ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Логінова Наталія Іванівна
ПОРІВНЯННЯ БІБЛІОТЕК PYTHONДЛЯ КЕРУВАННЯ БАЗАМИ ДАНИХ 486

Гура Володимир Ігорович
КОМПЛЕКСНИЙ АНАЛІЗ КІБЕРЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГОСИСТЕМАХ 489

Задерейко Олександр Владиславович
АНАЛІЗ ПРОБЛЕМАТИКИ ФОРМУВАННЯ РЕЛЕВАНТНОСТІ ПОШУКУ НАУКОВОЇ ІНФОРМАЦІЇ 493

Куклінова Тетяна Вікторівна, Куклінова Софія Іванівна
ШТУЧНИЙ ІНТЕЛЕКТ І ЗЕЛЕНИЙ ВОДЕНЬ ДЛЯ СТАЛОГО РОЗВИТКУ 497

Лобода Юлія Геннадіївна
ЕФЕКТИВНІ ІНСТРУМЕНТИ ТА ПІДХОДИ ВІЗУАЛІЗАЦІЇ ДАНИХ В АНАЛІТИЧНОМУ ПРОЦЕСІ 501

Манаков Сергій Юрійович
ПАТЕРНИ БЕЗСЕРВЕРНОЇ АРХІТЕКТУРИ 504

Трофименко Олена Григорівна
ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КОНКУРЕНТОСПРОМОЖНІСТЬ В ІТ 506

Чанишев Рашид Ібрагімович
PROTECTEU – НОВА ВНУТРІШНЯ СТРАТЕГІЯ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ 510

Чикунов Павло Олександрович
ПРОЄКТУВАННЯ ВЕБОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ УНІВЕРСАЛЬНОЇ ПЛАТФОРМИ WINDOWS 513

Щербина Юрій Володимирович
АНАЛІЗ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ . . . 517

Дика Анастасія Іванівна
ЗАСТОСУВАННЯ NLP-МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ XSS-АТАК 520

Грезіна Олена Миколаївна
ЗАСТОСУВАННЯ СИСТЕМНОГО АНАЛІЗУ ДЛЯ ІНТЕГРАЦІЇ РІЗНИХ БАЗ ДАНИХ В ВЕБЗАСТОСУНКАХ 523

Соловйов Артем Сергійович
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ КІБЕРБЕЗПЕКИ ОСОБИ В ЦИФРОВУ ЕПОХУ 526

Толокнов Анатолій Арнольдович
ПРОЦЕДУРНА ГЕНЕРАЦІЯ У ВІДЕОІГРАХ:ОГЛЯД МЕТОДІВ, ЗАСТОСУВАНЬ ТА ПЕРСПЕКТИВ 529

Гура Володимир Ігорович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук

КОМПЛЕКСНИЙ АНАЛІЗ КІБЕРЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГОСИСТЕМАХ

Сучасні інтелектуальні енергосистеми являють собою складні кіберфізичні системи, які інтегрують традиційні енергетичні мережі з передовими цифровими технологіями управління, моніторингу та обробки даних. Ця інтеграція забезпечує підвищення ефективності, надійності та адаптивності енергопостачання, але водночас створює нові вразливості, значно розширюючи поверхню атаки для потенційних зловмисників. Зростання складності таких систем супроводжується появою нових векторів атак, які можуть бути спрямовані як на фізичну інфраструктуру, так і на цифрові компоненти. За даними останніх досліджень, енергетичний сектор посідає друге місце за кількістю успішних кібератак після фінансових установ [1]. Наприклад, лише у 2023 році було зафіксовано понад 300 значних інцидентів, пов'язаних із компрометацією енергетичних систем у різних країнах світу [2]. Особливу занепокоєність викликають такі фактори, як стрімке збільшення кількості підключених IoT-пристроїв, які часто мають недостатній рівень захисту, використання застарілих протоколів зв'язку, таких як Modbus або DNP3, низький рівень кіберзахисту промислових систем управління (ICS), а також катастрофічні економічні та соціальні наслідки успішних атак на енергетичну інфраструктуру, що можуть призводити до відключення електроенергії на великих територіях.

Пропонований підхід до аналізу кіберзагроз базується на трирівневій архітектурі, яка дозволяє систематично підходити до виявлення, оцінки та нейтралізації ризиків. Перший рівень відповідає за збір даних і включає інвентаризацію всіх мережевих активів (наприклад, серверів, маршрутизаторів, датчиків), детальний збір інформації про конфігурації обладнання, регулярну актуалізацію бази відомих вразливостей (з використанням стандартів CVE), а також безперервний моніторинг мережевого трафіку для виявлення аномалій. Другий, аналітичний рівень, зосереджений на обробці зібраних даних: тут відбувається побудова моделей загроз, оцінка ймовірності реалізації атак за допомогою статистичних методів, розрахунок показників критичності окремих компонентів системи (наприклад, за методикою CVSS), а також детальний аналіз можливих наслідків, таких як втрата даних чи порушення функціонування мережі. Цей рівень частково спирається на принципи MITRE ATT&CK Framework, адаптовані для енергетичного сектору [3]. Третій рівень забезпечує візуалізацію результатів аналізу через створення інтерактивних звітів, побудову графів атак (з використанням концепцій Diamond Model [4; 5]), а також формування конкретних рекомендацій щодо підвищення безпеки, таких як оновлення програмного забезпечення чи впровадження додаткових засобів аутентифікації.

Для реалізації комплексного аналізу в системі застосовуються передові алгоритмічні методи, які дозволяють ефективно обробляти великі обсяги даних і прогнозувати складні сценарії атак. Основу складають методи теорії графів, які використовуються для моделювання можливих шляхів проникнення зловмисників у систему, враховуючи взаємозв'язки між компонентами [6; 7]. Наприклад, за допомогою графів можна виявити, як компрометація одного IoT-пристрою може призвести до доступу до критичного сервера SCADA. Байєсівські мережі застосовуються для ймовірнісного аналізу загроз, дозволяючи оцінити, наприклад, ймовірність успішного фішингового нападу чи експлуатації конкретної вразливості. Алгоритми багатокритеріальної оптимізації допомагають ранжувати ризики за такими параметрами, як складність атаки, потенційні збитки та доступність засобів захисту [3]. Особливу роль відіграють методи машинного навчання, зокрема кластеризація та класифікація, які підвищують точність виявлення аномалій у мережевому трафіку та ідентифікації нових типів атак, таких як zero-day експлойти [6].

Налаштований фреймворк GridAttackAnalyzer є інноваційним інструментом із широким набором функціональних можливостей. Він забезпечує автоматизовану побудову комплексних моделей загроз, враховуючи як відомі вразливості, так і потенційні нові загрози, проводить всебічну оцінку слабких місць системи, дозволяє моделювати різноманітні сценарії атак (наприклад, DDoS чи ін'єкцію шкідливого коду), а також надає кількісну оцінку ризиків у вигляді числових показників. Завдяки цьому фахівці з безпеки можуть не лише реагувати на поточні загрози, а й прогнозувати еволюцію кібератак, що відповідає принципам Cyber Kill Chain® [1]. Наприклад, система може визначити, на якому етапі ланцюга атаки (розвідка, проникнення чи ексфільтрація даних) перебуває зловмисник, і запропонувати відповідні контрзаходи.

Фреймворк вже продемонстрував свою ефективність під час практичного застосування в реальних енергосистемах. Зокрема, його використовували для аналізу вразливостей у системах SCADA, де було виявлено численні незахищені точки доступу, оцінки ризиків, пов'язаних із масовим розгортанням IoT-пристроїв у розумних мережах, а також для аналізу загроз, спрямованих на хмарні платформи управління енергосистемами, які дедалі частіше стають мішенню атак [6; 7]. У кожному з цих випадків GridAttackAnalyzer показав високу точність аналізу, виявивши навіть складні загрози, такі як скоординовані атаки на кілька компонентів системи одночасно. Наприклад, під час тестування в одній із європейських енергокомпаній система виявила потенційний вектор атаки через незахищений API хмарного сервісу, що могло призвести до повного відключення підстанції.

Для подальшого розвитку системи планується інтеграція найсучасніших технологій, які посилять її аналітичні та захисні можливості. Особливу увагу буде приділено методам глибокого навчання, таким як рекурентні нейронні мережі, для прогнозування складних атак на основі історичних даних. Перспективним

напрямком є впровадження блокчейн-технологій для захисту критично важливих даних, таких як журнали доступу чи конфігурації обладнання, від несанкціонованих змін. Також розглядається використання технології цифрових двійників, яка дозволить створювати віртуальні копії енергосистем для тестування сценаріїв атак і відпрацювання захисних заходів у безпечному середовищі, не впливаючи на реальну інфраструктуру. Наприклад, цифровий двійник може симулювати вплив ransomware на підстанцію без реальних наслідків.

Удосконалення аналітичних можливостей системи відбуватиметься за кількома ключовими напрямками. Важливим аспектом є врахування людського фактору, який часто стає слабкою ланкою через недостатню обізнаність персоналу чи помилки в конфігурації. Планується розробка методів моделювання ланцюжків поставок, щоб виявляти вразливості, пов'язані з постачальниками обладнання чи програмного забезпечення, наприклад, через використання компонентів із вбудованими бекдорами. Особливу увагу буде приділено аналізу стійкості до комбінованих атак, коли зловмисники одночасно експлуатують кілька вразливостей – наприклад, соціальну інженерію разом із технічними експлойтами – для максимізації шкоди. Додатково планується розширення функціоналу для аналізу поведінки інсайдерів, що може стати критичним у контексті зростаючої кількості внутрішніх загроз.

Проведений аналіз кіберзагроз в інтелектуальних енергосистемах підтвердив високу ефективність запропонованого підходу у виявленні, оцінці та прогнозуванні ризиків у складних кіберфізичних системах, що поєднують цифрові технології з традиційною енергетичною інфраструктурою. Зростаюча інтеграція цих компонентів значно розширює поверхню атак, роблячи енергетичний сектор однією з найбільш уразливих сфер. Це зумовлено не лише збільшенням кількості підключених пристроїв і використанням застарілих технологій зв'язку, а й складністю забезпечення захисту в умовах швидкої цифровізації. Запропонована трирівнева архітектура, яка включає етапи збору даних, аналітичного моделювання та візуалізації результатів, забезпечує системний і послідовний підхід до управління безпекою. Застосування сучасних методів, таких як теорія графів для побудови шляхів атак, ймовірнісний аналіз для оцінки ризиків і машинне навчання для класифікації загроз, дозволяє досягати високої точності та адаптивності в умовах мінливого кіберсередовища.

Для подальшого зміцнення системи необхідно приділити увагу кільком ключовим аспектам. Вплив людського фактору, як-от необережність персоналу чи недостатня обізнаність, залишається значним джерелом ризиків, що потребує розробки додаткових заходів, наприклад, навчальних програм чи автоматизованих перевірок. Аналіз вразливостей на етапах постачання обладнання, включаючи можливі слабкі місця в апаратному чи програмному забезпеченні від сторонніх постачальників, є ще одним важливим напрямом. Також слід зосередитися на підвищенні стійкості до комбінованих атак, коли зловмисники одночасно використовують кілька векторів, таких як соціальна інженерія та технічні екс-

плойти, для досягнення максимального ефекту. Усе це разом узяте підкреслює необхідність комплексного підходу до безпеки.

Таким чином, запропонований підхід та фреймворк GridAttackAnalyzer створюють міцну основу для забезпечення кібербезпеки інтелектуальних енергосистем. Вони поєднують теоретичні методи з практичними інструментами, дозволяючи не лише реагувати на поточні загрози, а й готуватися до майбутніх викликів. Удосконалення системи в напрямах інноваційних технологій і всебічного аналізу ризиків сприятиме підвищенню стійкості енергетичної інфраструктури, що є критично важливим у сучасних умовах стрімкої цифровізації та ускладнення кіберзагроз.

Список використаних джерел:

1. European Photovoltaic Industry Association. Market Trends in Solar Energy Deployment. Brussels, 2022. 45 p.
2. Lockheed Mn. Cyber Kill Chain®. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. MITRE ATT&CK Framework Explained. *Kalles Group.* March 2024. URL: https://kallesgroup.com/why-you-should-adapt-the-mitre-attck-framework-for-threat-intelligence/
4. Sánchez del Monte A., Hernández-Álvarez L. Analysis of cyber-intelligence frameworks for AI data processing. *Applied Sciences*. 2023. Vol. 13. № 16. P. 9328. DOI: 10.3390/app13169328
5. Alert Logic report reveals new Killchain efficiencies and cyber-attack automation that give attackers unprecedented advantage. *Alert Logic.* March 2024. URL: https://www.alertlogic.com/press-releases/alert-logic-releases-state-of-threat-detection-2018-report/
6. The Diamond Model: Simple intelligence-driven intrusion analysis. *Kraven Security.* July 2024. URL: https://kravensecurity.com/diamond-model-analysis/
7. Le T. D., Ge M., Anwar A. et al. Grid Attack Analyzer: A cyber attack analysis framework for smart grids. *Sensors.* 2022. Vol. 22. № 13. P. 4795. DOI: 10.3390/s22134795

Ключові слова: аналіз, кіберзагрози, енергосистеми, фреймворк, інформаційні технології, машинне навчання.

Keywords: analysis, cyber threats, energy systems, framework, information technology, machine learning.

Наукове видання

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

16 травня 2025 року

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Матеріали видано в авторській редакції

Підписано до друку 08.06.2025.
Формат 60x84/8. Ум-друк. арк. 41,62.
Зам. № 2506-03.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net

Виготовлювач ТОВ «7БЦ» Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017
03067, м. Київ, вул. Олекси Тихого, 84 e-mail: 7bc@ukr.net тел: (044) 592-00-8