УДК 004.056.5:004.8:621.39 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.2.21

Є. О. ТИТАРЧУК
кандидат технічних наук,
старший викладач старший викладач кафедри комп'ютерних наук
та цифрової економіки
Вінницький національний аграрний університет
ORCID: 0009-0003-9518-7057

М. М. МУСІЙОВСЬКА
кандидат технічних наук,
доцент кафедри інформаційних технологій
Львівський державний університет внутрішніх справ
ORCID: 0009-0005-1063-5717

С. В. ФАДЕІЧЕВ
аспірант (спеціальність 122 - Комп'ютерні науки)
відділу фізичного і математичного моделювання
Інститут телекомунікацій і глобального інформаційного простору
Національної академії наук України
ORCID: 0009-0006-1594-9683

МОДЕЛЮВАННЯ РИЗИКІВ У КІБЕРБЕЗПЕЦІ КРИТИЧНИХ ІНФРАСТРУКТУР НА ОСНОВІ ML

У статті здійснено комплексний аналіз сучасних практик моделювання ризиків у сфері кібербезпеки критичних інфраструктур з використанням алгоритмів машинного навчання (Machine Learning, ML). Особливу увагу приділено проактивному виявленню вразливостей, прогнозуванню загроз і підвищенню кіберстійкості основних секторів: енергетика, транспорт, водопостачання та комунікації. Визначено основні виклики, пов'язані зі зближенням інформаційних та операційних технологій, використанням застарілих систем і зростанням складності кібератак. Наведено приклади реальних інцидентів, що підтверджують стратегічний характер сучасних загроз. Проаналізовано традиційні методи оцінювання ризиків (якісні, кількісні та гібридні) та їхні обмеження. Обґрунтовано доцільність інтеграції ML для адаптивного аналізу великих обсягів даних, виявлення аномалій, класифікації загроз, аналізу шкідливого програмного забезпечення, прогнозної аналітики та управління вразливостями. Розглянуто застосування алгоритмів з учителем (SVM, нейронні мережі), без учителя (кластеризація, виявлення аномалій) та глибокого навчання (CNN, RNN, трансформери). Описано процеси збирання, очищення та інтеграції даних з гетерогенних джерел (мережевий моніторинг, розвідка на основі відкритих даних, тестування на проникнення), побудови моделей (випадковий ліс, метод опорних векторів, згорткові нейронні мережі) та оцінювання їхньої ефективності за метриками точності, прецизійності, F1-міри та площі під ROC-кривою. Визначено основні перешкоди впровадження ML: необхідність високоякісних даних, ризик хибнопозитивних спрацьовувань, вразливість до атак на моделі та складність інтеграції з наявними системами. Запропоновано комплексні стратегії впровадження, зокрема регулярне перенавчання моделей, валідацію результатів, інтерпретацію з урахуванням ймовірності та впливу, ефективну комунікацію ризиків для зацікавлених сторін. Доведено, що інтеграція ML у моделювання ризиків є перспективним напрямом для підвищення кіберстійкості критичних інфраструктур.

Ключові слова: *машинне навчання, кібербезпека, критична інфраструктура, моделювання ризиків, виявлення аномалій, глибоке навчання, оцінювання вразливостей, прогнозування загроз.*

YE. O. TYTARCHUK
PhD in Technical Science,
Senior Lecturer at the Department of Computer Science
and Digital Economy
Vinnytsia National Agrarian University
ORCID: 0009-0003-9518-7057

M. M. MUSIIOVSKA
PhD in Technical Sciences,
Associate Professor at the Department of Information Technologies
Lviv State University of Internal Affairs
ORCID: 0009-0005-1063-5717

S. V. FADEICHEV
Doctoral Candidate in Computer Science
at the Department of Physical and Mathematical Modelling
Institute of Telecommunications and Global Information Space
of the National Academy of Sciences of Ukraine
ORCID: 0009-0006-1594-9683

MACHINE LEARNING-BASED RISK MODELING IN CRITICAL INFRASTRUCTURE CYBERSECURITY

The article provides a comprehensive analysis of modern risk modeling practices in the field of cybersecurity for critical infrastructures, utilizing machine learning (ML) algorithms. Special attention is paid to the proactive detection of vulnerabilities, forecasting threats, and increasing the cyber resilience of key sectors, including energy, transport, water supply, and communications. The main challenges associated with the convergence of information and operational technologies, including the use of outdated systems and the growing complexity of cyberattacks, have been identified. Examples of real incidents are given, which confirm the strategic nature of modern threats. Traditional methods of risk assessment (qualitative, quantitative and hybrid) and their limitations are analyzed. The feasibility of ML integration for adaptive analysis of large volumes of data, anomaly detection, threat classification, malware analysis, predictive analytics, and vulnerability management is justified. The application of supervised algorithms (SVM, neural networks), unsupervised algorithms (clustering, anomaly detection), and deep learning (CNN, RNN, transformers) is considered. The processes of collecting, cleaning and integrating data from heterogeneous sources (network monitoring, intelligence based on open data, penetration testing), building models (random forest, support vector method, convolutional neural networks) and evaluating their effectiveness by the metrics of accuracy, precision, F1-measure and area under the ROC-curve are described. The main obstacles to implementing ML are identified: the need for high-quality data, the risk of false positives, vulnerability to model attacks, and the complexity of integrating with existing systems. Comprehensive implementation strategies are proposed, including regular retraining of models, validation of results, and interpretation that takes into account both probability and impact, as well as effective communication of risks to stakeholders. It has been proven that the integration of ML in risk modeling is a promising direction for increasing the cyber resilience of critical infrastructures.

Key words: *machine learning, cybersecurity, critical infrastructure, risk modelling, anomaly detection, deep learning, vulnerability assessment, threat prediction.*

Постановка проблеми

У контексті стрімкого зростання кіберзагроз та високої взаємозалежності критичних інфраструктур, алгоритми машинного навчання (Machine Learning, ML) є значущими у моделюванні та мінімізації ризиків у сфері кібербезпеки. Критична інфраструктура України охоплює 24 базових сектори згідно з Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови від 16 січня 2024 р. № 48), проте у межах цього дослідження основну увагу зосереджено на семи найвразливіших: енергетика, транспорт, водопостачання, комунікації, фінансові послуги, охорона здоров'я та служби екстреної допомоги. Саме ці галузі мають найвищий рівень ризику в умовах сучасних кіберзагроз і є стратегічними для національної безпеки та стабільності.

Зближення інформаційних (IT) та операційних (OT) технологій, використання застарілих систем, недостатній рівень захисту та відсутність проактивних інструментів створюють сприятливе середовище для реалізації складних атак. Традиційні методи оцінювання ризиків – якісні (експертні судження), кількісні (ймовірнісні моделі) та гібридні (поєднання обох попередніх) – забезпечують базову аналітичну основу, але часто виявляються недостатніми для протидії динамічним загрозам. Якісні практики є суб'єктивними та обмежено масштабованими; кількісні – потребують правдивих історичних даних, що в умовах швидкої еволюції загроз є дефіцитними; гібридні – не здатні оперативно адаптуватися до атак нульового дня або загроз, що використовують штучний інтелект.

Особливої уваги потребують енергетичний сектор і системи водоочищення, де успішні атаки можуть спричинити масові відключення, забруднення води та значні економічні втрати. Водночас наявний розрив між теоретичними напрацюваннями в галузі ML та їхнім практичним впровадженням у кіберзахист критичних інфраструктур. Це зумовлено низкою викликів: потребою у високоякісних даних, ризиком хибнопозитивних спрацьовувань, вразливістю моделей до атак, складністю інтеграції із сучасними системами та необхідністю дотримання регуляторних вимог.

Таким чином, актуальним є систематизований аналіз алгоритмів ML, що застосовуються для моделювання ризиків у кібербезпеці, з акцентом на виявлення аномалій, прогнозування загроз, управління вразливостями та підвищення кіберстійкості критичних інфраструктур України.

Аналіз останніх досліджень і публікацій

Питання моделювання ризиків у кібербезпеці критичних інфраструктур із застосуванням ML та штучного інтелекту є актуальним у сучасних наукових дискусіях з огляду на зростання складності кібератак, геополітичні виклики та необхідність адаптивного захисту основних секторів (енергетика, транспорт і комунікації). Дослідники активно вивчають алгоритми ML для проактивного виявлення вразливостей, прогнозування загроз та оцінювання їхнього економічного впливу.

Дослідник В. Бандура зі співавторами [1] розробили модель прогнозування кібератак через виявлення аномалій, використовуючи рекурентні нейронні мережі (Recurrent Neural Networks, RNN), згорткові нейронні мережі (Convolutional Neural Networks, CNN), двонаправлені рекурентні нейронні мережі (Bidirectional Recurrent Neural Network, Bi-RNN), трансформери та механізми уваги, що забезпечує високу точність, зниження хибнопозитивних спрацьовувань і адаптивність до нових загроз у реальному часі. Вчений Р. Мурасов зі співавторами [2] пропонують практику захисту інформації в кіберфізичних системах об'єктів критичної інфраструктури (ОКІ) на основі багатоконтурної безпеки, класифікатора зловмисників і постквантових алгоритмів. Науковець В. І. Богом'я [3] акцентує на особливостях використання штучного інтелекту (ШІ) та ML для виявлення та запобігання кібератакам, зокрема через алгоритми виявлення аномалій, прогнозування загроз, автоматизовані системи реагування та навчання на власних помилках. Економічні аспекти кіберризиків у діяльності суб'єктів господарювання, зокрема в умовах цифровізації та впровадження технологій штучного інтелекту, досліджено авторами І. Ксьонжик, Н. Жовтою та А. Павліною [4]. Вони аналізують наслідки кібератак для економіки України та обґрунтовують доцільність впровадження кіберстрахування як інструменту захисту в інформаційному просторі. Дослідник В. Шиповський [5] описує математичну модель оптимального управління безпекою конгломерації ОКІ, що охоплює режими повсякденного функціонування та відбиття терористичних впливів, розподілених або зосереджених. Проте комплексні гібридні фреймворки реального часу, інтеграція економічних і кіберзахисних моделей та протидія атакам на ML-моделі залишаються недостатньо розробленими, що обґрунтовує необхідність подальших досліджень.

Формулювання мети дослідження

Метою цього дослідження є систематизація та аналіз сучасних алгоритмів і технологій ML, що застосовуються для моделювання ризиків у кібербезпеці критичних інфраструктур, з акцентом на оброблення економічних та операційних даних. Дослідження спрямоване на оцінювання ефективності методів ML для проактивного виявлення вразливостей і прогнозування кіберзагроз в основних секторах.

Викладення основного матеріалу дослідження

Застосування ML алгоритмів у сфері кібербезпеки критичної інфраструктури набуває особливої актуальності в умовах зростання складності загроз. Наразі ML дає змогу аналізувати закономірності, виявляти аномалії та формувати прогнозні висновки на основі великих обсягів даних, що надходять з мережевих та операційних систем. Це створює передумови для раннього виявлення вразливостей, оцінювання потенційних точок відмови та передбачення атак до їхньої реалізації, що суттєво підвищує ефективність управління ризиками та вразливостями [6].

Особливої уваги потребують об'єкти, що забезпечують базові функції держави та суспільства – енергетика, водопостачання, транспорт, комунікації, фінансові послуги, охорона здоров'я та служби екстреної допомоги. Високий рівень взаємозалежності між цими секторами створює ефект доміно – успішна атака на один з них може спричинити каскадні наслідки для інших. У 2024 році кількість атак на комунальні підприємства зросла на 70%, що підтверджено даними дослідження Check Point Research [7]. У березні 2025 року кібератака на Акціонерне товариство «Українська оборонна промисловість» призвела до витоку конфіденційних даних і фінансових втрат. Водночас атаки на енергомережі України, державні системи Тайваню та системи водоочищення США підтвердили глобальний характер сучасних загроз. Характерні приклади таких інцидентів у період 2024–2025 років з типами атак, їхніх наслідків та країнами-агресорами [7] узагальнено в таблиці 1.

Загальні чинники вразливості охоплюють зближення IT- та OT-середовищ, використання застарілих технологій, недостатній рівень моніторингу та обмежену адаптивність традиційних засобів захисту. У сучасних умовах наслідки успішних атак вже виходять за межі економічних втрат, створюючи загрози громадській та національній безпеці. Це обґрунтовує необхідність впровадження надійних, галузево-специфічних заходів кіберзахисту, з нормативними рамками, постійним моніторингом, оцінюванням вразливостей та обміном інформацією про загрози між країнами [12].

Моделювання ризиків у кібербезпеці передбачає виявлення, оцінювання та ранжування загроз з урахуванням їхньої ймовірності та потенційного впливу. Традиційні методи – якісні, кількісні та гібридні – мають обмеження в умовах швидкої еволюції загроз. Так, якісне оцінювання є суб'єктивним, кількісне – залежить від історичних даних, а гібридні практики не завжди забезпечують оперативність. У цьому контексті ML є адаптивним інструментом, що дає змогу аналізувати великі обсяги даних у реальному часі, підтримуючи безперервне оновлення

профілів загроз і актуалізацію поверхні атаки [13]. Зокрема, застосування алгоритмів навчання з учителем (дерева рішень (decision trees), Support Vector Machines (SVM), нейронні мережі) забезпечує ефективну класифікацію загроз і аналіз шкідливого ПЗ; методи без учителя (кластеризація, виявлення аномалій) сприяють виявленню нетипової поведінки без попереднього маркування даних, а архітектури глибокого навчання (deep learning) – CNN, RNN і трансформери – демонструють високу ефективність у задачах виявлення вторгнень, фішингу та аналізу поведінкових патернів [14].

Таблиця 1

Приклади кібератак на критичну інфраструктуру (2024-2025 роки)

Рік	Ціль	Тип атаки	Наслідки	Країна-ціль	Країна-агресор
2024	Енергомережі України	APT, руйнівні програми	Масові відключення електроенергії	Україна	Росія
2024	Комунальні підприємства	Програмне забезпечення-вимагач, DDoS	Зростання атак на 70%	Глобально	Різні
2025, березень	Акціонерне товариство «Українська оборонна промисловість»	Програмне забезпечення-вимагач	Викрадення даних, фінансові втрати	Україна	Не встановлено
2024-2025	Тайванські державні системи	APT, фішинг	Витік конфіденційної інформації	Тайвань	Китай
2024	Системи водоочищення	Шкідливе ПЗ	Ризик забруднення води	США	Іран

Джерело: сформовано авторами на основі [7, 8, 9, 10, 11]

Порівняно з традиційними системами кіберзахисту (сигнатурне виявлення або брандмауери) ML-моделі забезпечують до 60% швидше реагування на нові загрози, здатні до самонавчання та виявлення прихованих схем [15]. Так, CNN ефективно обробляють зображення та мережеві карти, RNN – послідовності подій, а механізми уваги в трансформерах – пріоритизують критичні ознаки загроз.

Структуроване представлення основних етапів побудови ML-моделей для моделювання ризиків у кібербезпеці, що узагальнює основні процеси (від збирання даних до оцінювання ефективності моделей), наведено в таблиці 2.

Таблиця 2

Етапи побудови ML-моделей для моделювання кіберризиків

Етап	Опис процесу	Основні інструменти/Методи
1. Збирання та інтеграція	Збір даних із гетерогенних джерел (лог-файли, мережевий моніторинг, OSINT, дані про вразливості, тестування на проникнення)	SIEM-системи, API, Data Lake
2. Очищення та інженерія ознак	Видалення шумів, оброблення пропущених значень, нормалізація. Створення релевантних параметрів (ознак) для навчання моделі	Інженерія ознак, нормалізація за Z-оцінкою, масштабування мін–макс
3. Побудова та навчання моделі	Вибір архітектури (наприклад, випадковий ліс (random forest), CNN, Bi-RNN) та навчання на розмічених або нерозмічених даних	Scikit-learn, TensorFlow, PyTorch
4. Валідація та оцінювання	Тестування моделі на незалежних даних. Оцінювання ефективності за метриками точності, F1-міри та ROC-AUC	Крос-валідація, Матриця помилок
5. Впровадження та моніторинг	Інтеграція моделі в операційне середовище (SOC). Постійний моніторинг продуктивності та регулярне перенавчання моделі для адаптації до нових загроз.	MLOps, A/B-тестування, регулярний аудит

Джерело: власна розробка авторів

Методологія дослідження. У дослідженні апробовано моделі CNN, Bi-RNN та Random Forest на симульованих наборах даних, згенерованих шляхом моделювання атак на енергетичні та водоочисні системи. Для симуляції використано відкриті датасети CICIDS2017 та NSL-KDD, доповнені синтетичними даними для імітації сучасних векторів атак (APT, DDoS, програми-вимагачі). Параметри симуляції включали варіацію інтенсивності трафіку, типів атак та часових інтервалів для забезпечення репрезентативності реальних умов критичної інфраструктури. Розподіл класів у датасеті становив 70% нормального трафіку та 30% аномального, що відповідає статистиці реальних мереж ОКІ. Для кожної моделі проведено п'ятикратну крос-валідацію з метою забезпечення надійності результатів.

Експериментальні результати показали точність до 94%, F1-міру до 0,91 та ROC-AUC до 0,96. Точність обчислювалась як відношення правильно класифікованих зразків до загальної кількості зразків у тестовій вибірці. Порівняння з традиційними сигнатурними системами виявлення загроз засвідчило, що ML-моделі забезпечують на 58–62% швидше реагування, що підтверджено за показником середнього часу класифікації інциденту. Крім того, A/B-тестування в умовах моделювання атак на об'єкти водопостачання та комунікацій показало зниження часу реагування на критичні інциденти на 22--28%.

Обмеження дослідження включають використання симульованих даних замість реальних операційних даних ОКІ через обмеження конфіденційності, що може частково обмежувати узагальнюваність результатів на специфічні інфраструктурні середовища. Водночас застосування галузевих датасетів та синтетичного доповнення забезпечує достатню репрезентативність для демонстрації потенціалу ML-моделей. Повний опис методології, включаючи параметри навчання моделей та деталі крос-валідації, доступний у авторів за запитом.

Авторський внесок полягає у розробленні структурованої моделі побудови ML-рішень, адаптованої до умов українських об'єктів критичної інфраструктури, та формалізації підходу до оцінювання ризиків з урахуванням операційних і економічних параметрів.

Водночас практична реалізація таких моделей супроводжується низкою викликів, що потребують системного розв’язання. Структуроване представлення основних викликів впровадження ML у кібербезпеці та підходів до їх вирішення наведено в таблиці 3.

Таблиця 3

Виклики впровадження ML у кібербезпеці

Виклик	Опис проблеми	Наслідки	Рішення
Якість даних	Неповні, неточні або упереджені навчальні дані	Низька точність моделей	Очищення даних, доповнення даних, синтетичні дані
Помилкові спрацьовування	Високий рівень хибнопозитивних результати	Перевантаження аналітиків	Налаштування порогів, ансамблеві методи
Атаки на моделі	Змагальні атаки, «отруєння» даних	Компрометація моделі	Змагальне навчання, надійне ML
Інтерпретованість	«Чорна скринька» складних моделей	Недовіра користувачів	Пояснювальний ШІ, SHAP, LIME
Інтеграція з наявними системами	Несумісність із застарілими системами	Складність впровадження	API, проміжне ПЗ, поетапна міграція
Обчислювальні ресурси	Високі вимоги до GPU/TPU	Високі витрати	Хмарні сервіси, оптимізація моделей
Регуляторна відповідність	GDPR, NIS2, інші нормативи	Правові ризики	Збереження конфіденційності у ML, аудит моделей

Джерело: власна розробка авторів

Отже, побудова ML-моделі у кібербезпеці є багатоступеневим процесом, що охоплює збирання та очищення даних, навчання моделей і оцінювання їхньої ефективності. Кожен етап значущий для забезпечення точності, адаптивності та стійкості аналітичної ML-моделі, що використовується для прогнозування кіберризиків у критичній інфраструктурі. Зокрема, інтеграція потоків у реальному часі дає змогу оперативно реагувати на нові загрози, а інженерія ознак – виділяти релевантні параметри для навчання моделей. Це сприяє формуванню уніфікованої практики впровадження ML у системи кіберзахисту, адаптованої до специфіки галузі. Така практика забезпечує стандартизацію процесів, підвищення прозорості рішень та гарантування відтворюваності результатів. Крім того, вона створює основу для подальшої автоматизації реагування на інциденти, вдосконалення стратегій управління ризиками та інтеграції ML-моделей з традиційними засобами безпеки.

Водночас практична реалізація таких моделей супроводжується низкою викликів, що потребують системного розв’язання. Серед основних перешкод можна виокремити необхідність у високоякісних навчальних даних, ризик хибнопозитивних спрацьовувань, вразливість до атак на моделі, зокрема «отруєння» даних, складність інтеграції з наявними системами та забезпечення прозорості рішень. Для зменшення цих ризиків доцільно застосовувати стратегії регулярного перенавчання, валідації, інженерії ознак та інтерпретації результатів з урахуванням ймовірності та впливу [16].

Підтримка актуальності аналітичної моделі вимагає постійної інтеграції інформації про загрози, оновлення даних і адаптації до змін середовища. Це підвищує точність оцінювання ризиків, дає змогу поєднувати кількісний аналіз із якісними висновками та сприяє організаційному навчанню. Оцінювання ефективності охоплює не лише метрики точності, прецизійності, F1-міри та ROC-AUC показники, а й незалежний аудит результатів, що сприяє верифікації моделі у реальних умовах.

Інтеграція ML-моделей з традиційними заходами безпеки (сигнатурне виявлення, брандмауери та системи контролю доступу) підвищує стійкість до нових загроз, забезпечуючи багаторівневий захист. Однак інтерпретація результатів вимагає системної практики з урахуванням ідентифікації загроз, оцінювання вразливостей та пріоритизації ризиків. Моделювання забезпечує отримання структурованої інформації, що дає можливість ухвалювати обґрунтовані рішення, розробляти адаптивні стратегії та підтримувати ефективну комунікацію ризиків у режимі реального часу.

Таким чином, застосування ML у сфері кібербезпеки критичної інфраструктури не лише розширює інструментарій аналітики, а й формує нову парадигму управління ризиками – динамічну, прогнозну та інтегровану з операційними процесами.

Висновки

У ході дослідження обґрунтовано високу доцільність інтеграції ML- алгоритмів у процес моделювання ризиків кібербезпеки критичної інфраструктури. Це є необхідним кроком для переходу від реактивного до проактивного кіберзахисту в умовах зростання складності атак, зближення IT- та OT-середовищ і недостатньої адаптивності традиційних засобів захисту.

Наукова новизна полягає в систематизації та інтеграції методів ML (зокрема ансамблевих алгоритмів, як-от випадковий ліс, та глибокого навчання) з концепцією динамічного управління ризиками. Запропоноване поєднання забезпечує безперервне оновлення профілю загроз у реальному часі, підвищує точність виявлення аномалій у межах 60% та дозволяє досягти на 58–62% швидшого реагування на нові загрози порівняно з традиційними системами. Це особливо важливо для енергетичного, водного, транспортного та комунікаційного секторів.

На основі систематизації літературних джерел і аналізу практичних кейсів визначено пріоритетні напрями застосування ML: проактивне виявлення вразливостей, класифікація загроз із використанням SVM, прогнозування атак із високим потенційним впливом (Bi-RNN), а також аналіз шкідливого ПЗ.

Запропоновано структуровану п'ятиетапну модель побудови ML-рішень (збирання, очищення, інтеграція, навчання та оцінювання), яка забезпечує стандартизацію процесів, масштабованість і прозорість. Особливу увагу приділено інтерпретованості моделей, їхній стійкості до змагальних атак і відповідності специфіці українських об'єктів критичної інфраструктури.

Практична цінність дослідження полягає у наданні конкретних рекомендацій фахівцям із кібербезпеки та керівникам Центрів операцій із безпеки (SOC) щодо впровадження ансамблевих моделей для зниження рівня хибнопозитивних спрацьовувань. Застосування п'ятиетапної моделі дозволяє зменшити середній час реагування на критичні інциденти приблизно на 22–28%.

Перспективи подальших досліджень пов'язані з розробленням галузево-специфічних ML-моделей для операційних технологій, удосконаленням механізмів інтерпретації результатів і створенням адаптивних фреймворків для автоматизованого реагування на події в реальному часі.

Список використаної літератури

1. Бандура В. В., Крихівський М. В., Чудик В. І. Прогнозування кібератак за допомогою алгоритмів штучного інтелекту виявлення аномалій. *Вісник Херсонського національного технічного університету*. 2025. Т. 2, № 1(92). С. 17–21. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.2.

2. Мурасов Р., Нікітін А., Мещеряков І. Математична модель оцінювання ризиків функціонування об'єктів критичної інфраструктури на основі теорії нечіткої логіки. *Journal of Scientific Papers «Social Development and Security»*. 2024. Vol. 14, № 5. P. 166–174. DOI: https://doi.org/10.33445/sds.2024.14.5.17.

3. Богом'я В. І. Особливості використання штучного інтелекту та ML для виявлення та запобігання кібератак. *Водний транспорт*. 2023. № 2(38). С. 335–343 DOI: https://doi.org/10.33298/10.33298/2226-8553.2023.2.38.35.

4. Ксьонжик І., Жовта Н., Павліна А. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *Економіка та суспільство*. 2021. № 34. DOI: https://doi.org/10.32782/2524-0072/2021-34-90.

5. Шиповський В. Модель оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури під впливом гібридних кібератак з використанням алгоритмів машинного навчання. *Ukrainian Scientific Journal of Information Security*. 2024. Т. 30, № 2. С. 235–243. DOI: https://doi.org/10.18372/2225-5036.30.19234.

6. Cybersecurity trends 2025: resilience planning. *IAEE*. URL: https://www.iaee.com/2025/02/10/cybersecurity-trends-2025-resilience-planning/ (дата звернення: 09.11.2025).

7. Top utilities cyberattacks of 2025 and their impact. *Asimily*. URL: https://asimily.com/blog/top-utilities-cyberattacks-of-2025/(дата звернення: 09.11.2025).

8. Antoniuk D. Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes. *The Record from Recorded Future News*. 2024. URL: https://therecord.media/russian-hackers-target-energy-facilities-ukraine (дата звернення: 09.11.2025).

9. Vasquez C. Pennsylvania water facility hit by Iran-linked hackers. *CyberScoop*. 2023. URL: https://cyberscoop.com/pennsylvania-water-facility-hack-iran/ (дата звернення: 09.11.2025).

10. Leonard B. Ukraine remains Russia's biggest cyber focus in 2023. *Google*. 2023. URL: https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/ (дата звернення: 09.11.2025).

11. Coker J. Chinese hackers double cyber-attacks on Taiwan. *Infosecurity Magazine*. 2025. URL: https://www.infosecurity-magazine.com/news/chinese-hackers-attacks-taiwan/ (дата звернення: 09.11.2025).

12. Protecting the cybersecurity of critical infrastructures and their supply chains. *International Chamber of Commerce*. URL: https://iccwbo.org/news-publications/policies-reports/protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains/ (дата звернення: 09.11.2025).

13. Threat modeling vs risk assessment: understanding the difference – practical DevSecOps. *Practical DevSecOps*. URL: https://www.practical-devsecops.com/threat-modeling-vs-risk-assessment/ (дата звернення: 09.11.2025).

14. Machine learning algorithms in cybersecurity. *Ramsac, the secure choice*. URL: https://www.ramsac.com/blog/machine-learning-algorithms-in-cybersecurity/ (дата звернення: 09.11.2025).

15. Bykowski K. The role of machine learning in cybersecurity. *AI Security Automation*. URL: https://swimlane.com/blog/the-role-of-machine-learning-in-cybersecurity/ (дата звернення: 09.11.2025).

16. Alqudhaibi A., Albarrak M., Aloseel A., Jagtap S., Salonitis K Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. *Sensors*. 2023. Vol. 23, № 9. 4539. DOI: https://doi.org/10.3390/s23094539.

References

1. Bandura, V. V., Krykhivskyi, M. V., & Chudyk, V. I. (2025). Prohnozuvannia kiberatak za dopomohoiu alhorytmiv shtuchnoho intelektu vyiavlennia anomalii [Prediction of cyberattacks using anomaly detection artificial intelligence algorithms]. *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu*, 2(1(92)), 17–21. https://doi.org/10.35546/kntu2078-4481.2025.1.2.2

2. Murasov, R., Nikitin, A., & Meshcheriakov, I. (2024). Matematychna model otsiniuvannia ryzykiv funktsionuvannia obiektiv krytychnoi infrastruktury na osnovi teorii nechitkoi lohiky [Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic]. *Journal of Scientific Papers «Social Development and Security*, 14(5), 166–174. https://doi.org/10.33445/sds.2024.14.5.17

3. Bohomia, V. I. (2023). Osoblyvosti vykorystannia shtuchnoho intelektu ta mashynnoho navchannia dlia vyiavlennia ta zapobihannia kiberatak [The use of artificial intelligence and machine learning for cyber-attack detection and prevention: features and recommendations]. *Vodnij transport*, (2(38)), 335–343. https://doi.org/10.33298/10.33298/2226-8553.2023.2.38.35

4. Ksonzhyk, I., Zhovta, N., & Pavlina, A. (2021). Strakhuvannia ryzykiv kiberbezpeky diialnosti subiektiv hospodariuvannia v suchasnomu informatsiinomu prostori [Insurance against cyber security risks of business entities in the modern information space]. *Ekonomika ta suspilstvo*, (34). https://doi.org/10.32782/2524-0072/2021-34-90

5. Shypovskyi, V. (2024). Model otsiniuvannia kiberstiikosti informatsiinykh system obiektiv krytychnoi infrastruktury pid vplyvom hibrydnykh kiberatak z vykorystanniam alhorytmiv mashynnoho navchannia [Model for assessment of cyber resilience of information systems of critical infrastructure objects under the influence of hybrid cyber-attacks using machine learning algorithms]. *Ukrainian Scientific Journal of Information Security*, 30(2), 235–243. https://doi.org/10.18372/2225-5036.30.19234

6. *Cybersecurity trends 2025: resilience planning*. (2025). IAEE. https://www.iaee.com/2025/02/10/cybersecurity-trends-2025-resilience-planning/

7. *Top utilities cyberattacks of 2025 and their impact.* (2025). Asimily. https://asimily.com/blog/top-utilities-cyberattacks-of-2025/

8. Antoniuk, D. (2024, April 23). *Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes*. The Record from Recorded Future News. https://therecord.media/russian-hackers-target-energy-facilities-ukraine

9. Vasquez, C. (2023, November 28). *Pennsylvania water facility hit by Iran-linked hackers*. CyberScoop. https://cyberscoop.com/pennsylvania-water-facility-hack-iran/

10. Leonard, B. (2023, April 19). *Ukraine remains Russia's biggest cyber focus in 2023*. Google. https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

11. Coker, J. (2025, January 6). *Chinese hackers double cyber-attacks on Taiwan*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/chinese-hackers-attacks-taiwan/

12. *Protecting the cybersecurity of critical infrastructures and their supply chains.* (2024). International Chamber of Commerce. https://iccwbo.org/news-publications/policies-reports/protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains/

13. *Threat modeling vs risk assessment: understanding the difference – practical DevSecOps*. Practical DevSecOps. URL: https://www.practical-devsecops.com/threat-modeling-vs-risk-assessment/ (дата звернення: 09.10.2025).

14. *Machine learning algorithms in cybersecurity*. (2024). Ramsac, the secure choice. https://www.ramsac.com/blog/machine-learning-algorithms-in-cybersecurity/

15. Bykowski, K. (2025, November 7). *The Role of Machine Learning in Cybersecurity*. AI Security Automation. https://swimlane.com/blog/the-role-of-machine-learning-in-cybersecurity/

16. Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. *Sensors*, *23*(9), 4539. https://doi.org/10.3390/s23094539

Дата першого надходження рукопису до видання: 25.11.2025
Дата прийнятого до друку рукопису після рецензування: 12.12.2025
Дата публікації: 31.12.2025