal estimation.

In addition to all these applications, tools have also been developed for more precise analysis of TMAs. In this sense, and to assess some nonlinear aspects of TMA operation as radiating systems (e.g., the effect of mutual coupling between elements), Masotti et al. The paper addresses the full-wave calculation of the radiated far field by properly developing a multi-domain automated design platform.

Adaptive beamforming was first investigated from a practical and simplified point of view focusing on the synthesis of harmonic patterns.

Multi-beam characteristics of TMAs have also been proposed for spatial multiplexing by Y. Yashchyshyn et al [2]., although the performance with broadband signals has not been analyzed. Recent work has focused on the development of TMA hardware, which is used for spatial filtering of signals and for interference suppression in the millimeter range.

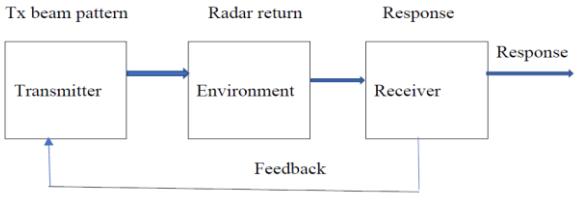


Figure 3 – Block diagram illustrating a continuous-time version of the system under study, in which a linearly modulated digital signal s(t) is first generated using an in-phase and quadrature modulator on the carrier fc, and then s(t) is radiated through the TMA

Biomimetic methods have been used to construct radar systems based on neural network technologies, the cognitive nature of which is their feature. That is, the external environment affects the operation of the radar and, in turn, the radar forms a probing signal, taking into account environmental indicators [3].

A cognitive radar contains a global feedback channel that rapidly scans the environment electronically and uses the capabilities of digital signal processing. The basic cognitive cycle begins with the illumination of the radar environment by the transmitter. The radar information contains data about spatial targets. The receiver continuously reads the radar environment, interacting with it to obtain the necessary information about the target and its interception. This information is sent in the reverse direction from the receiver to the transmitter of the phased array cognitive radar (PAR) with low probability of interception (LPI).

The effectiveness of the radar recognition system as a whole depends directly on the efficiency of the technical means and its mathematical support - software-implemented algorithms for constructing descriptions of classes of objects and phenomena in sign language. The obtained radar information is divided into groups of similar but not identical phenomena. We create a radar image of the object against the background of distorted information in real conditions. The characteristic property of the images is manifested in the fact that after getting acquainted with the finite number of manifestations of the object, we learn about any number of its representatives. Also, when teaching a radar neurocomputer (rebuilding multiprocessor) at different observation sites, the same objects are classified equally and independently of each other. The objective nature of the basic property of the images allows us to model the recognition process.

As a result of deep learning, the recognition system acquires the ability to respond with the same reactions to all objects of the same image and different - to all objects of different images. It is very important that the learning process be completed only by displaying a finite number of objects, without any “clues” [4].

The objects of training are radar objects, interference, radar specifications. It is also important that only the objects themselves and their affiliation with the image are indicated in the learning process. The training is followed by the process of recognizing new objects, which characterizes the actions of the already learned system. Automation of these procedures is a problem of pattern recognition training.

The most comprehensible to us is the spatial-temporal interpretation of tasks. Hence the problem of learning pattern recognition has received its geometric (spatial) and temporal (dynamic) interpretation. Any radar image resulting from the observation of an object in the course of training or testing can be represented as a vector, and hence as a point of some space.

If it is claimed that radar images can be uniquely assigned to one of two (or more) images, then it is claimed that in some space there are two (or more) areas that have no common points, and the images shown are points from these areas. Each such area can be assigned a name, that is, give a name to the corresponding image.

During deep training, points randomly selected from these areas are presented and information is given to which area these points belong. No additional information about these areas, ie the location of their borders, is reported during the training.

The purpose of the training is either to construct a surface that separates not only the points shown in the learning process, but all other points belonging to these areas, or the construction of surfaces that limit these areas of points so that each of them is only one point insult. That is, deep learning is about constructing such features from image vectors that would be, for example, positive at all points of one and negative at points of another image.

Due to the fact that the areas do not have common points, there is always a whole lot of such separating functions, and as a result of training one of them must be built. If the displayed images do not belong to two, but to a larger number of images, then the task is to build on the points shown in the course of training, separating all the areas corresponding to these images from each other. This problem can be solved, for example, by constructing a function that takes over the points of each area the same value and the points over the different areas different.

A deep learning mechanism is used to build the CFAR function. First of all, we solve the problems of object classification. Let there be some set of investigated objects $\Omega = \{\omega\}$, each of which is determined by the vector of its values in the phase space of some m given signs:

$$\omega_1 \to \bar{x}^1 = \{x_1^1, x_2^1, \ldots, x_m^1\};$$
$$\omega_2 \to \bar{x}^2 = \{x_1^2, x_2^2, \ldots, x_m^2\};$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;$$
$$\omega_t \to \bar{x}^t = \{x_1^t, x_2^t, \ldots, x_m^t\}\ .$$

We divide objects into homogeneous classes (their number can be specified or may be unknown), which we call clusters, and methods for finding them - by cluster analysis. There is no training sample in this case, that is, it is unknown to which classes the objects in the set belong $\Omega = \{\omega\}$. We define patterns of structure of objects in clusters. In particular, a "compactness hypothesis" can be used as a similar pattern, ie the requirement that objects belonging to the corresponding classes be located in a given characteristic space $\bar{x} = \{x_1, x_2, \ldots, x_m\}$ "compactly". This means that the "distance" between objects assigned to this class is no more than specified.

Other requirements may be formulated in the automatic classification, namely, the generated classes in the sign space must be spaced apart at certain distances. Essentially, with the help of a multidimensional function defined on an arbitrary grid, we construct some sign or a generalized image of a class, by which one can uniquely determine the belonging to one of two points of a point in the phase space of measurements of the values of some predefined features.

To separate the sets of points of two different visions, we use hyperplanes or their sets, but only if the sets of points of the visions are so far apart in the phase space of the signs that a separating hyperplane can be constructed between them. When this is not present, then we move on to a new signs space. As a rule, we are going to add new signs to existing ones and to increase the dimension space of the signs space. In this case, to obtain a guarantee of separation reliability, it is necessary to significantly add the number of training sample points.

The main task of training is not to keep all the available information about the object, but to minimize the irrelevant, highlight the most informative and leave only the essential, that is, what can only be called information about the object, not just a random set of data. Sets of image points can also be reliably separated in spaces with fewer features when the surfaces of the sets are of rather complex configuration and do not intersect. For this case, we write an algorithm for constructing a separating hypersurface in the form of a multidimensional function defined on an arbitrary grid. But first, let's write an algorithm for determining a multidimensional function on an arbitrary grid, which we will use to construct the function itself. To do this, we:

1) We set the points of the grid of ordinates in the multidimensional coordinate space - the number of these points and the values of the coordinate vector of each point;

2) Determine the values of the parameters for all components: Green's function for solving the wave equation from grid points plus elements of the polynomial kernel.[5]

Let some arbitrary grid of ordinates $\overline{P}$ be given in the form:

$\overline{P} = (P^{(1)}, P^{(2)}, \ldots, P^{(N)})$ the system of randomly arranged at R^n different unique points is given in the form:

$$P^{(k)} = (P_1^{(k)}, \ldots, P_n^{(k)}) \in R^n,\ k = \overline{1, N}$$

Define as follows on the grid $\overline{P}$ a multidimensional function $\sigma(\overline{P}; \overline{\lambda}; P)$, which at points of the grid takes some already set values: $r_i,\ i = \overline{1, N}$:

$$\sigma(\overline{P}; \overline{\lambda}; P^{(i)}) = r_i,\ i = \overline{1, N}, \tag{1}$$

and has a simple look - as a sum of some functions:

$$\sigma(\overline{P}; \overline{\lambda}; P) = \sum_{i=1}^{N} \lambda_i G_{m,n}(P - P^{(i)}) + \sum_{|\alpha| \le m-1} \nu_\alpha P^\alpha\ , \tag{2}$$

where $P^\alpha = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \ldots \cdot P_n^{\alpha_n}, P^* = (P_1, \ldots, P_n),\ P_k^{\alpha_k}$; k - coordinate in α_k - degree,

$\sum_{|\alpha| \le m-1}$ - the sum of all possible combinations: when $\alpha = 0$ - is the free ratio,

When $\alpha = 1$ - this is a free coefficient + components in linear form $\nu_0 + \sum_{k=1}^{n} \nu_k P_k$,

at $\alpha = 2$ - sum at $\alpha = 1$ + components at quadratic form $\sum_{k=1}^{n} \sum_{l=1}^{n} \nu_{kl} P_k P_l$ іт.д.,

(total $\frac{(n+m-1)!}{n!(m-1)!}$ components);

$$G_{m,n}(x-P) = \begin{cases} \|x-P\|^{2m-n} \ln\|x-P\|, n = 2k \\ \|x-P\|^{2m-n}, n = 2k-1 \end{cases},$$

$\|x-P\| = [\sum_{i=1}^{n} (x_i - P_i)^2]^{\frac{1}{2}}$, $P = (P_1, P_2, ..., P_n)^*$, $x = (x_1, x_2, ..., x_n)^*$.

The continuity of Green's $G_{m,n}(x-P)$ functions requires that the condition $m > n/2$ be satisfied. By summarizing the variation theory of constructing multidimensional functions on a chaotic grid to simple algebraic conditions, we can consider finding the coefficients of a multidimensional function as a solution of some system of linear equations. To do this, we simply introduce a continuous linear indexing for the coefficients ν of formula (2). Then we find the values of the coefficients $\lambda_i, i = \overline{1, N}$ and $\nu_l, l = \overline{1, \vartheta}$,

where $\vartheta = C_n^m = \frac{(n+m-1)!}{n!(m-1)!}$, by solving two algebraic conditions:

and, where $\vartheta = C_n^m = \frac{(n+m-1)!}{n!(m-1)!}$ to solve two algebraic conditions:

1) coincidence of values of multidimensional - function at given points $\overline{P}$ (1);
2) and the orthogonality of the polynomial kernel functions at each other at the same points.
In matrix form it has the following generalized form:

$$C \cdot \overline{\lambda} = \overline{r},$$

where the matrix C has dimension $(N+\vartheta) \times (N+\vartheta)$, or $\overline{\lambda} = (\lambda_1, \lambda_2, ..., \lambda_N, \nu_1, \nu_2, ..., \nu_\vartheta)^*$, $\overline{r} = (r_1, r_2, ..., r_N, 0, 0, ..., 0)^*$ - vectors of dimension $N + \vartheta$ each, $*$ - is the sign of transposition, $P^{(i)} = (x_1, x_2, ..., x_n)^*$, $i = \overline{1, N}$.

For the system to have a solution, a condition is required $N \geq \vartheta$. Consider constructing a separating hypersurface in the form of a multidimensional function defined on an arbitrary grid. Suppose two sets of m - measurable points X and Y with the number of points M and L respectively:

$$X = \{\overline{x}^1, \overline{x}^2, ..., \overline{x}^M\}, Y = \{\overline{y}^1, \overline{y}^2, ..., \overline{y}^N\},$$

where $\overline{x}^i = \{x_1^i, x_2^i, \ldots, x_m^i\}$, $i = \overline{1, M}$, $\overline{y}^i = \{y_1^i, y_2^i, \ldots, y_m^i\}$, $i = \overline{1, L}$.

We find a multidimensional function on an arbitrary grid that can sufficiently reliably divide sets of points X and Y, that is, divide into two intersecting regions by two sets in some multidimensional space of phase features, which are initially represented as two arbitrary sets of multidimensional points. The automatic construction of such a rule is the algorithm of machine learning. This is achieved by constructing a surface that separates not only the points shown in the learning process, but also all other points belonging to these areas [6].

To construct a multidimensional function on an arbitrary grid, we define a grid $\overline{P}$ ofNn - dimensional points and the values of the function in them $r_i, i = \overline{1, N}$. Due to the fact that we have not determined the direction from which to build the separating hypersurface, we have the opportunity to do so in the direction of each of the *m* coordinates. To do this, we use the value of one of the **m** coordinates as the value of a multidimensional function, and we use all other *(m-1)* coordinates as the values of points to determine the grid of ordinates with the dimension n = (m-1). With this approach, there are only **m** options for constructing a multidimensional function on an arbitrary grid. In addition, it can be built both from the side of the set X, checking for Y and vice versa. You can also try moving around the points of one set, searching for the closest points of the other and finding some averages and already, on them to look for a

hypersurface. In total, we have at least 2m + 1 options for constructing a multidimensional function of which we choose the most acceptable.

Conclusions

As a result of the study of intelligent remote sensing systems and spatial information processing in energy, results were obtained on the formalization of the antenna system as an information system. A historical excursion of research in this field was made, which showed that all research aimed at improving the antenna system itself does not meet modern requirements, which have low visibility, transience, and maneuverability. Therefore, we proposed to introduce calculations into the process of information capture itself, which allows us to detect objects and classify them. Issues of visibility, cognition, fault tolerance, and warranty are laid at the stage of forming the technical task.

TMA is developed for broadband signals [7]. It is proposed to form a beam using a preliminary Fourier transform of periodic pulses in the frequency domain - this is a discrete spectrum with pulses that are multiples of the time modulation frequency, the corresponding areas of which are 2 times larger than the corresponding coefficients of the exponential Fourier series. Research on TMAs is aimed at studying their properties and formalizing qualitative and quantitative characteristics depending on the antenna synthesis criteria [8].

1. G Stamatescu, R Entezari, K Römer, O Saukh. Deep and efficient impact models for edge characterization and control of energy events. 2019 IEEE 25th International Conference on Parallel and Distributed Systems.
2. Y. Yashchyshyn, J. Marczewski, K. Derzakowski, J. Modelski, and P. Grabiec, “Development and investigation of an antenna system with reconfigurable aperture,” IEEE Trans. Antennas Propag., vol.57, no. 1, pp. 2–8, Mar. 2009.
3. O Saukh. Embedded Sensing Systems: Design, Models, Algorithms, and Applications. Graz University of Technology.
4. Kosovets M., Tovstenko L.The practical aspect of using the artificial intellectual technology for building a multidimensional function CFAR for smart-handled LPI Radar. Magazine "Programming Problems". ISSN 1727-4907. 2020. No. 2-3. Special issue. Proceedings of the thirteenth international scientific-practical conference on PROGRAMMING. UkrPROG'2020. September 16-17, 2020 Kyiv, Ukraine. Pages 202 - 212. http://www.pp.isofts.kiev.ua.
5. M Keller, J Beutel, O Saukh, L Thiele. Visualizing large sensor network data sets in space and time with vizzly. 37th Annual IEEE Conference on Local Computer Networks-Workshops, 925-933.
6. D Hasenfratz, O Saukh, L Thiele. Model-driven accuracy bounds for noisy sensor readings. 2013 IEEE International Conference on Distributed Computing in Sensor. Bottom of Form.
7. D. Masotti, A. Costanzo, MD Prete, and V. Rizzoli, “Time-modulation of linear arrays for real-time reconfigurable wireless power transmission,” IEEE Trans. Microwave. Theory Techn., vol. 64, no. 2, pp. 331–342, Feb. 2016.
8. G. Bogdan and Y. Yashchyshyn, “Experimental study of signal reception by means of time-modulated antenna array,” in 21st Int. Conf. Microwave. Radar Wireless Commun. (MIKON), Krakow, Poland, May 2016, pp. 1–4.

F. Korobeynikov

SYNERGISTIC PRINCIPLES FOR BUILDINGA RESILIENT NATIONAL ENERGY SYSTEM

Risk analysis, a methodological approach that first appeared in the early 20th century, during a time of predictability and linear thinking, is the foundation of the current paradigm for guaranteeing the security of national energy systems. However, this paradigm is becoming dangerous as well as ineffective in the current environment of global crises, systemic uncertainty and interdependence, and stochastic risks because it is deceptive and gives the appearance of control and security in an environment where chaos, non-linearity, and threshold effects are prevalent. State energy system is not symply a mechanism or a collection of related mechanisms. Like the state overall, the energy system is a complex, open, evolving, nonlinear, and dissipative system whose behavior is dictated by the laws of self-organization and dynamic adaptation rather than by the sum of its parts.

The works of Ilya Prigogine on the behaviour of non-equilibrium systems, research by scientists from the Santa Fe Institute, such as Murray Gell-Mann, John Holland, Stuart Kauffman, as well as the works of Gregory Bateson and Herman Haken, have convincingly shown that in such systems, resilience and survival cannot be ensured through strict control or deliberate isolation of the system from fluctuations. On the contrary, isolation is harmful — it is extremely important to ensure conditions for the manifestation of the internal properties of such systems: self-organisation, autopoiesis, and adaptability. This requires a shift from a strategy of protection to adaptation engineering, from attempts to predict and prevent all risks to the formation of systems capable of transforming themselves in conditions of uncertainty. This is the essence of the principles of adaptive security.

According to the proposed methodology, the first step in building a resilient energy architecture for a state should be to identify system invariants – fundamental ontological properties of the system, those characteristics that must be preserved to maintain the identity and integrity of the system even under conditions of radical changes in the environment or its structure. In the context of a nation state, the source of such invariants is its founding normative act – the Constitution.

"The human being, his or her life and health, honour and dignity, inviolability and security are recognised in Ukraine as the highest social value" according to Article 3 of the Ukrainian Constitution. The context is further enhanced by Article 13, which states that "the land, its mineral wealth, atmosphere, water and other natural resources within the territory of Ukraine... are objects of property rights of the Ukrainian people." The ontological essence of the state as a system that exists primarily to ensure the security and well-being of its citizens can and should be interpreted as being indicated and emphasized by these provisions.

When it comes to a country's energy system, this means that people's access to electricity shouldn't be seen as a side effect of the government's goals, market efficiency, or, say, tech optimisation, but as a constant system invariant — a critical component that needs to be protected and preserved no matter what's going on outside or inside the country. This understanding fundamentally changes the logic of energy system and security system design, shifting from optimisation for state profit to an architecture capable of supporting basic functions that are important to citizens in times of stress, disruption and transformation.

The next conceptual step in building a resilient energy system is to recognize the fundamental role of self-organization and adaptation - processes that underlie the functioning of all complex nonlinear systems. According to Ilya Prigogine, open dissipative systems in a state of disequilibrium have the ability to spontaneously organize new structures in response to environmental fluctuations [1]. Research by Stuart Kauffman at the Santa Fe Institute has shown that the key mechanism of resilience in complex adaptive systems is the ability to self-organize without external directive control [2]. A similar line of thought was developed by Haken in his theory of synergetics, which views control parameters as triggers for structural reorganizations occurring within the system [3].

These scientific concepts allow us to formulate a key management principle: the main function of the state in matters of energy security in conditions of uncertainty is not directive control or an attempt to centralize all processes, but rather the creation of conditions for the internal self-organization of the system. This means stimulating adaptation processes, maintaining diversity of components, and developing flexibility and the ability to reorganize under pressure from external and internal shocks. An energy system operating according to this logic approaches a state of autopoiesis - the ability not only to maintain itself as a whole, but also to autonomously restructure and reproduce itself in response to changes in the environment [4]. Thus, the task of public policy is not so much to build a system as to create conditions under which it can build itself.

The institutional framework required to guarantee adaptive energy security is already in place in modern states. Correctly modifying the interactions of current structures based on a scientifically sound approach that can coordinate their efforts into a single, emergent sustainability strategy is more important than developing new ones. The logic of hierarchical management precludes such coordination, but the synergy principles found in complex systems theory make it possible. The goal of the synergistic approach is to improve nonlinear effects like self-organization, adaptation, collective efficiency, and the expansion of the system's reserve of sustainability by coordinating actions rather than adding them up.

A clear illustration of this is the mass purchase of backup power sources by Ukrainian citizens in 2022–2025: solar panels, wind turbines, fuel and hybrid generators, and energy storage systems. These actions were an intuitive manifestation of the autopoiesis of the socio-technical system, a reaction to the threat of blackouts. However, the lack of systematic state support led to fragmented and inefficient use of the potential of these solutions. Wind energy was introduced in areas with low wind speeds, and panels were installed without calculating the angle of insolation or conducting an energy audit.

The solution lies in launching a National Energy Resilience Program, which should be led not by bureaucrats, but by scientific and engineering communities: scientists, logisticians, designers, and engineers. The program should offer citizens expert opinions on the effectiveness of specific technologies, professional installation and maintenance of energy systems adapted to regional and local conditions. The mechanism should be synergistic: the state provides preferential loans, and citizens return not money, but a portion (for example, 25%) of the energy generated to the general power grid. Thus, what happens is not simply decentralization, but the formation of a horizontal energy network with a high level of adaptability, modularity, and resilience.

This approach can simultaneously solve the problems of social justice, energy security, and technological modernization within the framework of a unified evolutionary logic of a self-organizing state.

At the initial stage, when the state does not yet have its own production base for highly efficient energy solutions, intellectual technology transfer becomes an important element of the synergistic strategy. Instead of uncoordinated imports and chaotic purchases, the state should centrally search for and acquire the most efficient models of energy plants -solar, wind, hybrid - from countries that have already achieved technological maturity in these areas. Centralized wholesale procurement will not only significantly reduce the cost of equipment for citizens, but also standardize technical components, simplifying logistics, support, and training of technical personnel.

However, this should not simply involve using other countries' products and technologies, but rather the strategic adoption of global best practices with a view to subsequently transitioning to a sovereign technological cycle. Using accumulated data, engineering expertise, and statistics on the operation of installations in various climatic and infrastructural conditions, the state should initiate the launch of its own production facilities. This will not only strengthen energy independence, but also give a powerful impetus to the development of national science, engineering, and industry, increase employment, investment attractiveness, and strengthen the country's geopolitical position as a bearer of technological sovereignty.

In the context of energy turbulence and global transformation of the energy landscape, the search for new prototypes, technological solutions, and materials should become a matter of national strategy. To this end, it is advisable to leverage the intellectual resources of the intelligence community, redirecting them toward global monitoring of scientific and technological developments, start-ups, and laboratory initiatives related to the energy of the future. In this way, the energy resilience framework will include not only engineers and logisticians, but also strategists, analysts, and intelligence officers - all those who are capable of transforming the flow of global innovation into a resource for national survival and revival.

The widespread adoption of autonomous generation sources among the population - whether solar panels, wind turbines, or hybrid microgrids - can not only ensure the resilience of the national energy system, but also create a strategic resource: a structural surplus of electricity. However, it is not advisable to simply convert this surplus into exports. Energy exports are a tactical measure. Real strategic transformation begins when surplus energy is used to increase added value within the country itself.

One area of this transformation should be the creation of high-energy data centers. These centers could become the foundation for neural networks, simulation models, platforms for decision-making in uncertain conditions, and the energy base for sovereign AI architectures. The development of advanced IT infrastructure stimulates the development of science - special attention should be paid to the construction of scientific and educational campuses where the intellectual capital of a new generation is formed - an elite capable of integrating technical knowledge with the philosophy of complexity and the ethics of development.

In this setup, energy resilience isn't just about getting "light and heat". It's the architectural framework for building a knowledge economy, strengthening national sovereignty, and leading the way in smart thinking. A synergistic added value effect arises when investments in the resilience of a single subsystem – energylead to exponential growth in the adaptive, technological, and cultural potential of the entire state system.

But no system, no matter how innovative and scientifically sound, can work in real life without the right institutional environment. Corruption and authoritarianism remain the main obstacles to building a truly adaptive and resilient energy architecture. These phenomena are not merely social flaws, but stable dynamic structures with all the characteristics of complex systems. In terms of non-equilibrium thermodynamics, they are dissipative formations that strive for local order - a reduction in their own entropyby increasing the entropy of their environment. They perceive the state, its institutions, and, ultimately, civil society as such an environment.

Similar to any intricate autopoietic system, corrupt and authoritarian systems frequently incorporate their own norms, priorities, descriptive languages, and decision-making processes into the state's governing framework. They substitute their own local cycles of power reproduction, rent extraction, and self-organization suppression for the objectives of society's survival and advancement. The state consequently degenerates and loses its capacity for adaptation. By viewing this phenomenon through the lens of complex systems theory, we are able to not only condemn corruption but also acknowledge it as a self-organizing entity that preys on the negentropy of citizens, thereby weakening the resilience of a larger and more important system: the state. Thus, combating corruption and authoritarianism is a systemic requirement for preserving entropic balance and guaranteeing the state's long-term adaptability rather than a moral catchphrase. It is not a question of ideology, but of survival.

1. Prigogine, I., &Stengers, I. (1984). Order out of chaos: Man's new dialogue with nature. Bantam Books.
2. Kauffman, S. A. (1993). The origins of order: Self-organization and selectionin evolution. Oxford University Press.
3. Haken, H. (1983). Synergetics: An introduction. Nonequilibrium phase transitionsand self-organization in physics, chemistry and biology (3rd ed.). Springer.
4. Maturana, H. R., &Varela, F. J. (1980). Autopoiesis and cognition: The realization of the living. D. Reidel Publishing.

С.С. Шевченко

МОДЕЛЮВАННЯ СЦЕНАРІЇВ КІБЕРАТАК В ІНТЕРАКТИВНИХ 3D-СЕРЕДОВИЩАХ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ПЕРСОНАЛУ ЕНЕРГЕТИЧНИХ ПІДПРИЄМСТВ

Сучасна енергетична галузь, як критична інфраструктура держави, все частіше стає об’єктом цілеспрямованих кібератак [1]. Складність технологічних процесів, високий ступінь автоматизації та взаємозв’язок систем управління (АСУ ТП) створюють численні вектори для потенційних кіберзагроз. Наслідки таких атак можуть бути катастрофічними, призводячи до масштабних відключень, економічних збитків та навіть техногенних аварій [2]. У цьому контексті, підготовка персоналу, здатного ефективно розпізнавати, реагувати та протидіяти кіберзагрозам, набуває першочергового значення.

Традиційні методи навчання, такі як лекції, інструктажі чи навіть аналіз теоретичних кейсів, часто виявляються недостатніми для формування стійких практичних навичок дій в умовах реального кіберінциденту [3]. Вони не дозволяють відчути динаміку атаки, відпрацювати послідовність дій в стресовій ситуації та побачити безпосередні наслідки прийнятих рішень. Для вирішення цієї проблеми пропонується використання інтерактивних 3D-середовищ, які дозволяють моделювати реалістичні сценарії кібератак та забезпечувати ефективне навчання персоналу в безпечному віртуальному просторі [4, 8].

Ключові аспекти та переваги моделювання сценаріїв кібератак у 3D-середовищах:

1. **Підвищення рівня занурення та наочності для розуміння загроз:** Інтерактивні 3D-середовища дозволяють відтворити віртуальні копії реального промислового обладнання, пультів управління та інтерфейсів АСУ ТП енергетичних об'єктів [5]. Це забезпечує значно вищий рівень візуалізації та залученості персоналу порівняно з абстрактними схемами чи текстовими описами. Учасники навчання можуть наочно спостерігати за нетиповою поведінкою змодельованого обладнання, аномальними показаннями приладів чи змінами в інтерфейсах систем управління, що можуть бути індикаторами кібератаки. Такий підхід сприяє кращому розумінню механізмів атак та їх потенційних наслідків для технологічного процесу.
2. **Розробка та реалізація специфічних сценаріїв кібератак для енергетики:** Ефективність навчання значною мірою залежить від релевантності сценаріїв. Сценарії, що відображають специфіку кіберзагроз для енергетичної галузі, можуть включати:
   - **Маніпуляція даними та командами в АСУ ТП:** Моделювання атак, спрямованих на зміну установок контролерів (наприклад, зміна параметрів роботи генератора, трансформатора, захисних реле), фальсифікацію даних з датчиків (температура, тиск, частота струму), що може призвести до порушення режимів роботи обладнання або його аварійного відключення [6]. У 3D-середовищі це візуалізується через аномальну роботу віртуального обладнання, невідповідність показань приладів реальному стану, спрацювання сигналізації.
   - **Атаки на відмову в обслуговуванні (DoS/DDoS):** Імітація атак, що призводять до недоступності операторських станцій, серверів АСУ ТП або мережевих пристроїв. Учасники навчання мають навчитися ідентифікувати такі атаки та застосовувати процедури для відновлення функціонування або переходу на резервні системи управління.
   - **Компрометація облікових даних та несанкціонований доступ:** Сценарії, що включають елементи фішингу, використання викрадених облікових даних для отримання доступу до систем управління, з подальшим моделюванням дій зловмисника у віртуальному середовищі.
   - **Атаки на ланцюги постачання програмного та апаратного забезпечення:** Моделювання ситуацій, коли шкідливе ПЗ потрапляє в систему через оновлення або інсталяцію нового обладнання, з подальшим відпрацюванням дій з виявлення та ізоляції загрози.
3. **Формування практичних навичок реагування та прийняття рішень:** Інтерактивність 3D-тренажерів дозволяє не просто спостерігати за сценарієм, а й активно брати участь у ньому [7, 8]. Персонал може відпрацьовувати конкретні дії:
   - **Ідентифікація інциденту:** Аналіз даних, розпізнавання ознак кібератаки.
   - **Ізоляція загрози:** Відключення скомпрометованих сегментів мережі, блокування підозрілих з'єднань.
   - **Сповіщення та комунікація:** Правильна передача інформації про інцидент відповідним службам (служба безпеки, ІТ-департамент, керівництво).
   - **Застосування планів реагування:** Дії згідно із затвердженими інструкціями та протоколами.
   - **Збір доказів для розслідування:** Фіксація стану систем, збереження логів.
   - **Відновлення працездатності:** Переведення систем у безпечний режим, відновлення з резервних копій (у рамках змодельованого сценарію).

   Система фіксує дії користувача, час реакції та надає зворотний зв'язок, що дозволяє аналізувати помилки та закріплювати правильні алгоритми поведінки.
4. **Безпечне та контрольоване навчальне середовище:** Однією з ключових переваг є можливість моделювання найнебезпечніших сценаріїв кібератак без будь-якого ризику для реальних енергетичних об'єктів та технологічних процесів [2]. Це дозволяє проводити навчання в умовах, максимально наближених до реальних, але з повним контролем ситуації та можливістю зупинки, повторення або детального розбору будь-якого етапу сценарію.

Висновки:

Застосування інтерактивних 3D-середовищ для моделювання сценаріїв кібератак є потужним та сучасним інструментом для підготовки персоналу енергетичних підприємств. Такий підхід дозволяє значно підвищити практичні навички співробітників у сфері розпізнавання кіберзагроз та ефективного реагування на них, що, в свою чергу, сприяє зміцненню загальної кіберстійкості критичної інфраструктури [4, 5]. Візуалізація, інтерактивність та безпечність віртуальних тренажерів роблять їх незамінними для формування компетенцій, необхідних для протидії сучасним кіберзагрозам в енергетиці [8].

Подальші дослідження будуть спрямовані на розширення бібліотеки типових та кастомізованих сценаріїв кібератак, розробку методологій об'єктивної оцінки рівня підготовленості персоналу за результатами проходження тренажів, а також на інтеграцію можливостей для синхронізованого кооперативного навчання (СКН) для відпрацювання командних дій під час масштабних кіберінцидентів.

1. Bhamare D., Zolanvari M., Erbad A., Jain R., Khan K., Meskin N. Cybersecurity for industrial control systems: A survey. Computers & Security. 2020. Vol. 89. P. 101677. DOI: 10.1016/j.cose.2019.101677.
2. Langer L., Skopik F., Smith P., Kammerstetter M. From old to new: Assessing cybersecurity risks for an evolving smart grid. Computers & Security. 2016. Vol. 62. P. 165-176. DOI: 10.1016/j.cose.2016.07.008bjb.
3. YaminM., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, toolsand architecture. Computers & Security, vol. 88, p. 101636, 2020. DOI: 10.1016/j.cose.2019.101636.
4. Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity-Related Issues. Proceedings of the 2020 International Conference on Advanced Visual Interfaces (AVI '20), p.1–8. DOI: 10.1145/3399715.3399860.
5. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 2019. Vol. 21(2), 1851–1877. DOI:10.1109/COMST.2019.2891891.
6. He D., Chan S., Guizani M. Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wireless Communications. 2017. Vol. 24(6). P. 98-103. DOI: 10.1109/MWC.2017.1600283WC.
7. Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. Education and Information Technologies, 27, 5153–5177. DOI: 10.1007/s10639-021-10807-6.
8. Шевченко С.С. Інтерактивні автоматизовані дистанційні навчально-тренувальні системи як інструмент покращення безпеки енергетики у цифрову епоху. // VI Міжнародна конференція «Перспективи впровадження інновацій у атомну енергетику». 27 вересня 2024 року.

Р.І. Драгунцов

АЛГОРИТМ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ В УМОВАХ ЗНИЩЕННЯ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Повномасштабна російсько-українська війна висунула безпрецедентні виклики для кібербезпеки критичної інфраструктури. З осені 2022 року енергетична система України зазнала масованих ракетних ударів, які призводили до масштабних блекаутів в різних регіонахnews.pncip.gov.ua. Знеструмлення критичної інфраструктури створює новий клас ризиків кібербезпеки. Під час довготривалих відключень електроенергії різко зростають ризики втрати доступності ІТ-систем, відмови засобів кіберзахисту, втрати видимості (моніторингу) мереж і навіть фізичного ушкодження або знищення даних. Війна продемонструвала, що кіберстійкість критичної інфраструктури тісно залежить від її енергостійкості. У цьому дослідженні пропонується алгоритм управління ризикамикібербезпеки пов'язаними з проблематикою масштабних відключень електропостачання. Алгоритм враховує практичний досвід масових блекаутів в Україні 2022–2023 рр. і передбачає як організаційні, так і технічні заходи (резервне живлення, автономні системи тощо) для підтримання безперервності роботи. Наведено приклад застосування алгоритму для організації, що ілюструє ефективність запропонованих заходів.

Ключові ризики кібербезпеки під час блекаутів включають втрату доступності ІТ-систем, відключення засобів кіберзахисту, втрату видимості інфраструктури, знищення волатильного контенту, порушення комунікацій та управління. Перелічені ризики підтверджуються реальними інцидентами 2022-2024 років та більш ранніх епізодів. Зокрема, в грудні 2015 р. внаслідок кібератаки на Прикарпаттяобленерго (українська енергокомпанія) було на 6 годин знеструмлено регіон з ~230 тисячами споживачів ua.news, подібний випадок стався в Києві у 2016 [1]. У 2022 р. під часповномаштабної російсько-української війни зафіксовано комбіновані кібер-фізичні атаки, під час яких російська сторона здійснювала кібернетичні втручання в енергосистему синхронно з ракетними ударами [2]. Ці інциденти довели, що ризики для кібербезпеки і фізичної безпеки критичної інфраструктури поєднані. Необхідне інтегроване рішення з управління ризиками, яке передбачає нестандартні для звичного управління ризиками сценарії – довготривалий блекаут у поєднанні з кібератакою – і пропонує відповідні контролі безпеки (контрзаходи).

Розглянуті контрзаходи для забезпечення безперервної роботи включають резервне енергоживлення критичних систем з використаннямдизельних або бензинових генераторів, а також джерел безперебійного живлення (UPS) та акумуляторних батарей достатньої місткості, альтернативних джерел енергії на основі ВДЕ (відновлюваних джерел), захист та дублювання каналів зв'язку, локалізовані системи підтримки роботи (мікромережі)[3], організаційні заходи[4]. Ключовим результатом даного процесу передбачається досягнення багаторівневого захисту: кожен критичний компонент системи має резервування. Кінцева мета – забезпечити кіберстійкість (cyberresilience) інфраструктури, тобто спроможність продовжувати функціонування і підтримувати рівень гарантій безпеки навіть під час екстремальних умовблекауту.

На основі аналізу ризиків та доступних контрзаходів запропоновано покроковий алгоритм управління ризиками кібербезпеки для сценарію знищення (знеструмлення) енергетичної інфраструктури. Алгоритм поєднує підготовчі дії (до настання блекауту), дії під час кризової ситуації, та пост-інцидентні заходи в режимі "Plan-Do-Check-Act". В табл. 1 наводиться структурований опис алгоритму.

Таблиця 1 –Етапи алгоритму управління ризиками кібербезпеки під час масового відключення електропостачання

Етап	Опис
Ідентифікація критичних активів та залежностей	Визначення ІТ-систем критично важливих для функціонування та кіберстійкості та виявлення залежності активів від енергоживлення та зв'язку. Результатом є карта залежностей що визначає зв'язки об'єкта з системами резервування та забезпечення функціонування (енергоживлення, зв'язок, тощо). Для кожного зв'язку визначається метрика, яка характеризує тривалість роботи джерела в умовах відсутності енергопостачання.
Аналіз ризиків і сценаріїв блекауту	Виконується для кожного критичного активу з урахуванням різних сценаріїв блекауту. Сценарний аналіз включаєранжовані відключення: короткочасне (до 1 години), середнє (1-24 години) і тривале (добу і більше) відключення електропостачання; враховується можливість одночасної кібератаки. Для кожного сценарію оцінюється ймовірність на основі історичних даних і поточної обстановки та потенційні наслідки для активів. Ризик оцінюється як добуток імовірності на вплив. Значення оцінюються експертно або на основі статистики (CERT-UA фіксував у середньому понад 10 кібератак на добу на Україну у 2022 [1], Укренерго публікує графіки та прогнози відключень, перед більшістю масованих ракетно-дронових ударів заздалегідь надається оповіщення з боку повітряних сил [5]).

Продовження таблиці 1

Розробка стратегії та планів захисту	На основі оцінки ризиків приймаються рішення щодо їх мінімізації. Застосовуються підходи зменшення ризику шляхом впровадження контрзаходів. Формується план безперервності: визначаються ресурси для резервного живлення, процедури вводу їх у дію, відповідальні особи.
Впровадження протиризикових заходів	Практична реалізація обраної стратегії. Інсталяція обладнання, налаштування резервних каналів зв'язку тощо. Реалізуються організаційні заходи: тренінги персоналу щодо дій при блекауті, формування інструкцій і контактів. Системи кібербезпеки налаштовуються на роботу в умовах перебоїв.
Моніторинг та реагування під час інциденту	Під час дійсногоблекауту, абоблекауту у поєднанніз кібератакою, організація діє за підготовленим планом. Організовуєтьсяоперативний, виконується оцінка ситуації: які частини системи знеструмлені, які системи перейшли на резервне живлення, яка тривалість очікується. У разі наявності ознак кібератаки запускається план реагування на кіберінцидент. Критично важливо забезпечити моніторинг стану систем на резервному живленні.
Відновлення та аналіз після інциденту	Після відновлення основного електропостачання і стабілізації ситуації наступає фаза відновлення, що передбачає поступове повернення до штатної роботи. якщо мала місце кібератака – проводиться розслідування.
Удосконалення та підготовка до наступних загроз	Перехід в режим business-as-usual з урахуванням отриманих уроків. Організація оновлює регістр ризиків: ризики, що матеріалізувалися, можуть змінити свою імовірність чи вплив у майбутньому.

Математична модель ризиків та захисних заходів

Для наведеного вище поетапного алгоритму застосовується наступна математична модель. Представимо інфраструктуру критичної системи у вигляді орієнтованого графа $G = (V, E)$, де вузли V – це компоненти (активи) системи, а дуги E позначають залежності між ними та залежність від джерел електроживлення або мережевого з'єднання. Наприклад, вузол *Datacenter1* залежить від вузла *UPS* (ця дуга означає "живиться від UPS"), вузол *UPS* залежить від *Generator* та *PowerGrid*, вузол *Datacenter* також пов'язаний з вузлом *Firewall* отримує доступ в інтернет через фаєрвол. Для кожної дуги визначається коефіцієнт ваги, який визначає час автономного функціонування за при перериванні даного зв'язку. У такому графі відображаються точки відмови: якщо вузол *PowerGrid* виходить з ладу, то живлення може бути компенсоване вузлом *Generator*. Надійність системи щодо електроживлення можна оцінити через поняття зв'язності графа: необхідно, щоб для кожного критичного вузла існував хоча б один шлях до вузла-джерела живлення з ваговим коефіцієнтом більше нуля або більшим чи рівним за цільове значення мінімального часу без відмови. Введемо двійкову змінну стану для кожного вузла: $X_i = 1$, якщо вузол працездатний, і $X_i = 0$ у разі відмови (наприклад, відсутнє живлення). Тоді ціль – забезпечити $X_{Datacenter} = 1$ навіть якщо $X_{PowerGrid} = 0$, за рахунок шляху через генератор: формально, наявність резерву означає, що $X_{Datacenter} = X_{UPS}\ and\ (X_{powergrid}\ or\ X_{generator})$.

Розглянемо простий випадок: система має два незалежні джерела живлення (основне і резервне). Імовірність відмови основного джерела (блекаут електромережі) – позначимо $p_{\text{powergrid}} = P(X_{\text{powergrid}} = 0)$. Імовірність відмови резервного генератора (наприклад, він може не запуститися чи закінчиться пальне) – $p_{\text{gen}} = P(X_{\text{generator}} = 0)$. Для спрацювання резерву ці події мають бути незалежними (на практиці це майже так: відмова електромережі не впливає на механіку генератора, хоча можливі непрямі залежності як нестача пального через логістику під час блекауту, але припустимо незалежність). Тоді імовірність повної втрати живлення для критичного об'єкту є (1):

$$P(PowerLoss) = P(Xgrid = 0 \wedge Xgenerator = 0) = pgrid \cdot pgen.\ P(\text{Power Loss}) = P(X_{\text{grid}} = 0 \wedge X_{\text{generator}} = 0) = p_{\text{grid}} \cdot p_{\text{gen}}.\ P(PowerLoss) = P(Xgrid = 0 \wedge Xgenerator = 0) = pgrid \cdot pgen \quad (1)$$

Аналогічно можна промоделювати надійність зв'язку. Таким чином, графова модель дозволяє кількісно оцінити виграш від дублювання компонентів. У термінах теорії надійності, реалізовано резервування за схемою "n із m" (наприклад, 1 із 2 джерел має бути працездатним для функціонування системи). Формула для імовірності безвідмовної роботи при наявності резервів задається через комбінаторні ймовірності відмов, але в простому випадку 1 резерв саме добуток імовірностей відмов дає імовірність загальної відмови.

Висновки

На основі аналізу ризиків масових відмов енергопостачання та можливих контрзаходів запропоновано покроковий алгоритм управління ризиками кібербезпеки. Алгоритм спирається на математичну модель на основі теорії графів, що дозволяє оцінити покриття інфраструктури засобами резервування елктроживлення та зв'язку та їх адекватність наявним вимогам щодо поточних ризиків втрати електроживлення. Дана модель є спрощеною, однак, може застосовуватись на практиці для планування організаційних та інфраструктурних змін для забезпечення кіберстійкості організації.

1. Хмельова, І. (2022). *Кібератаки, Артилерія, Пропаганда. Загальний огляд вимірів російської агресії*. Рада Економічної Безпеки України.
2. *рф щодня здійснює понад 10 кібератак на стратегічні об'єкти України — керівник Департаменту кібербезпеки СБУ*. (2022, 9 листопада). АрміяInform – Інформаційне агентство АрміяInform. https://armyinform.com.ua/2022/11/09/ponad-10-kiberatak-na-strategichni-obyekty/
3. Ahshan, R., Iqbal, M. T., Mann, G. K. I., & Quaicoe, J. E. (2010). Micro-grid system based on renewable power generation units. У *2010 IEEE 23rd Canadian Conference on Electrical and Computer Engineering - CCECE*. IEEE. https://doi.org/10.1109/ccece.2010.5575112
4. Drahuntsov, R., & Zubok, V. (2023). Modeling of Cyber Threats Related To Massive Power Outages and Summary of Potential Countermeasures. *Èlektronnoe modelirovanie*, *45*(3), 116–128. https://doi.org/10.15407/emodel.45.03.116
5. Muravska, J. (б. д.). У *Getting serious about building Ukraine's air defence capabilities*. FREEMAN AIR & SPACE INSTITUTE.

В.С. Івкова, М.І. Мазуркевич

ВИКОРИСТАННЯ ЗАХОДІВ COUNTER-OSINT ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Сьогодні, коли цифрові технології стали невід'ємною частиною нашого життя, питання безпеки особистих даних постає нагальною проблемою. Часто навіть не усвідомлюючи цього, користувачі викладають у відкритий доступ велику кількість інформації про себе: фотографії, номери телефонів, місцезнаходження, електронні адреси. Достатньо мати базові технічні навички — і будь-хто може зібрати повний цифровий портрет людини або організації, при цьому формально не порушуючи закон.

Саме необізнаність і недбале ставлення до конфіденційності створюють ідеальні умови для використання методів відкритої розвідки — OSINT (Open Source Intelligence). Як противагу цьому, з'являється потреба у контрзаходах, які покликані зменшити доступність персональних даних — так званих Counter-OSINT практик.

Під OSINT розуміють збір і аналіз інформації з відкритих джерел: соціальних мереж, публічних реєстрів, баз даних, доменів, форумів, метаданих фото- та відеофайлів тощо [1].

Ця інформація не є секретною, проте її об'єднання дозволяє сформувати доволі повну картину про особу чи об'єкт. OSINT активно застосовується у сфері журналістики, безпеки, кібербезпеки, діяльності правоохоронних органів, а також бізнесу.

Найбільш відомими інструментами, які використовуються для цього, є Maltego, SpiderFoot, Shodan (пошукова система для виявлення пристроїв у мережі), Recon-ng і theHarvester [2]. Всі вони мають відкритий доступ і не потребують спеціального дозволу на використання.

Counter-OSINT — це не один інструмент, а комплекс дій, які користувач або організація може вжити. Наприклад, уникайте надмірної публічності в соціальних мережах: приховуйте інформацію про місцезнаходження, закривайте списки друзів, не використовуйте одні й ті самі фото чи псевдоніми на різних платформах.

Ефективною практикою є створення окремих облікових записів для роботи, особистих справ і публічної активності.Сюди ж відноситься і використання віртуальних машин, VPN-сервісів, браузерів із посиленими налаштуваннями конфіденційності, а також ретельне очищення метаданих у файлах перед публікацією [1].

Важливою складовою є й контроль за доменними даними: варто приховувати WHOIS-інформацію, використовувати проксі або сторонні реєстратори. Сервіси, на кшталт, HaveIBeenPwned чи DeHashed допоможуть виявити, чи ваші дані вже були скомпрометовані. Варто також періодично проводити самоперевірку — використовуючи OSINT-інструменти відносно власних даних, щоб дослідити, які саме відомості доступні у відкритих джерелах.

У корпоративному середовищі заходи Counter-OSINT є ще важливішими. Компаніям слід регулярно перевіряти, яка інформація про них доступна в пошукових сервісаї, аналізувати рівень відкритості структури, посад, службових адрес.

Корисно обмежити індексацію конфіденційного вмісту та проводити навчання працівників з цифрової гігієни. Із розвитком технологій захисту (наприклад, шифруванням) змінюється і сам підхід до роботи з даними — акцент переходить від збору до мінімізації доступу [3].

Не менш важливим напрямом у практиці Counter-OSINT є робота з власними звичками користувача: не варто використовувати однакові нікнейми чи аватари на різних платформах, особливо якщо один із акаунтів прив'язаний до особистих даних. Для перевірки того, де вже використовується ваш псевдонім або ім'я користувача, доцільно скористатися онлайн-інструментами на кшталт NameCheckr чи WhatsMyName. Зазначені інструменти дають змогу виявити пов'язані профілі та своєчасно вжити заходів для зменшення цифрового сліду.

Окремо загрозою можна вважати, використання соціальних мереж працівниками державних підприємств, установ організацій з метою публікації як робочої інформації так і ведення особистих профілів[4, с.166].

Як приклад, Йонг-Джун Лі, Парк Се-Джун, Парк Вон-Хен в своєму дослідженні «Military Information Leak Response Technology through OSINT Information Analysis Using SNSes» зазначають, що в результаті проведення експерименту з використанням усього чотирьох OSINT-систем, за пошуковими запитами з дев'яти ключових слів, які пов'язані з військовою інформацією, а саме: «військова таємниця», «обороно-промислові переваги», «оборонні компанії», «оборонний потенціал», «проекти вдосконалення», «офіцери», «системи озброєння» та «оборонні проекти», введеними англійською мовою, отримали 100209 результатів використання ключових слів в соціальних мережах [5, с. 4].

В Україні подібні дослідження не проводились, проте відповідно до звітів основних суб'єктів забезпечення кібербезпеки —соціальні мережі на постійній основі використовуються зловмисниками для збору інформації про об'єкт атаки, зокрема для поширення фішинговихпосилань, шкідливого програмного забезпечення, вчинення несанкціонованих втручань в роботу електронно-обчислювальної техніки, тощо. [4, с.167].

Отже, у світі, де інформація про нас постійно накопичується, здатність контролювати власну «цифрову тінь» стає критично важливою. Повністю приховатися в Інтернеті неможливо, проте впровадження навіть базових заходів протидії OSINT може істотно знизити ризики витоку особистої інформації. Це не лише технічне питання, а й справа цифрової культури.

1. Bazzell M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. – 8th ed. – 2021. – 547 p.
2. Shodan, Recon-ng, theHarvester [Електронні ресурси]. – Режим доступу: https://www.shodan.io/, https://github.com/lanmaster53/recon-ng, https://github.com/laramies/theHarvester.
3. Williams H.J., Blum I. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. – RAND Corporation, 2021. – 74 p.
4. Івкова, В., & Опірський, І. (2025). OSINT-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749.
5. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT.Wireless Communications and Mobile Computing, 2022, 1–14. https://doi.org/10.1155/2022/1290129.

I.O. Dubovkina

NEW ENERGY SAVING MODES OF PROCESSING LIQUIDS

Understanding how liquid interact with each other is key to conception how structures arise and how their properties arise from these[1].

Aquatic solutions were used for experimentation investigations. Aqua treatment and obtaining process was spent in the condition of the physical influence.

Agriculture occupies 38% of the Earth's surface and is the largest amount of land dedicated to a sole purpose[2].

Liquid nutrient solutions such as double distilled water, irrigation water for drip irrigation systems, and solutions with fertilizes were used for processing. Spring barley "Myronivskyi 22" and vigorous triticale "Soncedar kharkivskyi" were used for testing growing crops.

Rotary-pulsed apparatus of the cylindrical type with clearances 120×10^{-6} m was used. The method of testing growing crops and method of optical microscopy were used.

For growing of spring barley "Myronivskyi 22" such parameters were selected: processing time – 30 s, processing frequency 5, angular velocity – 315 s^{-1}, impulses of pressure – 390 kPa.

For growing of vigorous triticale "Soncedar kharkivskyi" selected parameters were: processing time – 15 s, processing frequency 1, angular velocity – 300 s^{-1}, impulses of pressure – 370 kPa.

The effects of analytical computation and mathematical modeling, statistical experiment have given the possibility to calculate basic design data of devices which influence on intensification of carrying out of obtaining processes for aquatic mediums, and also processing for the purpose of change of physical and chemical parameters and structural transformations. The research studies demonstrated the increasing of the pH of the water prepared for the technology on the 15%.

The nature and velocity of many physical and chemical processes which take place in such water systems changes.

The potential of hydrogen can greatly verify the velocity of itinerary of chemical reactions. Throughout processing of aquatic solutions and obtaining process in the conditions of linear speeds of the first rotor is 21,5 m/s and the second rotor is 23,5 m/s. The pressure of shift of a stream for the first rotor is 215 Pa and for the second rotor is 235 Pa.

The speeds of shift of a stream for the first rotor is $2,0 \times 10^5$ s^{-1} and for the second rotor is $2,5 \times 10^5$ s^{-1}. The speed of rotary motion of the rotors is n = 50 sec^{-1}. Through researches the potential of hydrogen of the aquatic solutions prepared on standard technology has raised on 15%. Employment the method of physical influence in technology of receiving of mediums allows receiving the activated aquatic solutions with the certain physical properties and parameters, assured value of a potential of hydrogen.

Carrying out of obtaining processes for mediums in continuous approach is giving the possibility to decrease reduction-oxidation potential on 25-55%.

By the modelling processes, mathematical and numerical modelling was found that the value of the linear speeds of a stream should be from 21.98 m/s to 22.13 m/s for the first rotor and from 23.58 m/s to 23.70 m/s for the second rotor. The value of angular velocity was 314 s^{-1} and the frequency of hydrodynamic oscillations was $3\cdot10^3$ Hz. The coaxial clearance between first rotors, stator and second rotor was from 100 to 500 μm.

The value of shear rate was for the first rotor from $2.2\cdot10^5$ s^{-1} to $0.44\cdot10^5$ s^{-1} and for the second rotor from $2.4\cdot10^5$ s^{-1} to $0.47\cdot10^5$ s^{-1}. The value of shear stress for the first rotor was from 219.8 Pa to 44.26 Pa and for the second rotor from 235.5 Pa to 47.4 Pa. The pressure difference between the input and the output liquid solutions at the working volume before and after treatment is $\Delta P = 50\cdot10^3$ Pa.

According to the results of the research, it was found that the alternating pressure pulses in the system are $\Delta P = 370\cdot10^3$ Pa near the outer surface of the inner rotor; $\Delta P = 240\cdot10^3$ Pa near the outer surface of the stator; $\Delta P = 155\cdot10^3$ Pa near the inner surface of the stator; $\Delta P = 190\cdot10^3$ Pa near the inner surface of the outer rotor.

The local pressure values in the zone of water and alcohol inlet and water-alcohol mixture outlet from the clearance change: near the outer surface of the inner rotor from $-50\cdot10^3$ Pa to $+300\cdot10^3$ Pa; near the outer surface of the stator from -150 to $100\cdot10^3$ Pa; near the inner surface of the stator from $+40\cdot10^3$ Pa to $-120\cdot10^3$ Pa; near the inner surface of the outer rotor from $+ 100\cdot10^3$ Pa to $-100\cdot10^3$ Pa.

It should be noted that the fluid flow in the RPA has a pulsating nature of movement; within one period the speed reaches 0.52 m/s and sharply decreases to the minimum value of 0.18 m/s.

The results of the experimental researches is established that using of no reagent methods of physical influence is of current interest and perspective for consciousness of control on physical and chemical parameters, properties and the structural organization for the purpose of an intensification of obtaining process of the aquatic solutions mediums.

Analysis of experimental data showed the effectiveness of using alternating pressure impulses for processing liquid nutrient solutions for hydroponic systems to increase the productivity of cultivated agricultural crops and the yield of green biomass.

1. Welton T. (2018), Ionic liquids: A brief history, Biophysical Reviews, 10(3), pp. 691–706, https://doi.org/10.1007/s12551-018-0419-2.
2. Foley J.A., Ramankutty N., Brauman K. A. (2011), Solutions for a cultivated planet, Nature, 478(7369), pp. 337–342, https://doi.org/10.1038/nature10452.

А.В. Бойченко, В.Р. Сенченко

ВИКОРИСТАННЯ ШІ ДЛЯ ПОБУДОВИ СЦЕНАРІЇВ КІБЕРАТАК НА ОБ'ЄКТИ ЕНЕРГЕТИКИ

У зв'язку з безперервною збройною агресією з боку РФ актуальним проблема безпеки енергетичної галузі набула надзвичайної актуальності. Використання штучного інтелекту (ШІ) для генерування можливих сценаріїв кібератак може бути потужним способом моделювання загроз, тестування захисту та покращення стану безпеки об'єктів енергетики.

Засоби штучного інтелекту включають машинне навчання, глибоке навчання, обробку природної мови (NLP), генеративні моделі, а також інструменти для аналізу великих даних. Ці технології здатні виявляти закономірності у великих масивах даних, прогнозувати поведінку систем, автоматизувати прийняття рішень і навіть генерувати нові сценарії на основі історичних прикладів. У поєднанні з потужностями хмарних обчислень і доступністю відкритого програмного забезпечення, ШІ стає дедалі доступнішим для широкого кола користувачів.

У сфері кібербезпеки, зокрема в контексті енергетичних систем, ШІ може застосовуватись як для захисту, так і для моделювання потенційних атак. Наприклад, моделі глибокого навчання можуть бути натреновані для імітації поведінки зловмисника, прогнозування вразливих точок у SCADA-системах, або створення фішингових повідомлень за допомогою NLP. Генеративні моделі, подібні до тих, що використовуються в генеративних моделях, можуть створювати сценарії соціальної інженерії, а інструменти розпізнавання шаблонів — ідентифікувати слабкі місця в логіці доступу до критичної інфраструктури.

Для побудови реалістичних сценаріїв кібератак ШІ може моделювати дії атакуючих груп, засновані на історичних даних про інциденти, використовувати алгоритми агентного моделювання для симуляції дій внутрішніх чи зовнішніх загроз, а також допомагати у створенні комплексних атак на основі комбінації векторів вторгнення. Такі симуляції можуть бути використані для підготовки персоналу, тестування надійності систем або для вдосконалення захисних стратегій, створюючи цифрові "пісочниці", в яких моделюються атаки без загрози для реальних систем.

Підстанції цифрових електромереж стикаються зі значними вразливостями в кібербезпеці через їхню зростаючу залежність від взаємопов'язаних технологій. Ці слабкі місця наражають електромережута можуть призводити до каскадних ефектів. Основні вразливості цифрових підстанції – це застарілі методи автентифікації, незашифровані протоколи зв'язку таки як GOOSE (GenericObjectOrientedSubstationEvent), відсутність VPN-з'єднання з мережами підстанцій, неналежне зберігання облікових даних та багато інших. Методи ШІ можуть допомогти автоматизувати створення реалістичних сценаріїв атак, які дозволяють виявляти вразливості цифрових підстанції, прогнозувати тактику противника та створюють умови для прийняття необхідних заходів щодо захисту енергетичних об'єктів. на потенційні збої, маніпуляції даними та несанкціонований контроль з боку злочинців.

Так, у роботі [3] нами було запропоновано підхід до моделювання сценаріїв розвитку події у галузі енергетики за допомогою знання-орієнтованої технології з використанням графової БД Neo4j. Ця технологія включає зокрема механізми формування графових моделей з даних, що містяться в XML файлах [5], і які у подальшому можуть використовуватись для навчання моделей ШІ.

На рис. 1 показано згенерований сценарій проникнення у мережу, до якої підключені цифрові підстанції.

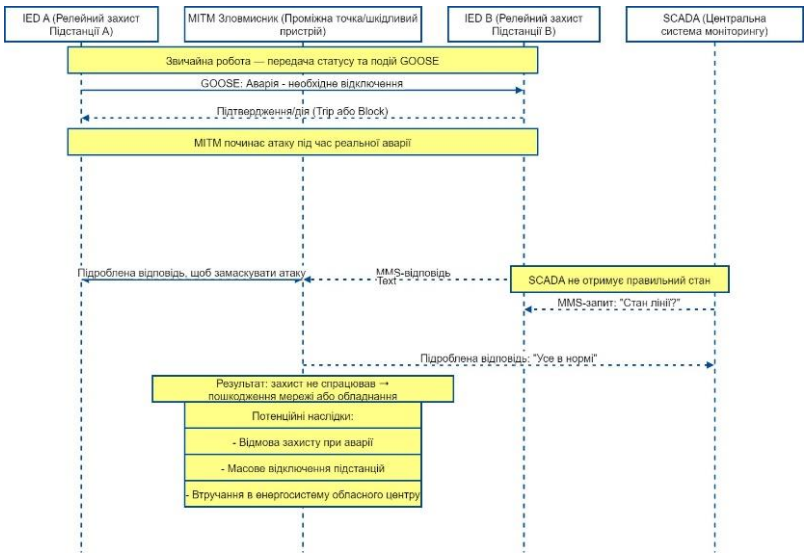


Рисунок 1 – Сценарій кібератаки на ресурси мережі IEC 61850

Дана діаграма демонструє реалізацію атаки "Man-in-the-Middle" (MITM) на прикладному рівні в мережі IEC 61850, орієнтовану на релейні пристрої підстанцій у типовому обласному центрі. У звичайному режимі пристрій релейного захисту підстанції A (IED A) передає повідомлення GOOSE про виявлену аварію до пристрою на підстанції B (IED B), який у відповідь виконує відповідну дію (наприклад, відключення лінії). Зловмисник (MITM), який знаходиться в мережі між цими пристроями, перехоплює справжнє повідомлення про аварію і підміняє його зміненим — наприклад, таким, що сигналізує про відсутність несправностей. У результаті IED B не спрацьовує, хоча аварійна ситуація дійсно має місце.Одночасно атакуючий перехоплює MMS-запити SCADA-системи до IED B, щоб дізнатися стан лінії, і підміняє відповіді, імітуючи нормальну роботу. Це дозволяє йому приховати справжній стан системи від операторів енергомережі.

Цей приклад демонструє доцільність використанні засобів ШІ для моделювання сценаріїв атак на критичну інфраструктуру, оскільки традиційні системи захисту, не здатні розпізнати підміну повідомлень на прикладному рівні, коли атака маскується під легітимну комунікацію. Зловмисник, діючи непомітно в реальному часі, може змінювати аварійні сигнали та відповіді системи, що призводить до невидимих, але потенційно катастрофічних наслідків для енергосистеми. ШІ, аналізуючи поведінкові аномалії, часові закономірності та контекст повідомлень, може виявити ознаки втручання, які не фіксуються традиційними засобами, тим самим забезпечуючи проактивний рівень захисту критичної інфраструктури.

Організації, що впроваджують виявлення загроз на основі штучного інтелекту, повідомляють про53% прискорення реагування на нові моделі атак, хоча модернізація застарілих систем залишається складною проблемою. Таким чином, комплексний аналіз кібербезпеки стає невід'ємною частиною забезпечення стабільності енергосистем у цифрову епоху.

1. Jaber, A., & Fritsch, L. (2022, October). Towards ai-powered cybersecurity attack modeling with simulation tools: Review of attack simulators. In International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 249-257). Cham: Springer International Publishing.
2. Rodriguez, M., Popa, R. A., Flynn, F., Liang, L., Dafoe, A., & Wang, A. (2025). A Framework for Evaluating Emerging Cyberattack Capabilities of AI. arXiv preprint arXiv:2503.11917.
3. Сенченко, В. Р., Бойченко, А. В., Коваль, О. В., Бисько, Р. М., & Хоменко, О. М. (2024). Огляд методів і технологій сценарного аналізу каскадних ефектів. Реєстрація, зберігання і обробка даних, 26(1), 24-54. DOI: 10.35681/1560-9189.2024.26.1.308506.
4. Бойченко А. В. Використання технологій ГШІ для аналізу каскадних ефектів критичної інфраструктури. //Інформаційні технології та безпека. Зб. наук. праць. – В.24. – К.: ІПРІ НАНУ, 2024. С.169-173. ISBN: 978-617-8180-00-3.
5. Boychenko A.V., Senchenko V.R. An approach to development of cyberattack scenarios for digital substations. Cybersecurity of energy, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine. May 29, 2024. Kyiv: PIMEE NAS of Ukraine, 2024. p. 4 – 6.
6. Cybersecurity Vulnerabilities and Threats in Smart Gridshttps://clouglobal.com/cybersecurity-vulnerabilities-and-threats-in-smart-grids/.

Д.П. Сінько, К.Д. Сінько

ВИРІШЕННЯ ПРОБЛЕМИ РОЗМІРНОСТІ У ЗАДАЧІ ПРОГНОЗУВАННЯ ПРОБЛЕМИ РОЗЩЕПЛЕННЯ КЛАСТЕРА

Анотація

В тезах розглядається прогнозування проблеми розщеплення кластера (ПРК). Основна увага приділяється викликам, пов'язаним із змінною розмірністю кластерів, що ускладнює подачу даних на вхід моделям машинного навчання. Проаналізовано сучасні методи уніфікації структур графів, зокрема техніки padding і маскування. Окремо розглянуто спектральні підходи двовимірне перетворення Лапласа та графове перетворення Фур'є. Робота підкреслює переваги та обмеження кожного з методів та окреслює напрямки для побудови розмірно-універсальних моделей.

Вступ

У сучасній архітектурі розподілених інформаційних систем майже неможливо обійтися без застосування мікросервісного підходу. Водночас мікросервісна архітектура супроводжується ризиками, зокрема виникненням проблеми розщеплення кластера (далі ПРК) критичного стану кластерних систем, спричиненого їх розподілом на ізольовані частини, в англомовній літературі це явище відоме як splitbrainproblem [1]. В контексті мілітарних загроз в Україні [2] та проблем зі світлом та зв'язком у світі [3] дане питання набуває надзвичайної актуальності.

У попередній роботі [4] було запропоновано використання методів та алгоритмів машинного навчання для прогнозування ПРК. Розглянуто метод забезпечення консистентності в кластерах з реплікацією типу singleleader [5], за якого одна з нод виконує функції лідера, а у випадку розділення кластера решта його частин орієнтуються на рішення цієї ноди. Залишається актуальною задача створення розмірно-універсальної моделі, яка б могла приймати кластери різного розміру та прогнозувати ймовірність ПРК. Проаналізуємо підходи з відкритих джерел.

Виклад основного матеріалу

У роботі [6] представлення кластеру відбувається у формі матриці суміжності та пропонується підхід перетворення вхідних даних змінної розмірності до фіксованого формату шляхом доповнення матриці спеціальними значеннями, що явно позначають відсутність нод. Такий метод дозволяє уніфікувати вхідні дані для моделі машинного навчання, не втрачаючи інформацію про початкову структуру кластера. Зокрема, при обробці кластерів менших за максимальний розмір (20 нод), відсутні елементи заповнюються маркером -1, що дає змогу моделі розрізняти реальні зв'язки та технічне доповнення. Крім того, передбачене кодування типів нод у вигляді цілих чисел, починаючи з 2, дозволяє моделі враховувати роль кожної ноди в загальній структурі. Така форма представлення забезпечує сталу розмірність (21×20) і дозволяє вирішити проблему подавамоїмо інформації. Цей метод також відомий як padding.

Однак просте застосування padding може призвести до спотворення навчального процесу, оскільки модель потенційно сприйматиме додані елементи як релевантні ознаки. Для вирішення цієї задачі доцільним є використання маскування. Цей метод включає побудови допоміжної маски, що вказує, які елементи є реальними, а які заповнювачами. Проблемою є те, що не всі, навіть сучасні моделі, підтримують маскування. Повністю ця можливість реалізована у нейромережах та лише частково у методі CatBoost.

В іншому напрямку перспективного вирішення проблем із змінною розмірністю у презентації кластерної структури, як демонструє [7], застосовують двовимірне Лапласове перетворення до матриці суміжності відповідного графа. Цей підхід дозволяє відобразити структуру системи як точку у векторі фіксованої розмірності, незалежно від того, скільки елементів мають система. Лапласове перетворення враховує топологічні особливості графа, включаючи зв'язність, локальні взаємозв'язки вершин та спектральні властивості, які істотні для опису внутрішньої організації структури. Можна також ввести деякі глобальні параметри, такі як пагін число вершин чи щільність зв'язків, які дозволять синтезувати уніфіковане представлення, яке можно буде подати вхідним параметром для моделей машинного навчання.

Іншим імовірним рішенням є використання графових перетворень Фур'є [8], що моделюють взаємозв'язки всередині кластеру. Під цим підходом граф трактують як сигнал, що заздалегідь визначений на множині вузлів, а спектральне перетворення підтасовується до графового оператора. Отримані спектральні коефіцієнти описують частотні компоненти сигналу, що лежать в основі масштабів варіацій у структурі графа. Така функція відбувається у просторовому чи спектральному представленні. Вибравши певну фіксовану кількість низькочастотних компонент, можна створити вектор ознак фіксованої довжини, що не залежить від початкової кількості вузлів у графі. Головною проблемою є те, що час від часу ці вектори можуть бути комплексними.

Висновок

У цій роботі проаналізовано підходи для вирішення проблеми розмірності матриці суміжності, що використовується для прогнозування ПРК в мікросервісних структурах.

Серед проаналізованих рішень окрему увагу приділено підходам на основі матриці суміжності, зокрема методам padding і маскування, що дозволяють унифікувати графи з різною кількістю нод. Хоча така зв'язка може бути дуже ефективною вона має ключову проблему. Більшість моделей машинного навчання не підтримують маскування, тому використання технології може бути дуже лімітованим.

Також було розглянуто спектральні методи, зокрема двовимірне перетворення Лапласа та графове перетворення Фур'є, які дозволяють перейти до спектрального простору, забезпечуючи вектор ознак сталої довжини, що важливо для моделювання ризиків ПРК. Проте спектральне представлення може включати комплексні компоненти, що ускладнює подальше використання у традиційних моделях, орієнтованих на дійсні значення.

Підсумовуючи, доцільне використання кожного з описаних методів може допомогти вирішити проблему розмірності кластера. Варто враховувати особливості методу та його сумісність з обраним алгоритмом машинного навчання. Подальші дослідження мають бути спрямовані на удосконалення структури розмірно-універсальної моделі, яка б знизила ймовірність збитків у випадку виникнення ПРК.

1. Bhuiyan, S., &Zheludkov, M. (2019). Apacheignitebook. LuluPress, Inc.
2. Ситуація в енергосистемі на 13 травня: через значні пошкодження енергооб'єктів і нестачу електроенергії можливі обмеження для промислових споживачів. (2023). https://www.kmu.gov.ua/news/sytuatsiia-v-enerhosystemi-na-13-travniacherez-znachni-poshkodzhennia-enerhoobiektiv-i-nestachu-elektroenerhii-mozhlyvi-obmezhennia-dlia-promyslovykh-spozhyvachiv.
3. Масштабний блекаут у Європі. У Португалії причиною вважають рідкісне явище. (2023). https://www.rbc.ua/rus/news/masshtabniy-blekaut-evropi-portugaliyi-prichinoyu-1745850993.html.
4. Сінько, Д. П., &Сінько, К. Д. (2025). Методи машинного навчання в задачах прогнозу факторів, що вказують на потенційне партиціювання кластеру. Èlektronnoe modelirovanie, 47(1), 22–39. https://doi.org/10.15407/emodel.47.01.022
5. Shang, Y. (2024). Resilient leaderess and leader-follower consensus over random networks through ℓ-hop communication. European Journal of Control, 101075. https://doi.org/10.1016/j.ejcon.2024.101075.
6. Сінько, Д. П., &Сінько, К. Д. (2025). Застосування машинного навчання у виявленні передумов до потенційного поділу кластера. Збірник матеріалів XLIII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. URL: https://ipme.kiev.ua/wp-content/uploads/2025/05/Materialy-KMV-2025.pdf.
7. Barabash, O. V. (2024). Comparative analysis of the approximation of a probabilistic indicator of functional stability using Bernstein polynomials and feed-forward neural networks. Connectivity, 169(3). https://doi.org/10.31673/2412-9070.2024.033237.
8. Sahai, T., Speranzon, A., &Banaszuk, A. (2009). Hearing the clustersin a graph: A distributed algorithm. URL: https://doi.org/10.48550/arXiv.0911.4729.

А.Р. Слободян, О.Ф. Буткевич

ЕКСПЕРИМЕНТАЛЬНО-МОДЕЛЬНІ ДОСЛІДЖЕННЯ ДИСПЕТЧЕРИЗАЦІЇ НАВАНТАЖЕНЬ АГРЕГОВАНИХ МІКРОМЕРЕЖ ДЛЯ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЛОКАЛЬНИХ ЕНЕРГОСИСТЕМ

Неодмінною умовою підвищення надійності електрозабезпечення споживачів в Україні є суттєве збільшення в структурі генеруючих потужностей ОЕС України частки розосереджених джерел генерування (РДГ), зокрема відновлюваних джерел енергії. Поряд з підвищенням надійності енергозабезпечення споживачів завдяки використанню РДГ та створенню мікромереж (в [1] мікромережа трактується як *форма, різновид децентралізованої енергосистеми*) функціонування локальних енергосистем з мікромережами різного ступеня агрегації передбачає також підвищення ефективності використання енергетичних ресурсів та забезпечення більшої гнучкості управління [2]. Тут варто підкреслити одну властивість такої складної системи, якою є локальна енергосистема з агрегованими мікромережами: за нормальних умов (не пов'язаних з виникненням аварій) ефективний режим функціонування кожної із мікромереж сприятиме досягненню ефективного режиму (умовного оптимуму) функціонування локальної енергосистеми (ця властивість не є характерною для складних систем, оскільки не узгоджується з принципом емерджентності – другим принцип В.Р. Ешбі), але у разі виникнення аварійних (післяаварійних) режимів завдання забезпечення резильєнтності локальної енергосистеми з агрегованими мікромережами має бути домінантним, мати вищий пріоритет ніж забезпечення ефективного режиму функціонування кожної із мікромереж. Різноманітні вимоги до архітектури, функцій систем моніторингу та управління мікромережами, до реалізації функцій, необхідних для забезпечення мережевих послуг, до диспетчеризації навантажень (з отриманням ефекту, відповідного саморегулюванню навантажень) для стабілізації частоти та напруги мікромереж змінного струму та багато іншого, зокрема деякі рекомендації та специфікації – все це міститься у відповідних стандартах, що стосуються мікромереж. Не дивлячись на певний прогрес в царині розвитку мікромереж в Україні та прийняття декількох гармонізованих з міжнародними національних стандартів щодо мікромереж та їхніх елементів, ще залишається значна кількість питань, які потребують подальших досліджень та опрацювань, зокрема і тих, що стосуються диспетчеризації навантажень агрегованих мікромереж та керованого використання енергоресурсів таких мікромереж для забезпечення резильєнтності локальних енергосистем у разі виникнення аварій. Нижче стисло наведено результати досліджень, що стосуються диспетчеризації навантажень агрегованої мікромережі.

Для проведення досліджень в середовищі MATLAB Simulink було створено модель агрегованої мікромережі територіальної громади, що базується на фрагменті реальної розподільної мережі, що містить районну електричну підстанцію 110/35/10 кВ. Сумарна потужність сонячних електростанцій (СЕС) агрегованої мікромережі становить 16 МВт, а установок зберігання електроенергії (УЗЕ) – 500 кВт з сумарною ємністю 1 МВт·год. Загальний вигляд такої мікромережі (із «блочним» зображенням її елементів, кожний з яких враховується своєю «розгорнутою» моделлю) показано на рис. 1.

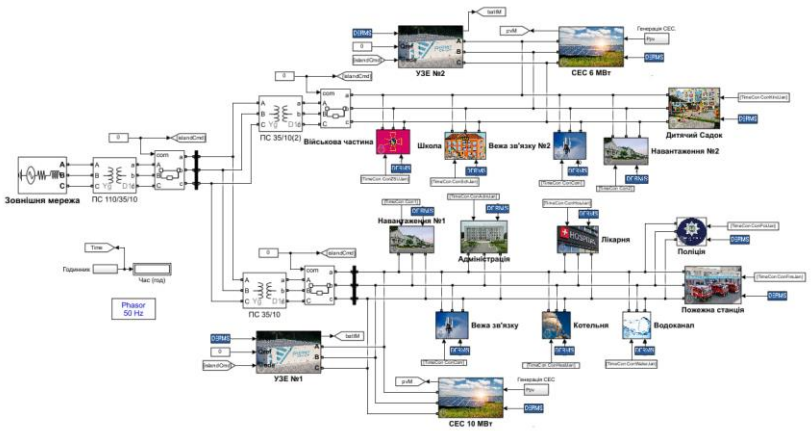
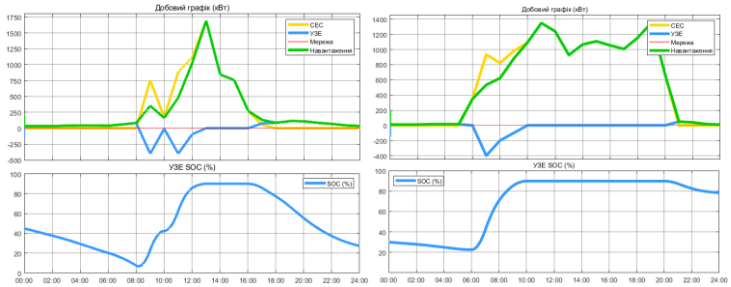


Рисунок 1 – «Блочне» зображення моделі агрегованої мікромережі

Усі споживачі територіальної громади (агрегованої мікромережі), залежно від пріоритетності електрозабезпечення, згруповано у вигляді кластерів. Формування кластерів починається з рівня *елементарних* мікромереж. Кількість кластерів залежить від особливостей споживачів електроенергії в аспекті їхнього впливу на життя (скоріше на резильєнтність) територіальної громади та «чутливості» до перерв електропостачання. Наприклад, кластер №1 – це споживачі критичної інфраструктури територіальної громади (медичні заклади, водоканал, системи зв'язку та ін.); кластер № 2 – пріоритетні споживачі, але менш вразливі до перерв електроживлення; кластер № 3 – побутові споживачі та споживачі, «стійкі» до перебоїв з електроживленням. У даному дослідженні було виконано поділ усіх споживачів на 2 кластери та використано ретроспективні дані щодо електричних режимів локальної енергосистеми. Потужність зимового та літнього максимумів сумарного електроспоживання становила відповідно 1692 МВт та 1354 МВт. З урахуванням відмінностей метеоумов та зазначених режимів дослідження було виконано як для зимового, так і літнього сценаріїв.

Під час реалізації функції диспетчеризації навантажень агрегованих мікромереж було просто використано дворівневу архітектуру системи керування, тому одним із питань, що потребує додаткового дослідження стосується доцільності використання такої дворівневої архітектури системи керування процесами електроживлення споживачів за будь-якої кількості *елементарних* мікромереж, агрегованих в локальну енергосистему. Перший рівень дворівневої системи утворюють системи керування *елементарних* мікромереж, вони діють незалежно за нормальних режимів, виходячи з умов досягнення максимуму ефективності функціонування «власної» мікромережі. Системі керування другого рівня надається лише відповідна «звітна» інформація щодо поточного стану *елементарної* мікромережі (заряду УЗЕ, потужності власного генерування, потужності споживання кожним із кластерів). У разі виникнення ізольованого режиму (внаслідок аварії) керування переходить до системи другого рівня. Саме цього випадку стосується результати досліджень.

Завдання полягає, насамперед, у забезпеченні електроживлення споживачів критичної інфраструктури (кластер №1), а решти – залежно від умов. У разі дефіциту електроенергії споживачі кластеру № 2 вимикаються, а УЗЕ переходить у режим розряду до стану заряду на рівні 10% SOC (State of Charge) від максимального. Для збереження ресурсу УЗЕ та уникнення глибокого розряду система керування встановлює граничні значення SOC (10–90%). Початковий SOC встановлено на рівні 45% для зимового сценарію та 35% для літнього. У періоди профіциту система керування спрямовує надлишкову енергію від РДГ для заряджання УЗЕ (до рівня 90%), після чого надлишок електроенергії використовується для живлення споживачів кластеру № 2. Добові графіки, отримані внаслідок моделювання ізольованого режиму агрегованої мікромережі за зимовим та літнім сценаріями наведено на рис. 2.



а) *б*)

Рисунок 2 – Результати моделювання ізольованого режиму агрегованої мікромережі:
а) зимовий сценарій; *б*) літній сценарій

Результати моделювання (рис. 2*а*) демонструють, що в умовах максимального навантаження досліджувана система здатна забезпечити безперебійне енергопостачання критичної інфраструктури протягом доби в ізольованому режимі. Висока сонячна активність дозволили використати генерацію СЕС у проміжках з 08:00 до 10:00 та з 11:00 до 16:00. Під час переходу до другої доби ізольованого режиму роботи, враховуючи значний розряд УЗЕ наприкінці першого дня, існує висока ймовірність виникнення дефіциту електроенергії для живлення споживачів кластеру №1, особливо за умов менш сприятливої погоди.

Результати моделювання за літнім сценарієм (рис. 2*б*) свідчать, що система здатна забезпечити живлення споживачів кластеру №1 протягом доби навіть за умов початкового заряду УЗЕ на рівні 30%. Висока сонячна активність, характерна для літнього періоду, сприяла стабільній генерації СЕС, що забезпечило живлення мікромережі з 05:00 до 20:00.

Протягом світлового дня забезпечується електроживлення усіх споживачів в повному обсязі. Вечірній період зниження потужності генерації призводить до поступового переходу до режиму забезпечення споживачів критичної інфраструктури за рахунок електроенергії УЗЕ. Наприкінці доби рівень SOC УЗЕ становить 78%, що свідчить про збереження достатнього запасу електроенергії для забезпечення споживачів кластеру №1 у разі повторення ізольованого режиму наступної доби.

Висновки

Результати виконаних досліджень свідчать про можливість використання дворівневої архітектури системи керування режимами агрегованих мікромереж з ситуативним (залежно від нормального чи ізольованого режиму роботи) розподілом функцій між рівнями системи.

Практична реалізація функцій диспетчеризації навантажень агрегованих мікромереж потребує наявності сучасної інформаційно-комунікаційної системи та множини телекерованих комутаційних пристроїв, що забезпечують вимкнення/увімкнення електроживлення споживачів різних кластерів.

Спроможність агрегованих мікромереж підвищувати резильєнтність локальних енергосистем залежить від характеристик компонентів мікромереж, насамперед від УЗЕ, визначення яких є окремою оптимізаційною задачею.

1. IEC TR 62898-4 Technical report. Microgrids – Part 4: Use cases. Edition 1.0 2023-04.
2. "IEEE Guide for Distributed Energy Resources Management Systems (DERMS) Functional Specification," in IEEE Std 2030.11-2021. doi: https://10.1109/IEEESTD.2021.9447316

В.М. Горбачук, М.С. Дунаєвський, Т.Г. Голоцукова, Д.О. Рибачок

СТАНДАРТИ ТА ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ КІБЕРБЕЗПЕКИ

Хоча штучний інтелект (ШІ) пропонує суттєві можливості для кібербезпеки, ШІ водночас генерує сценарії, в яких його можна використовувати для долання відомих заходів безпеки [1]. Умови таких сценаріїв часто включають витончені процедури, які експлуатують властиві вразливості самих систем ШІ. Можна вказати кілька ключових областей, де ШІ може потенційно обходити заходи кібербезпеки: 1) несприятливі атаки; 2) експлуатація (exploiting) вразливостей моделі ШІ; 3) розширені за допомогою ШІ методи атаки; 4) обмеження в робастності та пояснюваності ШІ.

1) Атаки з уникненням включають непомітне маніпулювання вхідними даними, що надходять у систему безпеки на основі ШІ. Зміни внаслідок цих атак нечасто сприйматимуться звичайною людиною, але можуть призводити до того, що ШІ невірно класифікуватиме шкідливий контент як безпечний. Приклади: модифікація пікселів у зображенні за допомогою зловмисного ПЗ, щоб уникати виявлення антивірусом на основі ШІ; деяка зміна слів у фішинговому електронному листі, щоб обходити спам-фільтр на основі ШІ.

Атаки з отруєнням включають введення зловмисних або маніпульованих даних у навчальний набір даних моделі безпеки ШІ. З часом це спотворюватиме навчання моделі, призводячи до невірних класифікацій нею чи розвитку її упереджень, які можуть експлуатуватися нападниками, пов'язаними з такими зловмисниками чи маніпуляторами. Подібні процеси спостерігалися і спостерігаються в інформаційних та гібридних війнах (проти України), зокрема у каскадному поширенні банківських панік і фінансових спекуляцій з метою пониження ринкової вартості активів суперника, у зловживанні інсайдерською інформацією, персональними даними, службовим становищем, ринковою владою, регуляторними лазівками [2].

Приклад: ін'єкція дещо змінених даних мережевого трафіку в систему виявлення вторгнень (атак) (Intrusion Detection System (IDS)) на основі ШІ призводитиме, врешті-решт, до того, IDS пропускатиме справжні атаки, схожі на попередньо отруєні дані (викривлену інформацію) [3].

2) В атаках інверсії моделі зловмисники намагаються реконструювати чутливу (конфіденційну) інформацію від самої моделі ШІ, аналізуючи її виходи та поведінку у відповідь на різні вхідні дані. Це потенційно може розкривати деталі про навчальні дані чи внутрішні параметри моделі.

В атаках крадіжки моделі зловмисники намагаються відтворювати пропрієтарну модель ШІ, спостерігаючи за її передбаченнями на великій кількості запитів. Після створення достатньо точної копії зловмисники можуть аналізувати її слабкі сторони (скажімо, проводити SWOT-аналіз) та розробляти цілеспрямовані атаки [4].

У бекдор-атаках зловмисники можуть навмисно вводити (запроваджувати) приховані вразливості (бекдори (backdoors; задні входи)) у моделі ШІ під час їх навчання. Ці бекдори (законсервовані агенти) можуть активуватися специфічними, часто непримітними сигналами (з використанням побутової техніки чи звичайних індивідуальних пристроїв), дозволяючи нападникам обходити нормативні функції безпеки моделі.

3) ШІ можна використовувати для автоматизації та персоналізації атак соціальної інженерії, що підсилює їх вплив та ускладнює їх своєчасне виявлення. Ці атаки включають складання досить цілеспрямованих фішингових електронних листів, створення реалістичних дипфейків для видавання себе за іншу особу (impersonation), автоматизацію спілкування з жертвами (особливо коли інтереси жертви зводяться до найпростіших), формування асоціальної (надмірно ризикованої) чи віктимної поведінки об'єкта розробки. Приклад: ШІ може аналізувати соціальні медіа та професійні профілі цільової особи (об'єкта розробки), щоб створювати достатньо персоналізований фішинговий електронний лист, що переконливо імітує довіреного колегу чи сервіс, який особа нечасто перевіряє [5].

Зловмисники можуть інтегрувати ШІ у зловмисне ПЗ, щоб підвищувати його спроможність уникати перевірок і здатність пристосовуватися. Таке ПЗ на основі ШІ може вивчати поведінку цільової особи (системи) та засоби захисту кібербезпеки, дозволяючи модифікації у своєму коді чи дії, щоб уникати свого виявлення.

Коли ШІ використовується для ефективнішого сканування мереж і систем, ідентифікації та автоматизованої експлуатації вразливостей, автоматизації процесів розвідки (reconnaissance), то швидкості та масштаби атак можуть істотно прискорюватися [6].

Оскільки моделям ШІ, особливо моделям глибокого навчання, іноді важко узагальнювати (усвідомлювати) нові чи невідомі типи атак, дані яких відрізняються від навчальних даних цих моделей, то нападники можуть експлуатувати такі обмеження в робастності та пояснюваності ШІ шляхом розробки новітніх методів атак [7].

4) Те, що деякі моделі ШІ за своєю природою є «чорними скриньками», ускладнює розуміння, чому вони приймають ті чи інші рішення. Така обмежена пояснюваність ШІ і такий брак прозорості може перешкоджати виявленню атак противника й аналізу неочікуваної поведінки.

Спеціальна тема «Машинне навчання на даних суперника» (Adversarial Machine Learning) зосереджується на розумінні та вірогідному виправленні вищезазначених вразливостей у системах ШІ. Активно ведуться дослідження і розробки більш робастних моделей ШІ, резильєнтних відносно несприятливих атак, та методів виявлення і захисту від кіберзагроз, розширених на основі ШІ. Ці методи захисту включають навчальні дані суперника (щоб власні моделі ШІ вчилися розпізнавати дані, структури і приклади суперників), очищення (sanitization) вхідних даних, виявлення аномалій, процедури пояснюваності для кращого розуміння прийняття рішень на основі ШІ. Оскільки ШІ продовжує інтегруватися в засоби захисту кібербезпеки, то важливо брати до уваги також потенціал зловживання ШІ з боку різноманітних зловмисників. Тому суттєво розвивати проактивний та адаптивний підхід, який враховує виграші та витрати (ризики) ШІ з метою підтримки сильної позиції безпеки добросовісного громадянина, суспільства і держави в цілому [8].

Застосунки ШІ для захисту ПЗ і стандарти кібербезпеки генерують радше продукти-доповнювачі, ніж продукти-замінники: такі застосунки є додатковими суттєвими компонентами ефективної та робастної стратегії захисту ПЗ, торкаючись різних аспектів безпеки зі своїми перевагами та недоліками. Мета полягає у створенні засадничого фреймворку найкращих практик, стратегій та методів для управління і зменшення ризиків кібербезпеки. Згадані продукти забезпечують структурований підхід до безпеки по всій організації, включаючи розробку ПЗ.

Перевагами стандартів є проактивне управління ризиками: наприклад, стандарти ISO/IEC 27001 («Information technology − Security techniques − Information security management systems − Requirements»; відомі версії 2005, 2013, 2022 рр.) і NIST CSF (CyberSecurity Framework) (оприлюднюється з 2014 р.) допомагають організаціям систематично ідентифікувати, оцінювати та зменшувати ризики до того, як ці ризики можуть ставати предметами експлуатації (зловмисниками) в ПЗ.

Дотримання стандартів GDPR (General Data Protection Regulation; регулювання ЄС, яке оприлюднюється з 2016 р.), HIPAA (Health Insurance Portability and Accountability Act; закон США, прийнятий у 1996 р.) [9] та PCI DSS (Payment Card Industry Data Security Standard; оприлюднюється з 2004 р.) часто є юридичною чи нормативною вимогою, що гарантує базовий рівень безпеки (базовий рівень якості продукту) та допомагає уникати штрафів.

Настанови з найкращих практик кодифікують колективні знання та досвід, пропонуючи перевірені методи безпечних практик розробки ПЗ, контролю доступу, захисту даних та реагування на інциденти. Впровадження стандартів сприяє формуванню організаційної культури безпеки в команді розробників і в організації в цілому. Приклад: 19 вересня 2024 р. Національний координаційний центр кібербезпеки прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури України; подібні рішення в ЄС стали важливими для сусідніх з Україною держав.

Стандарти часто включають механізми аудиту та процеси перевірки менеджменту, які створюють фреймворк для загального вдосконалення і стимулюють постійне поліпшення практик безпеки. Водночас стандарти мають обмеження через свій статичний характер, іноді відстаючи від ландшафту загроз, що швидко розгортається, і не вдаючись до ефективної протидії новим або ускладненим атакам.

Ефективне впровадження та підтримання відповідності стандартам може бути складним, трудомістким і ресурсомістким процесом, потребуючи від організації досвіду виконання новаторських проектів [10]. Стандарти надають керівні принципи, але не є безпосередніми технічними рішеннями: стандарти безпосередньо не запроваджують засоби технічного контролю безпеки в самому ПЗ.

Реалізація застосунків ШІ для захисту ПЗ означає використання машинного навчання та інших методів ШІ для покращення виявлення загроз, автоматизації реагування та надання більш динамічних і адаптивних заходів безпеки для ПЗ. ШІ може аналізувати великі обсяги даних у режимі реального часу, щоб ідентифікувати аномалії, шаблони та ознаки зловмисної діяльності (зокрема новітні та витончені атаки), які традиційні системи на основі правил можуть пропускати.

Окремим питанням є можливість розробки чи вдосконалення стандартів кібербезпеки за допомогою ШІ, який демонструє свої переваги у кодифікації національних і міжнародних регулювань, що реагують на сучасні виклики.

1. Karp, A. C., Zamiska, N. W. (2025). The Technological Republic: Hard Power, Soft Belief, and the Future of the West. Crown Currency. 320 p.
2. Горбачук, В. М., Дунаєвський, М. С., Сирку, А. А., Сулейманов, С.-Б. (2017). Економіка кібербезпеки. Інформаційні технології та взаємодії (с. 207–208). Київ: Київський національний університет імені Т.Шевченка.
3. Мохор, В. В. (2023). Цифрова трансформація енергетики як запорука забезпечення її стійкості. Стенограма доповіді на засіданні Президії НАН України 4 жовтня 2023 р. Вісник НАН України, № 12, 74−79.
4. Горбачук, В. М., Голоцуков, Г. В, Дунаєвський, М. С., Сирку, А. А., Сулейманов, С.-Б. (2022). Теоретико-ігрові та оптимізаційні моделі і методи підвищення безпеки кіберінфраструктур. Проблеми керування та інформатики, № 2, 92−105.
5. Горбачук, В., Гавриленко, С., Голоцуков, Г., Ніколенко, Д. (2020). Економіка Internet-застосунків і цифрового контенту. In M. Gavron-Lapuszek, A. Karpenko (eds.), The Role of Technology in the Socio-Economic Development of the Post-Quarantine World (pp. 81–88). Katowice, Poland: Katowice School of Technology.
6. Горбачук, В. М., Бардадим, Т. О., Дунаєвський, М. С., Сулейманов, С.-Б. (2025). Розробка віртуальної АЕС та її застосування в ядерній безпеці. С. В. Литовченко (ред.), Проблеми сучасної ядерної енергетики (16–18 квітня 2025 р., м. Харків) (с. 62): Київ: Українське ядерне товариство.
7. Gorbachuk, V., Dunaievskyi, M., Suleimanov, S.-B. (2025). Cybersecurity investments in networks. In A. A. Gaivoronski, P. S. Knopov, V. I. Norkin, V. A. Zaslavskyi (eds.), Stochastic Modeling and Optimization Methods for Critical Infrastructure Protection, Volume 2: Methods and Tools (pp. 211−234). Wiley-ISTE.
8. Горбачук, В. М., Дунаєвський, М. С., Морозов, О. О. (2017). Рівноважні інвестиції у кібербезпеку мережі ланцюгів постачання. Вісник Київського університету. Серія: фізико-математичні науки, № 2, 47–52.
9. Горбачук, В., Скобцов, Ю., Том І. (2021). Економічні аспекти забезпечення здоров'я в інформаційну еру. In N. Dubrovina, S. Filip (eds.), National Health as Determinant of Sustainable Development of Society (pp. 697−720). Bratislava, Slovakia: School of Economics and Management in Public Administration.
10. Горбачук, В., Гавриленко, С. (2020). Вплив ціноутворення хмарних сервісів на прибуток провайдера, споживчий надлишок і суспільний добробут. *Проблеми програмування*, № 2−3, 237−245.

О.А. Снєосіков, О.П. Нарєжній

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ СИСТЕМ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ВІД КІБЕРАТАК

Глобальні навігаційні супутникові системи (GNSS) за останні роки перетворилися на один із ключових елементів у багатьох критично важливих галузях - від енергетики й телекомунікацій до залізничного транспорту, водопостачання, економіки, фінансів, логістики, оборонної сфери та сільського господарства. Вони забезпечують не лише точне визначення координат, а й синхронізацію часу, що є фундаментом для стабільної та ефективної роботи цих систем. Однак із дедалі глибшою інтеграцією GNSS у життєво важливу інфраструктуру зростає і рівень кіберзагроз. Такі загрози можуть серйозно вплинути на конфіденційність, цілісність і доступність як навігаційних даних, так і сигналів точного часу, що своєю чергою створює суттєві ризики як для операційних процесів, так і для безпеки в цілому.

Згідно із Законом України "Про критичну інфраструктуру" № 1882-IX від 15 листопада 2021 року, до переліку критично важливих сфер включено, зокрема, «15) космічну діяльність, космічні технології та послуги» [1]. Це безпосередньо стосується GNSS, адже глобальні навігаційні супутникові системи є ключовим елементом космічних технологій і забезпечують надання життєво важливих послуг, що мають суттєве значення для національної безпеки, економіки та соціальної стабільності.

Основний перелік споживачів технологій GNSS включає автомобільні навігаційні системи, смартфони та планшети, логістичні та транспортні компанії, повітряну та морську навігацію, туризм і активний відпочинок, сільське господарство, наукові дослідження, аварійно-рятувальні служби, спортсменів та фітнес-програми, банківський сектор, бізнес-корпорації та служби доставки.

Кіберзагрози, спрямовані на GNSS, можуть призводити до спотворення сигналів, перехоплення навігаційних даних або повної втрати орієнтації користувачів, що становить серйозну небезпеку для стабільної роботи критичної інфраструктури. Порушення синхронізації часу в системах, які покладаються на GNSS, здатне спричинити масштабні збої в енергетичних мережах, телекомунікаційних системах, фінансовому секторі, а також у сфері авіаційної та морської навігації.

Транспортні системи, енергетика, аеропорти та морські порти дедалі стають об'єктами підвищеного ризику, оскільки їхнє функціонування значною мірою залежить від точних і достовірних даних GPS [2]. Враховуючи це, кібератаки на GPS можуть мати значні наслідки для суспільної безпеки та економічної стабільності країни [3]. У зв'язку з цим, забезпечення захисту GPS залежних систем стає надзвичайно важливим для підтримки функціонування цих критично важливих сфер та забезпечення національної безпеки.

Основні загрози на GNSS:

- Глушіння сигналів (GPS jamming) [3]: застосування перешкод потужністю понад −80 dBm повністю блокує навігацію, морський транспорт, автотранспорт та інші галузі.
- Спуфінг сигналів (GPS spoofing): підміна сигналів з метою дезорієнтації або для шахрайських схем.
- Кібератаки на наземну інфраструктуру GNSS [4,5], такі як DDoS-атаки, Атаки типу "людина посередині" (MitM), Фішинг, SQL-ін'єкції, Атаки з переповнення буфера, Шкідливе ПЗ (малваре), Атаки на VPN-інфраструктуру, Атаки на протоколи передачі (наприклад, NTRIP), та інші кібератаки.

Запропоновані моделі та методи захисту:

- Інтеграція GNSS з інерціальними навігаційними системами (ІНС) через фільтр Калмана [6] для перевірки достовірності даних. Ця комбінація дозволяє виявляти та протидіяти атакам типу спуфінгу та глушіння;
- Моніторинг співвідношення сигнал/шум (SNR): сигнал ≥10 dB-Hz вище норми – може свідчити про спуфінг-атаку;
- Автентифікація GNSS на рівні сигналу Galileo CAS (E6-C) [7], завдяки чому через перевірку отриманих навігаційних сигналів, можна підвищити захист від спуфінгу та інших видів атак на системи GNSS;
- Створення кіберзахищеної інформаційно-комунікаційної системи (ІКС) з підтримкою TLS 1.3, VPN (WireGuard), IDS/IPS, сегментації мереж та захищеного вебсервера;
- Впровадження та використання національних постквантових стандартів: «Калина» (ДСТУ 7624:2014), «Скеля», «Вершина», «Купина».
- Застосування квантового генератора (QRNG) для генерації криптоключів.

Отже, стрімке зростання використання глобальних навігаційних супутникових систем (GNSS) супроводжується відповідним збільшенням кількості та складності кіберзагроз, які здатні порушити стабільну роботу критичної інфраструктури та створити серйозні ризики для безпеки населення. Особливу небезпеку становить поява високотехнологічного нелегального обладнання, що значно розширює можливості зловмисників щодо реалізації атак. Серед найпоширеніших загроз — підміна сигналів (GPS spoofing), їх глушіння (GPS jamming), а також спроби несанкціонованого доступу до інформаційно-комунікаційних систем (ІКС) автономних систем диференціальної корекції (Autonomous DGNSS). Подібні атаки суттєво ускладнюють функціонування таких галузей, як автомобільний транспорт, логістика, агропромисловий комплекс, малий і великий бізнес. Це, у свою чергу, актуалізує потребу в системному посиленні кіберзахисту GNSS-інфраструктури.

У цій роботі представлено основні підходи до розробки моделей захисту та методів протидії таким кібератакам, зокрема посилення кібербезпеки цих систем у постквантову еру завдяки пропозиції застосування постквантових криптографічних стандартів та квантового генератора випадкових чисел (QRNG).

Запропоновані методи спрямовані на забезпечення надійності, цілісності та доступності даних критичної інфраструктури GNSS. Подальші дослідження передбачають практичне впровадження і верифікацію запропонованих засобів захисту в реальних умовах з метою оцінки їх ефективності проти динамічно змінюваних кіберзагроз.

1. Закон України «Про критичну інфраструктуру» № 1882-IX (2021). https://zakon.rada.gov.ua/go/1882-20.
2. Westbrook T. A.(2023). Taxonomy of Radio Frequency Jamming and Spoofing Strategies and Criminal Motives. *Journal of Strategic Security*, 16(2), 68-80. https://doi.org/10.5038/1944-0472.16.2.2081.
3. Westbrook T.(2019) The Global Positioning System and Military Jamming: The geographies of electronic warfare. *Journal of Strategic Security*. Вип. 12(2) 1-16. https://doi.org/10.5038/1944-0472.12.2.1720.
4. Shumilova, Kateryna. (2022). НАВІГАЦІЙНІ РИЗИКИ В АСПЕКТІ КІБЕРБЕЗПЕКИ ТРАНСПОРТНИХ СУДЕН І ВІЙСЬКОВИХ КОРАБЛІВ. *InterConf*. 391-408. 10.51582/interconf.19-20.08.2022.037.
5. BleepingComputer.(2020). *Garmin outage caused by confirmed WastedLocker ransomware attack*. https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/.
6. Li, Shuo & Mikhaylov, Maxim & Mikhaylov, Nikolay & Pany, Thomas. (2023). Deep Learning Based Kalman Filter for GNSS/INS Integration: Neural Network Architecture and Feature Selection. 1-7. 10.1109/ICL-GNSS57829.2023.10148914.
7. European GNSS Service Centre. (2019). European Union, Galileo E6-B/C Codes Technical Note. https://www.gsc-europa.eu/sites/default/files/sites/all/files/E6BC_SIS_Technical_Note.pdf.

С.В. Кулик, А.В. Давидюк

ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСАХ МІГРАЦІЇ ДАНИХ

У міру розвитку технологій штучного інтелекту (далі - ШІ) зростає кількість інструментів міграції даних, які включають алгоритми машинного навчання, прогнозування ризиків та адаптивного реагування. З огляду на це метою даного дослідження єаналіз сучасногопрограмного забезпечення (далі -ПЗ) з ШІ, що реалізує ключові функції – моніторинг, прогнозування ризиків, оптимізацію рішень і адаптацію – які є критично важливими під час процесів міграції даних. Здійснено аналіз функціональних компонентів сучасного ПЗ, що використовує ШІ для автоматизації та підвищення ефективності ключових етапів міграції — зокрема профілювання, трансформації, адаптації, контролю цілісності та виявлення аномалій. Показановаріанти використання моделей ШІ, що дозволяють реалізувати високоточні й масштабовані сценарії обробки, адаптації та перенесення даних між джерелами початкових даних й цільовими системами. Проведено порівняльний огляд відповідного ПЗ, охарактеризовано існуючі ШІ-компоненти та типові алгоритми. Отримані результати можуть бути покладені в основу подальшої розробки методик оцінки функціональності ШІ у сфері захищеної міграції даних.

Міграція даних у межах гетерогенної інфраструктури супроводжується значними викликами з точки зору надійності, безпеки, відповідності нормативам та забезпечення безперервності бізнес-процесів. Традиційні підходи часто не здатні оперативно реагувати на зміну умов інфраструктури чи кіберзагроз. У цьому контексті технології ШІ виступають як інструмент для контролю якості даних, скорочення простоїв і обробки складних трансформацій у режимі реального часу.

ШІможе відігравати ключову роль у підвищенні ефективності процесів міграції даних, забезпечуючи автоматизоване профілювання й очищення інформації, що включає виявлення дублікатів, заповнення пропусків і виправлення помилок у наборах даних за допомогою методів кластеризації (наприклад, K-Means [1], DBSCAN [2]) та моделей імовірнісного висновку: в контексті міграції даних, ці моделі дозволяютьробити припущення про відсутні або суперечливі записи, оцінювати вплив зміни схеми бази даних на її цілісність та виявляти потенційні збої в процесі на основі історичних шаблонів [3].

За допомогою ШІ може бути реалізовано інтелектуальне відображення та трансформація структури даних, що суттєво зменшує потребу в ручному втручанні при зіставленні схем і полів між початковими джерелами данихта цільовими системами, зокрема завдяки алгоритмам глибокого навчання, як-от Sequence-to-Sequence (Seq2Seq) моделі та трансформери (наприклад, T5 або BERT для задач семантичного зіставлення) [4].

Паралельний аналіз логічних і функціональних залежностей у структурованих даних забезпечується за допомогою графових нейронних мереж (GraphNeuralNetworks, GNNs), які демонструють здатність моделювати взаємозв'язки між сутностями в гнучкій та адаптивній формі. Згідно з дослідженням [5], GNN реалізує концепцію агрегації інформації від сусідніх вузлів графа, дозволяючи зберігати структурний контекст та підтримувати цілісність зв'язків між об'єктами у процесі трансформації або переносу даних. Це особливо важливо при роботі з гетерогенними структурами даних, де традиційні моделі не здатні врахувати змінність кількості сусідів чи топологічні особливості. GNN дозволяють реалізовувати функцію індуктивного навчання на нових графових структурах, що підвищує їхню придатність до задач міграції даних між різними системами, не вимагаючи ручного кодування залежностей. Структура таких моделей включає в себе компоненти, які поєднують локальну агрегацію, нелінійну трансформацію та можливість глибокої багаторівневої репрезентації, що підтверджено на практиці в задачах класифікації, прогнозування та семантичного зіставлення. Таким чином, використання GNN у процесах міграції даних дозволяє забезпечити збереження логічної структури, виявлення аномалій зв'язків та підвищення якості відповідності між початковими джерелами даних та цільовими системами.

На завершальному рівні процесу міграції даних може бути впроваджено механізми постійного контролю відповідності політикам безпеки та бізнес-вимогам, що реалізується за допомогою алгоритмів виявлення аномалій у режимі реального часу. До найефективніших відносяться методи, засновані на глибоких автоенкодерах, класифікаторах XGBoost, а також ізоляційних дерев (IsolationForest). Зокрема, алгоритм IsolationForest, на відміну від традиційних підходів, не створює профіль нормальних даних, а спеціалізується на ізоляції аномальних зразків, що, як показано у роботі [6], дає змогу досягати високої точності при низькому навантаженні на пам'ять та із лінійною обчислювальною складністю. Завдяки особливості ізолювати «рідкісні та відмінні» дані поблизу кореня дерева, цей підхід ефективно справляється зі складними випадками в умовах великих обсягів та високої розмірності даних. Механізм коротших середніх шляхів у дереві дозволяє формувати інтегральну оцінку аномальності, що може бути використана як сигнал для запуску механізмів реагування на потенційні загрози цілісності або витоку даних під час їх переміщення.

Застосування таких методологій ШІ сприяє побудові самоналагоджуваних, адаптивних систем, які здатні до самостійного навчання на нових патернах поведінки даних без залучення експертів на кожному етапі.

З урахуванням того, що на сьогодні вже розроблено низку програмних рішень, які інтегрують технології ШІ для підвищення ефективності процесів міграції даних, доцільно здійснити узагальнений огляд на прикладі таких ПЗ, що реалізують ключові функціональні компоненти відповідно до сучасних вимог стійкості, адаптивності та контролю.

Таблиця 1 – Огляд ПЗ, що використовує ШІ для міграції даних

ПЗ	Призначення	Алгоритми
Datafold [7]	Автоматична перевірка якості під час міграції	Моделі глибокого навчання, такі як згорткові нейронні мережі (CNN), для аналізу структурних змін у базах даних [8]
QASourceDataMigrationTool [9]	Тестування та відповідність при міграції	Алгоритми класифікації та виявлення аномалій, такі як IsolationForest.
AlibabaCloud AI Migrations [10]	Оптимізація процесу міграції	Алгоритми кластеризації та прогнозування для виявлення залежностей і оптимізації процесу міграції.
KNIME [11]	Аналітика і трансформація даних	Підтримує алгоритми класифікації, кластеризації та регресії для аналізу та трансформації даних.
RapidMiner [12]	Підготовка та аналіз даних	Підтримує широкий спектр алгоритмів, включаючи дерева рішень, нейронні мережі та методи кластеризації.

На сьогодні в Україні впровадження ШІ у роботі дата-центрів перебуває на початковому етапі. Хоча деякі хмарні провайдери починають інтегрувати ШІ для оптимізації енергоспоживання та моніторингу, широке використання цієї технології ще не стало поширеним явищем.Впровадження ШІ в українських центрах обробки даних [13] є обмеженим через різноманітність інженерної інфраструктури та необхідність значних інвестицій. Більшість систем моніторингу лише повідомляють про необхідність втручання, але не автоматизують процеси реагування повністю. Деякі українські дата-центри починають використовувати ШІ для оптимізації енергоспоживання та моніторингу систем. Наприклад [14], компанія SchneiderElectric пропонує рішення для оптимізації інфраструктури дата-центрів за допомогою ШІ, що дозволяє зменшити вплив на навколишнє середовище та підвищити енергоефективність.

Інтеграція ШІ в процеси міграції даних створює передумови для формування нової архітектури управління стійкістю інформаційних потоків в умовах високих ризиків. На основі такого огляду сучасного ПЗ можна виокремити чотири базові функції, що ним реалізуються, а саме моніторинг, прогнозування ризиків, оптимізація рішень та адаптація до змін, реалізація яких із застосуванням ШІ забезпечує зростання рівня точності, швидкодії та автономності в управлінні процесами міграції. Кожна з цих функцій уже знаходить практичне застосування у спеціалізованих інструментах, що використовують алгоритми машинного навчання, глибокі нейронні мережі та методи виявлення аномалій.

ШІ стає важливою складовою безпечної, ефективної та адаптивної міграції даних, особливо для об’єктівкритичної інфраструктури. Із зростанням складності та масштабів міграційних сценаріїв, інтелектуальні системи стають необхідністю.

1. MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In L. M. Le Cam & J. Neyman (Eds.), *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability* (Vol. 1, pp. 281–297). University of California Press. https://projecteuclid.org/euclid.bsmsp/1200512992.
2. Ester, M., Kriegel, H.-P., Sander, J., & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. In *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD'96)* (pp. 226–231). AAAI Press. https://www.aaai.org/Papers/KDD/1996/KDD96-037.pdf.
3. Hua, C., Luan, S., Zhang, Q., Fu, J., & Wolf, G. (2025). Graph neural networks meet probabilistic graphical models: A survey. У *ICASSP 2025 - 2025 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (с. 1–5). IEEE. https://doi.org/10.1109/icassp49660.2025.10889283.
4. Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., &Liu, P. J. (2020). *Exploring the limits of transfer learningwith a unifiedtext-to-texttransformer*. Journal of Machine Learning Research. https://jmlr.org/papers/volume21/20-074/20-074.pdf.
5. Ye, Z., Kumar, Y. J., Sing, G. O., Song, F., & Wang, J. (2022). A Comprehensive Survey of Graph Neural Networks for Knowledge Graphs. IEEE Access, 1. https://doi.org/10.1109/access.2022.3191784.
6. Liu, F. T., Ting, K. M., &Zhou, Z.-H. (2008). *Isolationforest.* У 2008 eighth IEEE international conference on datamining (ICDM). IEEE. https://doi.org/10.1109/icdm.2008.17.
7. *Datafold migration agent - datafold*. (б. д.). Welcome - Datafold. https://docs.datafold.com/data-migration-automation/datafold-migration-agent.
8. *Convolutional neural networks (cnns): A deep dive - viso.ai*. (б. д.). viso.ai. https://viso.ai/deep-learning/convolutional-neural-networks/.
9. *Enhancing data migration testing with AI in 2024*. (б. д.). Best QA and Testing Blogs. https://blog.qasource.com/enhancing-data-migration-with-ai-a-strategic-approach.
10. *Jingdong: Flink SQL optimization practice*. (б. д.). Alibaba Cloud Community. https://www.alibabacloud.com/blog/ai-powered-migrations-employing-machine-learning_598235.
11. *How AI changed my way of working with data | KNIME*. (б. д.). KNIME. https://www.knime.com/blog/how-AI-changed-my-way-of-working-with-data.
12. *How data lineage ensures effective AI governance*. (б. д.). Default. https://altair.com/blog/articles/how-data-lineage-ensures-effective-ai-governance.
13. Гогілашвілі, Є. (2023, 29 вересня). *Коли в українських датацентрах з’явиться ШІ*. Speka - онлайн-медіа про підприємництво та технології | SPEKA.media | SPEKA.media. https://speka.media/koli-v-ukrayinskix-datacentrax-zyavitsya-si-p0kolv.
14. *Як ШІ впливає на дата-центри: Проблеми та рекомендації від SchneiderElectric*. (2024, 16 серпня). nv.ua. https://nv.ua/ukr/ukraine/events/revolyuciya-shi-v-data-centrah-shlyahi-optimizaciji-energospozhivannya-ta-stiyki-rishennya-vid-schneider-electric-50438465.html.

О.С. Потенко

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

У рамках нормативних документів технічного захисту інформації (НД ТЗІ), профіль захищеності є ключовим елементом для встановлення вимог та характеристик безпеки, які повинні бути виконані інформаційною системою або окремим технічним засобом для забезпечення ефективного захисту інформації. Це своєрідний стандарт, що окреслює набір функцій та заходів, які гарантують захист даних від несанкціонованого доступу, модифікації чи витоку.

Важливим аспектом є те, що стандартні функціональні профілі створюються на основі актуальних вимог до захисту конкретної інформації від відомих загроз. Вони включають ті функціональні можливості та послуги, які здатні нейтралізувати ці загрози та забезпечити відповідність стандартам захисту. Розробка таких профілів дозволяє створити ефективну архітектуру захисту, яка є адаптованою до актуальних ризиків.

Ключовим моментом є те, що для стандартних функціональних профілів захищеності не вимагається розробка окремої політики безпеки чи додаткових рівнів гарантій, хоча наявність цих елементів може бути доцільною за необхідності. Політика безпеки, що супроводжує систему, яка реалізує стандартний профіль, зазвичай «успадковується» з існуючих нормативних документів, що регламентують обробку інформації в автоматизованих системах. Це означає, що один і той же профіль захищеності може бути застосований як для опису вимог до захисту інформації в операційних системах, так і в системах управління базами даних (СУБД), хоча специфіка політики безпеки та об'єкти захисту можуть дещо відрізнятися.

У цьому контексті важливою є роль методів визначення функціональних профілів захисту, оскільки вони дають змогу системно підходити до забезпечення безпеки автоматизованих систем. Завдяки цим методам, організації можуть стандартизувати підходи до захисту, враховуючи різноманітні загрози і забезпечуючи належну надійність системи. Зокрема, ці методи дозволяють точно визначити, які саме функціональні характеристики повинні бути вбудовані в систему для ефективного захисту від несанкціонованого доступу, що в свою чергу забезпечує відповідність вимогам законодавства та стандартів безпеки. Далі проаналізуємо ці методи.

Стандартний метод, представлений у НД ТЗІ 2.5-004-99, простий і зручний завдяки готовим шаблонам та можливості уточнення вибору за призначенням АС. Проте є недоліки: складність аналізу безпеки та відсутність чіткого зв'язку між загрозами та заходами захисту [1].

А.В. Лєншин запропонував два методи для аналізу функціональних профілів безпеки: метод перевірки несуперечностей та метод побудови таксономії функцій безпеки. Метод перевірки несуперечностей швидкий і простий, але потребує висококваліфікованих фахівців для точної оцінки безпеки [2] . Метод таксономії дозволяє визначити ієрархію та співвідношення рівнів захисту і є корисним для системного аналізу вимог до безпеки, але вимагає значних ресурсів і часу [1].

Метод паретооптимальних ФПЗ [3] дозволяє обрати рішення, які забезпечують найкращий рівень захисту при оптимальних витратах. Недоліки методу — потреба у високій кваліфікації експертів і великий час на визначення ФПЗ. Переваги — можливість графічного представлення ФПЗ.

У роботі [4] запропоновано вдосконалений метод автоматизації визначення ФПЗ в ІТС, що дозволяє швидко і ефективно проводити аналіз при середньому рівні кваліфікації експерта.

Метод визначення функціонального профілю захисту автоматизованої системи (ВФПЗАС)[5], який базується на принципі оптимальності Беллмана та виміру математичного очікування успішної протидії окремої функціональної послуги безпеки, дозволяють у формальному вигляді сформувати необхідний набір величин для реалізації процесу вибору рівня захисту.

Таблиця 1 – Результати дослідження

Метод побудови ФПЗ	Витрати (рівень)	Використання стандартних ФПЗ	Використання нестандартних ФПЗ	Часові витрати	Кваліфікація експерта	Чисельне вираження ФПБ
Стандартний метод	високий	+	+	високі	середня	-
Метод перевірки несуперечності та повноти	високий	-	+	високі	висока	-
Метод побудови таксономії	високий	-	+	високі	висока	-
Метод парето-оптимальних ФПЗ	високий	-	+	високі	висока	-
Удосконалений метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР	невисокі	+	+	середні	середня	-
Метод ВФПЗАС	невисокі	+	+	низькі	середня	+

У табл. 1 представлено зведений аналіз методів за ключовими параметрами, зокрема: витратами, можливістю застосування як стандартних, так і нестандартних форм представлення знань (ФПЗ), рівнем кваліфікації експерта, способом вираження інформації та часовими витратами, що були розглянуті в межах даного дослідження.

Функціональний профіль захищеності (ФПЗ) відіграє ключову роль у розробці та впровадженні засобів інформаційної безпеки, оскільки саме він визначає вимоги до захисту автоматизованих систем. Існує кілька методів його побудови, кожен із яких має свої переваги та недоліки. Традиційні методи забезпечують високу точність, але потребують значних ресурсів і високої кваліфікації експертів, тоді як удосконалені та оптимізаційні підходи, зокрема метод ВФПЗАС, дозволяють зменшити витрати часу й ресурсів при збереженні достатнього рівня надійності, тому раціональний вибір методу залежить від конкретних вимог до захищеності, наявних ресурсів і підготовки фахівців.

1. Лєншин А.В., Буслов П.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу. Радіоелектронні і комп'ютерні системи. 2010. Вип. 7(48). С. 77–81. URL: http://nbuv.gov.ua/UJRN/recs_2010_7_15.
2. Потій О.В., Лєншин А.В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу. Науково-технічний журнал "Прикладна радіоелектроніка. Тематичний випуск, присвячений проблемам забезпечення інформаційної безпеки". 2010. Т. 9, №3. С. 479–488. URL: http://openarchive.nure.ua/handle/document/410.
3. Берестов Д. С., Гульков М. О., Козачок В. А. Побудова парето-оптимальних функціональних профілів захищеності. Збірник наукових праць. 2009. Вип. 1.39. С. 89-94.
4. Юдін О. К., Бучик С. С., Мельник С. В. Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу. Наукоємні технології. 2016. Вип. 2. С. 195-205.
5. Потенко О.С.. Визначення функціонального профілю захисту автоматизованої системи/ Потенко О.С. - К.: Інститут проблем моделювання в енергетиці ім. Г.Є Пухова НАН України, 2024. 146 с. ISBN 978-617-8579-06-7 (https://ipme.kiev.ua/books/Monog-VFPZ-AS-Potenko-2024.pdf).

С.Ю. Максимов, С.Д. Винничук, О.О. Прилипко

ВИКОРИСТАННЯ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ОПТИМІЗАЦІЇ ЗОВНІШНЬОГОЕЛЕКТРОМАГНІТНОГО ВПЛИВУ ПРИ ЗВАРЮВАНІ В ВОДНОМУ СЕРЕДОВИЩІ

Зварні шви сучасних підводних металоконструкцій відповідального призначення часто за рівнем механічних властивостей не повинні поступатися швам, виконаним на суші. У той же час фізико-хімічні та металургійні процеси при зварюванні під водою протікають в важких, екстремальних умовах, що обумовлює складність отримання якісних з'єднань.

Попередні досліди з використанням спеціального складу порошкового дроту підтвердили ефективність цього напряму. Але чутливість технології до хімічного складу сталі та навіть незначних відхилень умов зварювання (солона чи прісна вода, її температура, глибина зварювання та інше) викликають необхідність спеціальних досліджень. При порушенні нормального перебігу процесу зварювання можливі виникнення різних дефектів у будові шва, які знижують механічні властивості шва та з'єднання загалом, особливо їх міцність.

Цей процес протікає тим сильніше, що більший гідростатичний тиск. Зміна умов зварювання істотно змінює структуру зварного з’єднання. При мокрому зварюванні під водою навколишнє середовище чинить подвійний ефект на механічні властивості металу зварних з’єднань. З одного боку, у результаті прискореного охолодження міцність зварних з’єднань зростає, з іншого боку, знижується їх пластичність.

Усунення цього недоліку можливо металургійним шляхом, а саме легуванням металу швів для одержання необхідної мікроструктури. Одним із основних впливів водного середовища – це газонасичення воднем і киснем зварювальної ванни, що призводить до утворення пор в металі шва і холодних тріщин в зоні термічного впливута формування структури з високим ступенем недосконалості.

Альтернативою металургійному підходу може служити створення умов примусової дегазації зварювальної ванни та збільшення часу її існування шляхом застосування зовнішнього електромагнітного впливу (ЗЕВ). Перемішування зварювальної ванни в результаті (ЗЕВ) чинить суттєвий вплив на процес кристалізації розплавленого металу, газообмінні реакції і формування структури металу шва [1-3].

Важливою складовою параметрівЗЕВ є індукційні струми, вимірювати які і аналізувати їх внесок у зварювальний процес безвідповідного математичного опису, програмних засобів та імітаційних моделей дуже важко, а частіше – неможливо.

При моделюванні процесів, що протікають при дуговому зварюванні з використаннямЗЕВ, однією з найважливіших шуканих величин є густина вихрових струмів у масивнихтілах. Ці струми суттєво впливають на магнітне поле індуктора і, як наслідок, на розподілелектродинамічних зусиль у потоках розплаву ванни. В даний час існує ряд чисельнихметодів, які дозволяють моделювати електромагнітну дію на рідкий метал при підводномудуговому зварюванні.

Для подальшого вдосконалення технології механізованого підводного зварювання буловикористано методи математичного моделювання, як найбільш раціональні для оптимізаціїекспериментальних досліджень в умовах водного середовища. Математичні моделідозволили врахувати вплив як первинних чинників, а саме заданий струм і напругу взварювальному ланцюгу і індукторі, властивості матеріалів і умови протікання процесу, такі вторинних - формування структури металу шва і зони термічного впливу і властивостізварного з'єднання.

Максимальне підвищення технологічних та фізико-хімічних властивостей зварних з’єднань досягається у певному діапазоні параметрів електромагнітного впливу. Для цього за заданою геометрією системи, фізичними характеристиками матеріалів, з яких виготовлені конструктивні елементи, електричному з'єднанню елементів, заданими струмами в первинних обмотках необхідно визначити розподіл електродинамічних зусиль в рідкому провіднику - розплаві ванни. В загальному випадку моделювання розподілу електродинамічних зусиль в потоках розплаву ванни є складною задачею, що включає моделювання розподілу самого зварювального струму, моделювання зовнішнього електромагнітного поля в потоках ванни з урахуванням впливу вихрових струмів, моделювання розподілу електродинамічних зусиль в зварювальній ванні.

Розроблений алгоритм дозволяє спростити процес розрахунків для оптимізаціїтехнологічного процесу і підвищення якості зварного виробу. За допомогою розробленоїпрограми на мові Delphi 7 проведені чисельні експерименти із дослідження поведінкирідкого металу в зварювальній ванні залежно від параметрів зовнішньогоелектромагнітного впливу і режимів зварювання [4-6].

Вирішення проблеми ефективності процесу дугового зварювання з дією керуючихмагнітних полів дозволить підвищити продуктивність процесу. Проведені дослідженняпідтвердили ефективність використання ЗЕВ в умовахзварювання під водою для усунення негативного впливу гідростатичного тиску та водногосередовища.

Проведені раніше експерименти показали значне зниження розмірів пор і їх більш рівномірне розташування в об’ємі металу зварних швів, зменшення параметра кристалічної ґратки. Однак механізм впливу магнітного поля на структурні перетворення в металі зварних швів є мало вивченим.

Мета роботи - дослідження впливу дії зовнішнього електромагнітного поля на мікроструктуру, фазовий склад, дислокаційну структуру металу зварних з'єднань низьколегованої сталі при зварюванні під водою. Дослідження структури проводили методами оптичної металографії (мікроскопи Neophot32 і Versamet-2,

Японія) і трансмісійної електроної мікроскопії (ТЕМ, мікроскоп JEM200CX фірми JEOL, Японія). Твердість (HV, МПа) вимірювали на твердомірі М-400 (фірми Leco, США).

Співставленням структури металу з ЗЕВ при порівнянні з варіантом без ЗЕВ встановлено, що у центрі шва ширина кристалітів зменшується практично у 2 рази. Поблизу лінії сплавлення (метал шва), а також в ЗТВ відбувається подрібнення зеленної та пакетної структури в 1,3…1, 4 рази. При цьому в металі ЗТВ спостерігається зниження мікротвердості. Така структура забезпечує рівномірний рівень міцності і пластичності вздовж лінії сплавлення. Зіставленням особливостей тонкої структури досліджуваних зразків встановлено, що в металі варіанту без ЗЕВ спостерігаються найбільші градієнти за розмірами рейкових структур, а також по густині дислокацій, що може призводити до нерівномірного рівня механічних властивостей металу, підвищення рівня локальних внутрішніх напружень і, відповідно, зниження його тріщиностійкості.

У металі варіанту з ЗЕВ спостерігається диспергування структури при загальному зниженні і рівномірному розподілі дислокацій в об’ємі структурних складових. У металі ЗТВ зварного з'єднання варіанту з ЗЕВ спостерігається рівномірний розподіл густини дислокацій в об’ємі структурних складових, що не призводить до градієнтів внутрішніх напружень при відносно низькому їх рівні. Це, відповідно, буде забезпечувати високу тріщиностійкість зварних з’єднань [7,8].

Виконано аналіз впливу структурних факторів на дислокаційному рівні на зміну локальних внутрішніх напружень – зон локалізації деформації в структурах верхнього та нижнього бейніту для досліджуваних варіантів зварних з'єднань. Встановлено структурні умови одержання якісних зварних з'єднань при зварюванні низьколегованих сталей під водою, які забезпечують їх тріщиностійкість.

Найбільш прийнятна структура металу зварних з’єднань при зварюванні під водою формується в умовах застосування ЗЕВ, що забезпечує високий рівень механічних властивостей та тріщиностійкість зварних з'єднань. Контрольоване керування вимушеними переміщеннями потоків розплаву ванни при зварюванні з ЗЕВ дозволяє значно покращити механічні властивості швів, підвищити їх корозійну стійкість і стійкість проти утворення гарячих і холодних тріщин, знизити рівень пористості.

1. Рижов Р. Н., Максимов С. Ю., Приліпко Є. А. Вплив зовнішніх електромагнітних впливів на пористість швів при підводному мокрому зварюванні // Вест.НТУУ "КПІ".- 2006. - № 48. - С. 226-229.
2. Застосування зовнішніх електромагнітних впливів для покращення механічних властивостей швів при підводному мокрому зварюванні / Р. Н. Рижов, В. А. Кожухар, С. Ю. Максимов, Є. А. Приліпко // Автомат. зварювання.- 2004. - № 11. - С. 53-54.
3. Вплив зовнішнього електромагнітного впливу на вміст водню при мокрому підводному зварюванні / С. Ю. Максимов, Р. Н. Рижов, Е. А. Приліпко, В.А.Кожухар // Автоматичне зварювання.-2003.-№6.-С.55-56.
4. Євдокимов В.Ф., Максимов С.Ю., Петрушенко Є.І., Приліпко Є.А., Рибалкін Є.А.Тривимірна інтегральна модель розподілу зварювального струму при дуговому зварюванні зазору в пластині // Електронне моделювання.- 2008. - Т. 30. - № 6. - С. 3 - 18.
5. Максимов С.Ю., Петрушенко Є.І., Приліпко Є.А., Рибалкін Є.А.Інтегральне рівняння для моделювання розподілу синусоїдального струму в перерізі масивного осесиметричногобагатовиткового індуктора в режимі струму та напруги // Збірник наукових праць ІПМЕ ім.Г. Є.Пухова НАН України.- 2008. - Віп.45. - С. 60 - 69.
6. С.Ю.Максимов, О.О.Приліпко, О.М.Берднікова.Особливості формування структури при зварюванні під водою в умовах зовнішнього електромагнітного впливу Міжнародна конференція «Інноваційні технології та інжиніринг у зварюванні та споріднених процесах – PolyWeld 2021».27-28 травня 2021р.м. Київ.
7. А.Д.Розмишляєв, С.Ю.Максимов, О.О.Приліпко, О.М.Бердникова.С.Ю. О.С.Кушнарьова, Є.В.Половецький.Структура зварних з'єднань низьколегованих сталі при зварюванні пІл дією зовнішнього електромагнітного поля. Фізико-хімічна механіка матеріалів. Том 58 № 5, 2022. С.55-59
8. С.Ю.Максимов, О.О.Приліпко, О.М.Берднікова.Особливості формування структури при зварюванні під водою в умовах зовнішнього електромагнітного впливу Міжнародна конференція «Інноваційні технології та інжиніринг у зварюванні та споріднених процесах – PolyWeld 2021».27-28 травня 2021р.м. Київ.

В.М. Буняк, В.В. Лукічов

АНАЛІЗ ТЕОРЕТИЧНИХ ВЛАСТИВОСТЕЙ КРИТЕРІЮ ЕФЕКТИВНОСТІ КОНТРЗАХОДІВ В ЕНЕРГОМЕРЕЖАХ

Метою цієї роботи є докладне теоретичне дослідження критерію ефективності контрзаходів η_i, який визначається як відношення абсолютного зниження агрегованого ризику до нормалізованих ресурсних витрат. У межах аналізу сформульовано основні компоненти моделі, встановлено ключові аналітичні властивості функції η_i, а також обґрунтовано необхідність її мультикритеріального розширення ξ_i для гнучкого балансування між абсолютним і відносним зниженням ризику. Особлива увага приділена перевірці поведінки метрики в граничних сценаріях, властивості монотонності та інваріантності до масштабування одиниць виміру.

Для побудови моделі спочатку вводиться поняття агрегованого ризику до застосування контрзаходу, що позначається R_{before} і обчислюється як сума внесків усіх компонентів енергомережі з урахуванням ймовірності настання загрози P і потенційного збитку I для кожного вузла. Після врахування впливу заходу оновлений системний ризик R_{after} визначається за тими ж алгоритмічними кроками, але з модифікованими параметрами P та/або I у відповідних компонентах. Різниця між цими величинами,

$$\Delta R = R_{before} - R_{before}, \tag{1}$$

є показником абсолютного зниження ризику, яке забезпечується конкретним контрзаходом [1].

Паралельно із обчисленням ΔR для кожного заходу визначається його нормалізована вартість C_{norm}. Цей показник формується шляхом ділення фактичних ресурсних витрат на впровадження заходу на максимальну вартість серед усіх доступних опцій. Такий підхід дозволяє привести різнорідні показники витрат — фінансові, трудові, часові — до єдиної безрозмірної шкали, що забезпечує коректне порівняння ефективності заходів незалежно від їхніх початкових одиниць виміру [3]. Безпосередньо критерій η_i формується як відношення абсолютного зниження ризику до нормалізованої вартості заходу:

$$\eta_i = \frac{\Delta R}{C_{norm}}, \tag{2}$$

Це дозволяє оцінити «віддачу на одиницю витрат» для кожного контрзаходу й ранжувати заходи за спаданням цього показника. За значенням η_i вибирають ті заходи, які забезпечують найбільший зниження ризику за найменших ресурсних витрат, що є критичною вимогою за жорстких бюджетних обмежень [1].

Методика ранжування передбачає, що всі контрзаходи впорядковуються за спаданням значень η_i. Такий підхід гарантує оптимальне розподілення ресурсів між заходами: спочатку впроваджуються ті контрзаходи, які забезпечують максимальний приріст безпеки на кожну одиницю витрат, а вже потім — менш ефективні.

Водночас пряме відношення ΔR до C_{norm} не завжди враховує синергетичні ефекти від одночасного застосування декількох заходів. Для вирішення цієї проблеми вводиться мультикритеріальний показник ξ_i, який формується як лінійна комбінація відносного зниження ризику (ΔR до R_{before}) та абсолютного зниження ΔR з ваговими коефіцієнтами w_2 і w_2 [4]:

$$\xi_i = w_1 \cdot \left(\frac{\Delta R}{C_{norm}}\right) + w_2 \cdot \left(\frac{\Delta R}{R_{before}}\right) \tag{3}$$

Цей багатовимірний підхід дозволяє налаштовувати пріоритети залежно від стратегічних чи бюджетних вимог: можна посилити роль абсолютного виграшу в ризику або приділити більше уваги відносному зниженню [2].

Аналіз математичних властивостей критерію показав, що η_i є монотонною функцією від вхідних параметрів. Збільшення ймовірності загрози P або потенційного впливу I завжди призводить до зростання абсолютного зниження ΔR, а отже — до збільшення значення η_i. Це забезпечує логічне ранжування: найбільш критичні сценарії отримують вищий пріоритет у захисній стратегії [1].

Критерій також демонструє однорідність нульового порядку, тобто інваріантний до масштабних перетворень одиниць виміру витрат чи ризику. Якщо витрати виражаються в різних умовних одиницях — тисячах чи мільйонах гривень, днях або енергетичних одиницях — відношення ΔR до C_{norm} залишається незмінним, оскільки обидві складові масштабуються пропорційно. Це спрощує практичне застосування метрики у різних проєктах без необхідності адаптації формул.

Граничний аналіз поведінки η_i у крайових сценаріях доводить її коректність та внутрішню узгодженість. При $P \to 0$ або $I \to 0$ абсолютне зниження $\Delta R \to 0$, отже $\eta_i \to 0$, що відображає відсутність користі від контрзаходів за відсутності реальної загрози чи збитку. Натомість коли $P = 1$ та $I = 1$, абсолютне зниження ризику досягає максимальної величини, а η_i наближається до свого верхнього граничного значення, що гарантує правильне оцінювання «віддачі» навіть у надзвичайно критичних умовах.

Нерідко трапляються випадки, коли кілька контрзаходів застосовуються одночасно, і їхній комбінований ефект виявляється неадитивним: сумарне ΔR комбінації може бути більше або менше суми індивідуальних ΔR через перетинні чи синергетичні ефекти. Саме з метою врахування таких нелінійних взаємодій і було

розроблено мультикритеріальний показник ξ_i, який здатен коригувати приоритезацію заходів залежно від їхньої спільної дії та визначати оптимальні комбінації.

Практична реалізація критеріїв η_i і ξ_i передбачає їхню інтеграцію в моделі оптимізації кібер-фізичного захисту систем ICS/SCADA. Обидві метрики можуть бути безпосередньо включені в цільову функцію, поряд з технічними, економічними й часовими обмеженнями, що дозволяє одночасно мінімізувати системний ризик та оптимізувати розподіл ресурсів у складних мережевих середовищах із великою кількістю вузлів і потенційних загроз [1].

Критерії також можуть застосовуватися в режимі реального часу з використанням телеметрії SCADA-IDS. Потокові дані про події та зміну параметрів дозволяють оперативно коригувати значення P і I для кожного елемента мережі, перераховувати η_i та ξ_i та перегруповувати пріоритети контрзаходів у відповідь на динамічні зміни в кібер-фізичному середовищі. Це відкриває можливості для створення автоматизованих систем моніторингу та адаптивного управління безпекою [1].

Висновки. У результаті проведеного аналізу встановлено, що критерій η_i є міцно обґрунтованим інструментом для кількісного ранжування контрзаходів у енергомережах, забезпечуючи прозоре й інтуїтивно зрозуміле порівняння «віддачі на одиницю витрат». Мультикритеріальне розширення ξ_i додає необхідну гнучкість для стратегічного балансування між абсолютним і відносним зниженням ризику, що є ключовим для формування оптимального портфеля заходів.

Перспективи подальших досліджень включають валідацію описаних властивостей на цифрових двійниках та реальних сценаріях інтелектуальних енергомереж, розробку програмних модулів автоматизації розрахунку η_i і ξ_i для інтеграції в платформи SCADA-IDS, адаптацію алгоритмів до онлайн-режиму з урахуванням економічних показників CAPEX/OPEX та метрик стійкості типу MTTR/MTTF, а також дослідження синергетичних ефектів комбінованих заходів для підвищення резильєнтності енергосистем [5].

1. Kavallieratos G., Sppathoulas G., Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems // Sensors. — 2021. — Т. 21, № 5. — Арт. 1691. — DOI: 10.3390/s21051691.
2. Ahmad A., Hadwan M. H. M. Multi-criteria decision-making approaches for cybersecurity control selection in smart grids // Int. J. Crit. Infra. Prot. — 2020. — Т. 28. — С. 100–115. — DOI: 10.1016/j.ijcip.2020.100415.
3. Lahaye S., Borgianni Y., Guerriero F. Bayesian risk assessment framework for cyber-physical energy systems // Energies. — 2020. — Т. 13, № 18. — Арт. 4700. — DOI: 10.3390/en13184700.
4. Mousavi S., Sarreshtedari H. G. A fuzzy MCDM approach to cybersecurity control selection in power utility networks // Electr. Power Syst. Res. — 2019. — Т. 170. — С. 171–183. — DOI: 10.1016/j.epsr.2019.01.006.
5. Hosseini S., Barker K., Ramirez-Marquez J. E. A review of definitions and measures of system resilience // Reliab. Eng. Syst. Saf. — 2016. — Т. 145. — С. 47–61. — DOI: 10.1016/j.ress.2015.08.006.

О.О. Висоцька

ВИЯВЛЕННЯ ФІШИНГОВИХ САЙТІВ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Завдання виявлення фішингових сайтів є однією з пріоритетних проблем у сфері кібербезпеки, оскільки фішинг є основним методом соціальної інженерії, який спрямований на викрадення конфіденційних даних користувачів через підроблені веб-сайти [1-3].

Існує кілька основних підходів до вирішення проблеми виявлення фішингових сайтів, кожен з яких має свої особливості, переваги та недоліки.

Підхід на основі аналізу URL-адрес. Цей підхід орієнтований на виявлення фішингових сайтів шляхом аналізу характеристик URL-адреси. Фішингові сайти часто використовують схожі на оригінальні URL-адреси, зокрема з незначними змінами, щоб заплутати користувачів. Основні методи в рамках цього підходу:

- Аналіз довжини URL: фішингові сайти часто мають довгі та складні URL-адреси, які містять додаткові символи, числові значення та випадкові слова.

- Аналіз домену: перевірка наявності підозрілих піддоменів або субдоменів, що імітують відомі бренди. Наприклад, замість «bank.com» може бути використано «bank-login-secure.com».

- Перевірка на наявність IP-адрес у URL: фішингові сайти іноді використовують IP-адреси замість доменних імен, оскільки це дозволяє уникати блокувань.

- Аналіз на наявність підозрілих символів: фішингові URL часто містять символи «@», «-», «//» та інші, щоб створювати видимість легітимності, але це є однією з ознак фішингу.

Переваги та недоліки такого підходу: він дозволяє з високою швидкістю та достатньою точністю ідентифікувати потенційно фішингові сайти, проте він має обмеження, оскільки нові фішингові сайти можуть обходити такі перевірки, замінюючи деякі символи або використовуючи інші техніки маскування.

Підхід на основі аналізу контенту веб-сайту. Такий підхід передбачає перевірку внутрішнього контенту веб-сторінки для виявлення потенційних ознак фішингу. В рамках цього підходу використовуються такі методи:

- Аналіз ключових слів: фішингові сайти часто використовують певні слова чи фрази, що привертають увагу, такі як «увійдіть», «безпечно», «захист», які спрямовані на виклик довіри у користувачів.

- Аналіз форми авторизації: фішингові сайти здебільшого містять форми для введення особистих даних. Наявність полів для введення паролів, номерів кредитних карт тощо часто може слугувати ознакою фішингу.

- Перевірка схожості з легітимними сайтами: застосування методів порівняння зображення чи текстової схожості з відомими сайтами. Це можуть бути порівняння логотипів, кольорових схем, структури меню тощо.

Переваги та недоліків такого підходу: цей підхід забезпечує глибший аналіз, але потребує більше часу та обчислювальних ресурсів, що може знижувати його ефективність у реальному часі.

Підхід на основі аналізу метаданих. Аналіз метаданих включає перевірку різних показників сайту, які можуть бути ознаками фішингу. Метадані, такі як SSL-сертифікати, реєстраційні дані домену, інформація про сервер, дата створення та оновлення сайту, можуть свідчити про надійність або підозрілість ресурсу. Основні методи в рамках цього підходу:

- Перевірка SSL-сертифікатів: легітимні сайти зазвичай мають дійсні сертифікати SSL. Відсутність SSL або використання самопідписаних сертифікатів може вказувати на фішинговий сайт.

- Перевірка дати створення домену: багато фішингових сайтів мають новостворені домени, які використовуються протягом короткого періоду часу.

- Аналіз популярності домену: сайти з низькою кількістю відвідувачів можуть бути підозрілими, особливо якщо вони претендують на відомі бренди.

Переваги підходу: аналіз метаданих може ефективно працювати як додатковий фільтр, оскільки підроблені сайти не завжди проходять через надійний процес реєстрації.

Саме такі характеристики, як URL-адреса, контент веб-сайту та метадані, передаються в нейронну мережу для ефективного виявлення фішингових сайтів.

Машинне навчання та нейронні мережі. Сучасний і один із найефективніших підходів до виявлення фішингових сайтів ґрунтується на використанні машинного навчання та нейронних мереж. Машинні моделі, навчені на великих масивах даних про фішингові та легітимні сайти, можуть самостійно виділяти особливості та шаблони, характерні для фішингових ресурсів.

Основні етапи цього підходу:

- Вибір параметрів для навчання моделі: використовуються різні параметри URL, метадані, а також текстові та графічні ознаки. Кожна з цих ознак має свою вагу при ідентифікації фішингових сайтів.

- Вибір архітектури нейронної мережі: залежно від цілей аналізу можуть використовуватися різні архітектури, такі як рекурентні нейронні мережі (RNN), згорткові нейронні мережі (CNN), багатошарові перцептрони (MLP).

- Навчання та тестування моделі: Модель навчається на великій вибірці фішингових і легітимних сайтів для виявлення патернів, а потім проходить тестування на нових даних.

Такий підхід є ефективним завдяки здатності моделі адаптуватися до нових загроз, але в той же час він вимагає значних обчислювальних ресурсів для навчання і періодичного оновлення даних для підвищення точності.

Для ефективного застосування будь-якої нейронної мережі критично важливо правильно обрати параметри, які будуть аналізуватись для розпізнавання.

На основі проведеного дослідження, в котрому аналізувались 100 легітимних та 100 фішингових сайтів, були визначені наступні критичні ознаки, аналіз котрих є доцільним для виявлення фішингових сайтів:

1. Довжина URL та hostname: фішингові сайти мають довші URL, часто з додатковими піддоменами та параметрами.
2. Символи в URL: спеціальні символи, такі як «= , ;», частіше зустрічаються у фішингових сайтах.
3. Кількість піддоменів: фішингові сайти використовують більше піддоменів, часто для маскування.
4. Аномальні піддомени: фішингові сайти частіше мають підозрілі піддомени.
5. Префікси та суфікси в домені: частіше зустрічаються у фішингових сайтах.
6. Підозрілі TLD (Top-Level Domain): можуть свідчити про потенційний фішинг.
7. External favicon: зовнішні іконки частіше зустрічаються у фішингових сайтах.
8. Popup вікна: popup вікна майже однаково розповсюджені в обох типах сайтів, але в фішингових більше (найменш значимий параметр).
9. Safe anchor: фішингові сайти частіше використовують небезпечні прив'язки (unsafe anchors).
10. On mouse over: зустрічається лише у фішингових сайтах.
11. Загальна кількість посилань: фішингові сайти містять значно більше посилань.
12. Зовнішні посилання: велика кількість зовнішніх посилань – маркер фішингових сайтів.
13. Підозрілі скрипти: фішингові сайти частіше містять підозрілі скрипти.
14. Підозрілі посилання на Telegram: посилання на Telegram нечасті, але фішингові сайти використовують їх частіше.
15. Присутність в білому списку: більшість легітимних сайтів зазвичай знаходиться у білому списку.
16. Присутність в чорному списку: частина (зазвичай невелика) фішингових сайтів присутня у чорному списку.
17. Запити на доступ до камери або мікрофона: фішингові сайти частіше запитують доступ до камери або мікрофона.
18. Імітація брендів: фішингові сайти намагаються імітувати бренди, що є важливим маркером для їх ідентифікації.
19. Валідний SSL-сертифікат: легітимні сайти частіше мають валідний SSL-сертифікат.

Як вже було сказано, нейронні мережі – це вельми ефективний механізм виявлення фішингових сайтів, але у такого підході є і переваги, і проблеми.

Переваги нейронних мереж у виявленні фішингових атак:

1. Висока точність і здатність до узагальнення. Нейронні мережі здатні розпізнавати навіть тонкі особливості та відмінності між фішинговими і легітимними сайтами. Вони ефективно працюють з великою кількістю вхідних характеристик.
2. Адаптивність до нових технік фішингу. Завдяки можливості постійного перенавчання, нейронні мережі можуть швидко адаптуватися до змін у техніках фішингу. Для прикладу, мережа може бути оновлена або перенавчена на нових фішингових зразках, що дозволяє системі оперативно реагувати на нові види атак.
3. Масштабованість і автоматизація. Нейронні мережі можуть обробляти велику кількість даних у режимі реального часу, що дозволяє автоматично аналізувати і класифікувати веб-сторінки та електронні листи що значно полегшує роботу для систем безпеки та дозволяє забезпечити постійний моніторинг на великих платформах.
4. Виявлення прихованих патернів. Нейронні мережі здатні виявляти нелінійні зв'язки між різними характеристиками, що іноді неочевидні для людей. Вони можуть знайти комбінації певних слів, розташування символів у URL або структуру HTML-коду, що є ознакою фішингового сайту.

Проблематика нейронних мереж у виявленні фішингових атак:

1. Потреба в великій кількості якісних даних. Для точного навчання нейронних мереж потрібно мати велику кількість зразків як легітимних, так і фішингових сайтів або листів. Недостатня або неповна навчальна вибірка може призвести до низької точності або упередженості результатів.
2. Ризик перенавчання та загальні проблеми з узагальненням. Нейронні мережі можуть перенавчитися на особливостях навчальної вибірки, що призведе до поганої роботи з новими, раніше не баченими зразками. Це є особливою проблемою у випадках, коли фішингові техніки постійно змінюються.
3. Чутливість до змін у техніках атак. Фішингові сайти часто модифікують свої методи, що ускладнює задачу нейронним мережам, навченим на попередніх патернах. Банальна зміна в шаблонах URL-адрес або оновлення стилю листів може знизити ефективність нейромережі, якщо не провести повторне навчання мережі.
4. Високі обчислювальні ресурси та затримки. Для досягнення високої точності нейронним мережам часто потрібні значні обчислювальні потужності, особливо при обробці великих обсягів даних у режимі реального часу і це може бути проблемою для систем, які потребують миттєвої реакції на фішингові атаки.
5. Складність пояснення (аргументації) результатів. Нейронні мережі, а особливо глибокі моделі, є так званими "чорними ящиками", де важко пояснити чому саме система класифікувала той чи інший сайт як фішинговий і це може знижувати довіру до результатів аналізу та ускладнювати прийняття рішення для операторів систем безпеки.

Але незважаючи на вказані проблеми, нейронні мережі, на сьогоднішній день, – це один з найбільш ефективних механізмів виявлення фішингових сайтів, при умові оптимального вибору типу та архітектури мережі, а також параметрів, що аналізуються.

1. СБУ попередила про фішингову розсилку листів від її імені. https://ms.detector.media/kiberbezpeka/post/34011/2024-01-19-sbu-poperedylapro-fishyngovu-rozsylku-lystiv-vid-ii-imeni/.
2. The State of Phishing 2023. https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf.
3. Фішинг як один із основних різновидів інтернет-шахрайства. https://science.donnu.edu.ua/wp-content/uploads/sites/6/2020/06/fishing.pdf.

Ю.М. Здоренко, І.В. Ромашко, С.В. Любарський

АДАПТАЦІЯ ПАРАМЕТРІВ ПРОТОКОЛУ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТУКТУРИ

Постійна доступність сервісів інформаційно-телекомунікаційних мереж критичної інфраструктури є важливим компонентом їх кібернетичної захищеності. Для сучасних умов функціонування таких мереж характерною є постійна зміна їхньої топології, що може призводити до переривання передавання інформації. Так, при змінах топології ІТМ, протокол динамічної маршрутизації здійснює пошук нового оптимального маршруту. Цей процес супроводжується обміном службовими повідомленнями з сусідніми маршрутизаторами, оновленням метрик маршрутів та таблиць маршрутизації. Важливим при цьому є значення часу необхідного для цього. Час збіжності мережі при використанні різних протоколів динамічної маршрутизації може бути різним, але в загальному аналіз їх алгоритмів показав, що вони включають в себе статичні параметри, які використовуються для різних умов функціонування ІТМ. Це може призводити до збільшення часу збіжності мережі та як наслідок збільшення втрат інформаційних пакетів, зростання затримки та зниження якості обслуговування QoS. Такі сценарії для об'єктів критичної інфраструктури є неприйнятними. Тому актуальною є задача адаптації значень параметрів протоколів динамічної маршрутизації, що дозволить мінімізувати час збіжності мережі, зменшити втрати інформаційних пакетів, мінімізувати службовий трафік та забезпечити постійну доступність інформаційних сервісів згідно вимог QoS. Для рішення цієї задачі пропонується розробити метод по адаптації статичних таймерів протоколів динамічної маршрутизації. Аналіз протоколів динамічної маршрутизації показав, що значення таймерів опитування сусідніх маршрутизаторів є постійними. Так, згідно з алгоритмом, який застосовується в динамічному протоколі EIGRP (Cisco), таймер надсилання пакетів повідомлення Hello дорівнює 5 с, а в протоколі RIP величина такого таймеру для відправки Hello-повідомлень складає 30с. Разом з тим в багатьох маршрутизаторах допускається експертне налаштування значень цих таймерів. Однак таке налаштування має ряд недоліків, а саме: є сталим на весь період функціонування; занадто мале значення таймеру може призвести до збільшення службового трафіку, постійності процесу збіжності мережі; занадто велике значення може призвести до втрати актуальної інформації про стан сусідніх маршрутизаторів та як наслідок втрат пакетів через надсилання інформації по вже неіснуючим маршрутам.

Тому для протоколів динамічної маршрутизації при адаптивному налаштуванні таймерів пропонується враховувати такі параметри: поточний стан використання (завантаженості) маршрутів (інтенсивність трафіку) та інтенсивність зміни топології мережі. Так, при збільшенні інтенсивності зміни топології мережі, інтервал надсилання Hello-пакетів необхідно зменшувати. При цьому необхідно враховувати рівень завантаженості альтернативних маршрутів [1]. Так, при значних рівнях завантаженості відповідних маршрутів, значення таймеру опитування пропонується збільшувати. При цьому виникає потреба знаходження збалансованого значення для відповідних таймерів протоколів динамічної маршрутизації. Рішення цієї задачі пропонується здійснювати на основі використання математичного апарату нечіткої логіки [2], [3].

Для ІТМ об'єктів критичної інфраструктури, пропонується реалізувати новий метод оновлення таймерів відправки Hello-повідомлень, який в умовах недостатньої (неточної) інформації ґрунтується, на використанні нечітких систем логічного виведення. Для налаштування та адаптації параметрів таких систем можуть бути використані відомі підходи на основі математичного апарату штучних нейронних мереж. В якості вхідних параметрів таких нейро-нечітких систем для оновлення таймерів відправки Hello-повідомлень пропонується використати значення, що характеризує рівень динамічності (частоту) зміни топології ІТМ за попередній період спостереження, середнє ковзне попереднього параметру та рівень завантаженості мережі (інтенсивність трафіку). Вихідний параметр, оптимальне значення таймеру, визначається в процесі навчання такої fuzzy-системи з використанням алгоритму оберненого поширення помилки. Дані для навчання пропонується зібрати в процесі експериментальних досліджень за показниками якості обслуговування в середовищі моделювання GNS3. Створення fuzzy-системи та її навчання пропонується здійснювати в середовищі Matlab [4]. Передбачається, що використання такого методу адаптації таймерів на основі накопичених даних спостереження показників QoS дозволить забезпечити оптимальні значення таймерів для зменшення часу збіжності мережі та постійну доступність сервісів ІТМ критичної інфраструктури.

1. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість / О. В. Лемешко,–Харків, 2020. – 307 с.
2. Zadeh, L. A. (1997). Toward a theory of fuzzy information granulation and ITM centrality in human reasoning and fuzzy logic, Fuzzy sets and systems, 90(2), 111–127. DOI: https://doi.org/10.1016/S0165-0114(97)00077-8.
3. Takagi, T, Sugeno, M.: Fuzzy identification of systems and its applications to modeling and control. IEEE Transactions on Systems, Man, and Cybernetics 15(1), 116–132 (1985). https://doi.org/10.1109/TSMC.1985.6313399.
4. S. N. Sivanandam, S. Sumathi, S. N. Deepa Introduction to Fuzzy Logic using MATLAB / Topics: Mathematical and Computational Engineering, Artificial Intelligence, Computer Imaging, Vision, Pattern Recognition and Graphics, Edition Number 1, pp.430, (2007). https://doi.org/10.1007/978-3-540-35781-0.

R. Ivanova

INTERNATIONAL ORGANIZATIONS AND LEGAL FRAMEWORKS FOR ENERGY CYBERSECURITY: CHALLENGES FOR UKRAINE IN THE GLOBAL DIGITAL AGE

In today's digitally connected world, the energy sector is considered to be information technology's newest target and possibly the most important and vulnerable sector that suffers cyber attacks. Modern energy systems are complex, interconnected, and greatly rely on information technologies for supervision, control, and communication. Therefore, protecting cyber risks of energy systems infrastructure is now a matter of national security, legal governance, and multi-national collaboration.

Energy grids, nuclear facilities, oil pipelines, and smart grids sustaining cyber attacks can no longer be classified as problematic nor complex. In fact, these forms of attack are increasingly becoming prevalent with dire consequences for public protection, economic growth, and international relations. To tackle these issues, global institutions have assumed advanced responsibility towards defining international legal and strategic boundaries in cyber security.

The UN has addressed issues of cybersecurity in the reports of the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG). These groups created voluntary norms of responsible state behavior in cyberspace that requires the protection of vital constituents such as critical infrastructure. Though these reports do not constitute a legal obligation, they do provide a basis for forming national law and establishing international legal discourse.

The Network and Information Security Directives NIS and NIS2, alongside the Cybersecurity Act, and the Europe Energy Security Strategy are all created by The European Union which places legal obligations on other member states and allied countries to appoint critical operators of services, analyze risks of cyber attacks, report incidents, and enforce security protocols. The Union's core body entrusted with this task is the European Union Agency for Cybersecurity (ENISA) whose responsibilities include providing threat intelligence and sector specific guidance like for the energy sector.

Simultaneously, the IEA (International Energy Agency) has also put forth new recommendations to advance the governance of cybersecurity pertaining to smart grids as well as the digital supply chains and renewables energy systems. These recommendations advocate for the creation of national energy CSIRTs (Computer Security Incident Response Teams), routine resilience evaluation exercises, and enhanced public-private collaboration.

Alongside other UN bodies, the International Telecommunication Union (ITU) actively participates in global coordination and capacity building on cyber security by concentrating on the cross- border legal framework, common standards such as ITU-T X.1205, and institutional frameworks for cyber crisis response including the Cyber emergency response international standard. Under the framework law of its Global Cybersecurity Index which measures country capabilities, Ukraine is also included.

We're modernizing our legislative and institutional frameworks on cybersecurity in the energy sector as a consequence of current wartime realities and European integration objectives. The infrastructural, operational, and technological components defined by "The Law of Ukraine On the Basic Principles of Ensuring Cybersecurity" (2017), the National Cybersecurity Strategy in conjunction with the recently approved National Recovery Plan relating to India's CII (Critical Energy Infrastructure) Cybersecurity Framework focus on protecting energy critical infrastructure but lack full implementation detailing and mechanism integration.

Ukraine's collaboration and participation in international projects like EU4Digital and NATO's Cyber Centre of Excellence (NATO CCDCOE) alongside USAID projects on energy security leverage international frameworks to design sustainable domestic resiliency strategies and showcase the value of cooperating partners.

Another distinct issue is the legal definition of cyber incidents constituting force majeure (acts of God) in contracts and insurance policies in the energy sector. While international legal doctrine does accept this position conditionally, it lacks specific structures to claim these provisions. Certain definitions and processes defining attribution, responsibility, and reparation must be established to eliminate legal ambiguity and distortion in business continuity.Additionally, the matter of investigating cross-border cybercrimes and mutual legal assistance is still unsolved. Organizations like INTERPOL, Council of Europe (through the Budapest Convention), and OECD structure collaboration frameworks. However, Ukraine's participation in these mechanisms needs further enhancement through legal adjustments and institutional advocacy.

Focusing on these, international organizations function not only as state norm creators, but also as active implementing entities within risk evaluation, capacity enhancement, and policy framework design. Their support is unique for states like Ukraine which, at the same time, experiences a digital transformation coupled with legal updates and post-war rebuilding efforts.

The direction of energy cybersecurity development in Ukraine is restrained by a need to equally balance national legal sovereignty and international alignment, with assistance from international institutions and multilateral alliances. Key strategies must include the legal framework capturing cybersecurity responsibilities of energy sector operators, creation of independent regulatory oversight bodies, active participation in regional cybersecurity exercises, and establishment of information exchange platforms.

1. European Union Agency for Cybersecurity (ENISA). (2023). *Cybersecurity for the energy sector* [Electronic resource]. Retrieved from https://www.enisa.europa.eu/topics/csirt-cert-services/energy.

2. European Commission. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*. Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.
3. International Energy Agency. (2023). *Enhancing cybersecurity in the energy sector*. Paris: IEA. https://www.iea.org/reports/cybersecurity.
4. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Requirements*. Geneva: ISO. https://www.iso.org/standard/27001.
5. United Nations. (2021). *Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015–2021)* [Electronic resource]. Retrieved from https://www.un.org/disarmament/group-of-governmental-experts/.

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов, В.П. Яшенков, Т.М. Клименко

ВЕКТОР СОЦІОІНЖЕНЕРНОЇ АТАКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГАЛУЗІ ЕНЕРГЕТИКИ

Використання соціальної інженерії зловмисниками для «несанкціонованого» доступу як до окремих комп'ютерів, так і мереж загалом визначають окремий вектор атаки [1]. Основою направленості його реалізування є експлуатування уразливостей працівників організацій [2]. З-поміж них виокремлюються об'єкти критичної інфраструктури галузі енергетики. Непорушність властивостей інформації у їхніх інформаційних інфраструктурах гарантується упровадженням галузевої системи забезпечування кібербезпеки [3]. Насамперед це дозволяє протидіяти експлуатуванню уразливостей працівників об'єктів критичної інформаційної інфраструктури галузі енергетики. Першочерговість виконання даного завдання обумовлюється поширеністю і, як наслідок, небезпечністю такого різновиду загроз [1–3]. Тому визначання вектору соціоінженерної атаки об'єктів критичної інформаційної інфраструктури галузі енергетики актуальне.

Для узагальненого використання соціальної інженерії, як приклад, можна розглянути фреймворк з шести етапів [4]. Зокрема розвідування, підготовляння і використання інформації, встановлювання початкового контакту, налагоджування взаємодії, експлуатування, використання результатів експлуатування. Загалом ці етапи визначають вектор соціоінженерної атаки. Потенційною жертвою є працівник організації (наприклад, об'єкта критичної інформаційної інфраструктури). За результатами розвідування інформації про нього зловмисником формується історія прикриття використання соціальної інженерії. Нею відображається і психологічний, і поведінковий профілі працівника організації. Це дозволяє зловмиснику обирати моделі, методи, фреймворки та інструментальні засоби використання соціальної інженерії. На основі встановлювання прикриття ним ініціюється контакт з потенційною жертвою. Після цього зловмисник взаємодіє з працівником організації. За результатами такого експлуатування здійснюються спроби виконання дій залежно від кінцевої мети використання соціальної інженерії.

Водночас з огляду на те, що вектор соціоінженерної атаки визначається відповідними моделями, методами та фреймворками. Приклад їх зіставлення відповідно до встановлених критеріїв оприлюднено в [5]. Завдяки цьому розроблено технічну модель використання соціальної інженерії. Характерною її особливістю є зведеність до виконання тільки трьох етапів (збирання інформації, підготовляння і реалізування соціоінженерної атаки) і, як наслідок, подальше автоматизування з інструментальною підтримкою. Основою першого етапу є процес розвідування інформації з відкритих джерел, зокрема, з соціальних мереж. Підготовлянню соціоінженерної атаки передує обирання сценарію її реалізування. З огляду на це використовуються відповідні моделі, методи, фреймворки та інструментальні засоби.

До того ж при визначанні вектору соціоінженерної атаки беруться до уваги психічні процеси працівника організації. Приклад представлення архітектури відповідного фреймворку розглянуто в [6]. У даному випадку вектор соціоінженерної атаки структурується завдяки високорівневому відображенні когнітивних процесів. Цим ураховуються припущення про впливання на процес пізнання людини певних типів явищ, контексту або поведінки. Кожен зі зазначених процесів ініціюється певним стимулом (наприклад, отриманням листа зі зловмисним вкладенням або посиланням на зловмисний вебресурс). Далі він перетворюється на сприйняття (наприклад, усвідомлювання стилю написання електронного листа) і спрямовується через увагу (наприклад, отримання у листі типового завдання). Унаслідок обробляння отриманої зі стимулом інформації формується поведінка людини як результат когнітивного процесу (наприклад, працівник організації відкриває вкладення для виконання типового для нього завдання).

Отже, вектор соціоінженерної атаки об'єктів критичної інформаційної інфраструктури галузі енергетики визначається обраним сценарієм експлуатування уразливостей їх працівників. Як наслідок, може реалізуватися залежно від обраних моделей, методів, фреймворків та інструментальних засобів. Характерною особливістю вектору соціоінженерної атаки є поетапне виконання дій з боку зловмисника. Їх кількість обумовлюється обраним фреймворком і може коливатися у діапазоні, наприклад, від трьох до шести етапів.

1. Attack Vector Definition. URL: https://www.fortinet.com/resources/cyberglossary/attack- vector (accessed on: 07.05.2025).
2. Мохор В. В., Цуркан О. В., Герасимов Р. П., Клименко Т. М., Яшенков В. П. Соціоінженерний аспект використання генеративного штучного інтелекту. *Кібербезпека енергетики* : матеріали (Київ, 29 травня 2024 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2024. С. 114–115.
3. Ракович В. С., Цуркан В. В., Чурсін Г. В., Прокопець О. М. Функція візуалізування інформації про події кібербезпеки об'єктів критичної інформаційної інфраструктури галузі енергетики. *XLIII науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* : збірник матеріалів (Київ, 14 травня 2025 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2025. С. 27–28. DOI: https://doi.org/10.5281/zenodo.15518885.
4. Nowakowski W. Social Engineering Analysis Framework: A Comprehensive Playbook for Human Hacking, *IEEE Access*. 2025. Vol. 13. P. 18827–18849. DOI: https://doi.org/10.1109/ACCESS.2025.3532999.
5. Dana D., Schrittwieser S., Kieseberg P. Automated Social Engineering Tools – Overview and Comparison with Respect to Capabilities and Detectability. Computing in the Global Information Technology (Athens, Greece, 10 – 14 March 2024). P. 1–12. URL: https://personales.upv.es/thinkmind/dl/conferences/iccgi/iccgi_2024/iccgi_2024_1_10_ 10002.pdf (accessed on: 07.05.2025).
6. Burda P., Allodi L., Zannone N. Cognition in Social Engineering Empirical Research: A Systematic Literature Review. *ACM Transactions on Computer-Human Interaction*. 2024. Vol. 31. Iss. 2. P. 1–55. DOI: https://doi.org/10.1145/3635149.

ЗМІСТ

МАТЕРІАЛИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»
28 травня 2025 року

Відповідальні за випуск:

О.В. Цуркан, Т.М. Клименко

Місце проведення: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України; м. Київ, вул. Генерала Наумова, 15.

З питаннями щодо конференції звертатися:

ІПМЕ ім. Г.Є. Пухова НАН України, вул. Генерала Наумова, 15,
кім. 303, Цуркан Оксана володимирівна, тел. 424-91-62,
068-014-57-22, e-mail: otsurkan24@gmail.com

Інститут проблем моделювання в енергетиці
ім. Г. Є. Пухова НАН України,
вул. Генерала Наумова, 15, Київ, 03164, Україна,
тел.: +38 044 424 91 62, факс: +38 044 424 10 63
веб сайт: https://ipme.kiev.ua/