АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 004.056:004.8:005.8

DOI https://doi.org/10.5281/zenodo.15717543

Інтелектуалізація кіберзахисту: роль штучного інтелекту у своєчасному виявленні аномалій в умовах еволюції гібридних загроз

Сердюков Костянтин Сергійович

аспірант кафедри публічного управління, менеджменту та маркетингу,

Східноукраїнський національний університет ім. В. Даля,

вул. Іоанна Павла II, 17, м. Київ, 01042, Україна,

serdiukovk@gmail.com,

https://orcid.org/0009-0009-7098-3907

Прийнято: 11.06.2025| Опубліковано: 21.06.2025

Анотація. *У сучасних умовах цифрової трансформації діяльність організацій нерозривно пов'язана із впровадженням інформаційно-комунікаційних технологій. Така взаємодія зумовлює зростання залежності підприємств, державних установ і критичної інфраструктури від кіберпростору, що, у свою чергу, підвищує їхню вразливість до різноманітних загроз, зокрема гібридного характеру. У відповідь на ці виклики штучний інтелект (ШІ) набуває все ширшого застосування у сфері кібербезпеки завдяки своїм можливостям щодо автоматизації обробки великих обсягів даних, оперативного виявлення аномалій та прогнозування потенційних загроз.* ***Мета.*** *Обґрунтувати та вивчити перспективи інтеграції технологій штучного інтелекту в систему кібербезпеки організації з метою збільшення ефективності виявлення аномалій та протидії гібридним загрозам як складової інформаційно-організаційного забезпечення управлінської*

діяльності в умовах цифровізації. ***Методи.*** *Методами дослідження є системний підхід, порівняльний аналіз, моделювання та формалізація.* ***Результати.*** *В цьому дослідженні проведено всебічний теоретичний аналіз основ кібербезпеки в умовах гібридних загроз. Зокрема, були визначені основні фактори, що впливають на інформаційну стійкість організацій. Огляд сучасних підходів до класифікації та моделювання гібридних небезпек зосереджений на ролі кіберпростору та його впливі на функціонування організаційних структур. Особлива увага приділена вивченню потенціалу штучного інтелекту в забезпеченні мережевої безпеки. Також досліджено актуальні методи для виявлення аномалій і загроз за допомогою технологій штучного інтелекту, включно з машинним навчанням, глибинним навчанням і нейронними мережами. На основі отриманих результатів запропоновано концепцію інтеграції інструментів штучного інтелекту в систему управління мережевою безпекою організації, що забезпечує підвищення її адаптивності та стійкості до кіберзагроз. Запропоновано напрямки оптимізації процесів виявлення аномалій та реагування на кіберінциденти з використанням інструментів ШІ.* ***Висновки.*** *Висновок показує, що інтегрування штучного інтелекту в систему мережевої безпеки дає організаціям можливість досягти вищого рівня захисту, реагувати швидше на загрози, гарантувати безперервність діяльності та підтримувати довіру клієнтів та партнерів в умовах безперервних кіберзагроз.*

Ключові слова: *інформаційні технології, автоматизація, кіберзахист, кібератака, цифрова трансформація, аналітика ризиків, управління організацією.*

 ISSN 3041-2129

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Intellectualization of cyber defense: the role of artificial intelligence in timely detection of anomalies in the context of evolution of hybrid threats

Serdiukov Kostiantyn
graduate student of the Department of Public Administration, Management and Marketing,
Volodymyr Dahl East Ukrainian National University,
Ioanna Pavla II St, 17, Kyiv, 01042, Ukraine,
serdiukovk@gmail.com,
https://orcid.org/0009-0009-7098-3907

Abstract. *Currently, the digitalization of organizations is closely linked to the implementation of information and communication technologies. This renders businesses, government entities, and essential infrastructure dependent on cyberspace, subjecting them to risks, including hybrid threats. Artificial intelligence (AI) is increasingly utilized in cybersecurity because of its capacity to automate extensive data analysis, identify breaches swiftly, and foresee potential threats.* ***Purpose.*** *To validate and examine the possibilities for incorporating artificial intelligence technologies into the organization's cybersecurity system to enhance the effectiveness of anomaly detection and counter hybrid threats as a piece of information and organizational support for management actions in the setting of digitalization.* ***Methods.*** *The research methods are a systematic approach, comparative analysis, modeling, and formalization.* ***Results.*** *In this study, a comprehensive theoretical analysis of the basics of cybersecurity in the context of hybrid threats was conducted. In particular, the main factors affecting the information resilience of organizations were identified. The assessment of contemporary approaches to the categorization and modeling of hybrid threats centers on the part of cyberspace and its effect on the operation of organizational frameworks. Specific consideration is given to examining the potential of artificial*

intelligence in assuring network security. It further investigates current methods for spotting anomalies and dangers utilizing artificial intelligence technologies, including machine learning, deep learning, and neural networks. Based on the results achieved, the concept of incorporating artificial intelligence tools into the organization's network security administration system is suggested, guaranteeing a boost in its adaptability and resilience versus cyber threats. Directions for streamlining the processes of detecting anomalies and responding to cyber incidents using AI tools are presented. ***Conclusions.*** *The results indicate that integrating artificial intelligence into network security permits organizations to attain a superior level of defense, react quicker to threats, guarantee business continuity, and preserve customer and partner trust amidst persistent cyber threats.*

Keywords: *information technology, automation, cybersecurity, cyberattack, digital transformation, risk analytics, organization management.*

Постановка проблеми. У сучасних умовах стрімкої діджиталізації роль інформаційних технологій в діяльності організацій набуває вирішального значення. Водночас така залежність спричиняє зростання ризиків у сфері кібербезпеки. Все більш актуальною стає проблема захисту інформаційних систем від гібридних загроз. Ці загрози поєднують різні форми впливу - від кібератак до інформаційно-психологічного тиску, включаючи маніпулятивні стратегії та деструктивні інформаційні кампанії. Стандартні методи виявлення та нейтралізації таких загроз часто виявляються малоефективними через їхню високу динамічність, складний характер і постійне еволюціонування.

Технології штучного інтелекту дедалі активніше проникають у світ сучасних систем кібербезпеки, відкриваючи нові можливості для автоматизованого виявлення порушень і прогнозування потенційних загроз. Проте, незважаючи на швидкий прогрес у цій галузі, питання ефективного впровадження інструментів штучного інтелекту в інфраструктуру кібербезпеки, з урахуванням нюансів управління та контексту оброблюваної

інформації, залишається недостатньо дослідженим. Це підкреслює необхідність розробки нових підходів, які зможуть вдосконалити використання штучного інтелекту для підвищення ефективності моніторингу аномальної активності та забезпечення проактивної реакції на гібридні загрози в управлінських процесах.

Зі зростанням загрози кібератак, важливо впроваджувати нові підходи, особливо використовуючи технології штучного інтелекту. Їхня мета полягає в підвищенні ефективності систем виявлення аномалій та створенні превентивних механізмів для запобігання загрозам в інформаційному середовищі організації.

Аналіз останніх досліджень і публікацій. Вивчення проблематика інтеграції штучного інтелекту у кібербезпековій системі організації досліджувалася багатьма науковцями. Зокрема, О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк, М. Ворохоб [1,с. 6] розглядали метод оцінювання ризиків від застосування ШІ в різних сферах та засоби їх опрацювання. Запропоновані способи використання системи штучного інтелекту для виявлення та оцінювання ризиків, що виникають внаслідок застосування систем штучного інтелекту. Л.В. Шостак, А.А. Федонюк, О.О. Помазун [2, с. 121], О. Кузьменко, О. Маклюк, О. Чернишова [3] досліджували властивості забезпечення кібербезпеки вітчизняного бізнесу шляхом узагальнення основних видів кіберзагроз з можливими їх наслідками для вітчизняного бізнесу та визначення стратегій вирішення зазначених проблем.

К. Ю. Завражний та А. К. Кулик [4, с. 81] акцентують увагу на нагальній необхідності впровадження ефективних систем кіберзахисту, які здатні істотно зменшити ризики, пов’язані з кібератаками, несанкціонованим доступом до персональних даних, а також іншими формами онлайн-шахрайства. У свою чергу, А. П. Хряпинський [5, с. 641] підкреслює, що одним із визначальних аспектів сучасних якісно-інноваційних підходів до ідентифікації та протидії гібридним загрозам є їхня практична орієнтація до

міжнародного контексту.

М. Климаш, Н. Бальковський та О. Шпур [6, с. 1] здійснили порівняльний аналіз ефективності трьох поширених алгоритмів машинного навчання, що використовуються для виявлення аномалій у цифровому середовищі. Отримані результати мають прикладне значення для вдосконалення існуючих методів кіберзахисту, зокрема у сфері захисту критичної інфраструктури, де своєчасне виявлення загроз є вирішальним фактором забезпечення безпеки.

Г. М. Лявинець, Й. Й. Роглєв, О. В. Бортнічук [7] зауважили, що в умовах сучасного конкурентного ринку та світових криз виявлення аномалій стає потребою для успішного розвитку та стійкості підприємств в теперішніх кризових умовах, що не тільки мінімізує фінансові та репутаційні ризики, а й сприяє підвищенню прозорості, операційної ефективності.

M. Schmitt [8] головну увагу зосереджував на оцінці класифікаторів та ансамблів на основі ШІ для виявлення шкідливого ПЗ на базі аномалій та виявлення вторгнень у мережу, а також способам інтеграції цих моделей в контексті мережевої безпеки, мобільної безпеки та безпеки Інтернету речей. В обговоренні підкреслюються проблеми, пов'язані з розгортанням та інтеграцією рішень кібербезпеки на базі ШІ, в наявні корпоративні системи та IT-інфраструктури, включно з варіантами вирішення цих проблем.

O. Marwan [9] провів детальний огляд інтегрованих підходів до використання технологій штучного інтелекту, щоб підвищити рівень мережевої безпеки та оптимізувати управління в організаціях. У дослідженні J. Hudson [10] підкреслюється важливість сучасних методів захисту баз даних - таких як управління доступом, виявлення аномалій і захист за допомогою паролів - для протидії загрозам, які виникають перед моделями штучного інтелекту. D. G. Marron, S. I.- L. Martinez, L. A.-S. Valadez, A. G. Ceron [11] відзначили, що інформаційні технології на основі штучного інтелекту можуть помітно поліпшити виявлення мережевих аномалій, тим самим збільшуючи

загальну безпеку мережі.

Попри помітні наукові здобутки в цій царині, деякі аспекти все ще потребують більш ґрунтовного вивчення. Майбутні дослідження повинні зосередитися на впровадженні новітніх методів для виявлення відхилень у контексті гібридних небезпек. Це допоможе створити ефективні стратегії захисту та гарантувати безперервність бізнес-процесів в управлінні організаційними структурами.

Виділення невирішених раніше частин загальної проблеми. Інтелектуальні технології швидко розвиваються у сфері кібербезпеки, але все ще залишаються важливі питання, які потребують більш глибокого дослідження. Щоб покращити організаційне управління на ранніх етапах впровадження, потрібно більше зосередитися на вивченні можливостей використання штучного інтелекту, адже більшість існуючих досліджень зосереджені переважно на технічних аспектах виявлення аномальних моделей.

Впровадження рішень на основі штучного інтелекту стикається з безліччю викликів у економічній та організаційній діяльності, незалежно від того, на якому етапі цифрової зрілості перебувають різні галузі. Щоб створити надійні, ефективні та керовані системи кібербезпеки, важливо розуміти ці труднощі та цілеспрямовано їх долати, адже технології штучного інтелекту відіграють у цьому центральну роль.

Дослідження цих питань допоможе розширити теоретичні уявлення про роль штучного інтелекту, який не тільки виявляє кіберзагрози, адаптовані до сучасних гібридних викликів, але й стає важливим елементом інтелектуального управління безпекою в організації. Значення цього дослідження полягає в створенні багаторівневої системи захисту, де ШІ відіграє центральну роль у виявленні, аналізі та нейтралізації ризиків у реальному часі. Це досягається шляхом розробки концепції інтеграції ШІ в систему управління кібербезпекою організації, що не тільки підвищує технічний рівень захисту, а й забезпечує новий рівень управління

конкурентоспроможністю.

Формулювання цілей статті (постановка завдання). Мета дослідження - обґрунтувати та розробити сучасні підходи інтеграції штучного інтелекту в систему кібербезпеки організації, як ключового інструменту інтелектуалізації кіберзахисту організації, для збільшення ефективності виявлення аномалій і протидії гібридним загрозам в контексті управління інформаційно-організаційною діяльністю в умовах цифровізації. Завдання дослідження:

- дослідити особливості кібербезпеки в контексті гібридних загроз та визначити їх ключові фактори;

- розглянути вплив гібридних загроз в кіберпросторі на діяльність організацій;

- визначити роль і можливості штучного розуму в системах гарантування кібербезпеки;

- використовуючи інструменти штучного інтелекту, надати рекомендації щодо виявлення аномалій і захисту від кібератак.

Виклад основного матеріалу дослідження. У сфері кібербезпеки контекст гібридних загроз є надзвичайно складним і багатогранним, що потребує глибокого теоретичного розуміння та розробки системних підходів до захисту інформаційних систем організацій. Поєднання традиційних кібератак з гібридними загрозами, які охоплюють інформаційні, психологічні, соціальні та політичні аспекти, значно ускладнює їх виявлення. Інформаційна стабільність організацій у контексті гібридних загроз залежить від кількох ключових факторів, які показані на рис. 1.

Рис. 1. Ключові фактори впливу на інформаційну стійкість організацій в умовах гібридних загроз

Джерело: сформовано та доповнено автором на основі [12, с. 322]

Для того, щоб організації мали надійну інформацію, їм потрібно вжити технічних, організаційних та управлінських дій, які відповідають характеристикам гібридних загроз. Гібридні небезпеки - це складні, змішані загрози, які використовують різні види та шляхи нападів, такі як кібератаки, інформація та психологічні впливи, політичні маніпуляції, економічний тиск та інші способи непрямого впливу [13, с. 6], щоб досягти стратегічних цілей противника. Моделі гібридних загроз у кібербезпеці часто включають такі елементи (рис. 2):

Рис. 2. Складові гібридних загроз у кібербезпеці

Джерело: сформовано автором на основі [14, с. 52]

Гібридні загрози серйозно впливають на роботу організацій, знижуючи їхню ефективність, порушуючи бізнес-процеси, розкриваючи конфіденційну інформацію, шкодячи репутації та викликаючи юридичні й фінансові проблеми. Особливо вразливі ті організації, які не мають інтегрованих систем захисту і не готові до раптових змін у небезпечних умовах. Тому важливо, щоб організації впроваджували комплексні стратегії для протистояння гібридним загрозам, які поєднують технічні інструменти, політику організації та навчання працівників.

За допомогою моделей штучного інтелекту сучасні системи кібербезпеки допомагають виявляти та прогнозувати зміни в поведінці, що можуть призвести до атак. Як прогресивна мережа безпеки, штучний інтелект має здатність аналізувати великі обсяги даних, виявляти незвичайні патерни та прогнозувати потенційні загрози в реальному часі. Завдяки цьому інструменту можна значно пришвидшити реакцію на кібератаки та підвищити ефективність інформаційних систем. Основна роль штучного інтелекту в кібербезпеці представлена в табл. 1.

Таблиця 1

Роль ШІ у кібербезпеці

Критерій	Особливості
Автоматизоване знаходження загроз та аномалій	Здатність аналізувати поведінку користувачів та мережевий трафік, які можуть свідчити про внутрішні атаки або загрози.
Прогнозування кіберзагроз	AI для визначення тенденції та прогнозування атак
Автоматична реакція на інциденти	Автоматичне реагування на атаки, блокування шкідливих процесів та інформування відповідальних осіб
Покращення систем автентифікації та керування доступом	Створення динамічних систем контролю доступу, які враховують контекст та поведінкові особливості користувачів
Забезпечення кібербезпеки у складних середовищах	Захист складних гібридних систем, де традиційні методи не завжди можуть швидко і точно реагувати на нові види загроз

Джерело: сформовано автором на основі [15, с. 40]

Разом з тим, використання ШІ у кібербезпеці вимагає зважати на можливі небезпеки - приміром, вірогідність маніпулювання алгоритмами, етичні аспекти, а також потребу у кваліфікованих фахівцях для налаштування та контролю таких систем. Надзвичайно важливим завданням для виявлення потенційних загроз, враховуючи невідомі атаки (zero-day) [16], внутрішні порушення чи зловмисні дії, що оминають традиційні засоби захисту є виявлення аномалій у системах кібербезпеки. Сучасні підходи базуються на застосуванні технологій штучного інтелекту, які здатні виявляти відхилення від нормальної поведінки в даних (табл. 2).

Таблиця 2

Сучасні підходи до виявлення аномалій на основі штучного інтелекту

Підходи	Основні методи	Переваги
Машинне навчання (ML)	SVM, Decision Trees, Random Forest, KNN, K-Means, PCA	Велика швидкість. Придатний для впорядкованих даних. Легкість втілення
Ненаглядне навчання	Clustering (K-Means, DBSCAN), Isolation Forest, PCA	Не потребує міток даних. Добре розпізнає невідомі аномалії
Глибоке навчання (DL)	Autoencoders, LSTM, RNN, CNN	Виявлення комплексних закономірностей. Праця з великими обсягами даних.

		Пристосованість
Нейронні мережі (ANN)	Штучні нейронні мережі, гібридні моделі	Гнучкість. Здатність багатоступеневої обробки даних
Комбіновані підходи	ML + SIEM, DL у поєднанні з правилами або експертними системами	Підвищення точності. Зменшення помилкових спрацьовувань

Джерело: сформовано автором на основі [17, с. 180]

З новими та складними кіберзагрозами дозволяють ефективно боротися сучасні методи виявлення аномалій, що базуються на штучному інтелекті. Для підвищення інформаційної стійкості організацій в умовах гібридних загроз важливо інтегрувати ці технології у їхні системи кібербезпеки. Таким чином, виникає потреба у переході до інтелектуальних систем захисту, здатних діяти в реальному часі, адаптуватися до нових викликів та забезпечувати проактивне управління ризиками. Впровадження штучного інтелекту в системи управління кібербезпекою організації є одним із найбільш перспективних методів розвитку [18, с. 222].

Для захисту інформаційного простору інтеграція штучного інтелекту в систему кібербезпеки є стратегічним кроком, який не лише допомагає виявляти та запобігати сучасним кіберзагрозам, але й створює динамічну самонавчальну архітектуру. Використовуючи штучний інтелект як основний інструмент для аналітики, автоматизації та ухвалення рішень цей процес об'єднує технологічні, організаційні та управлінські елементи.

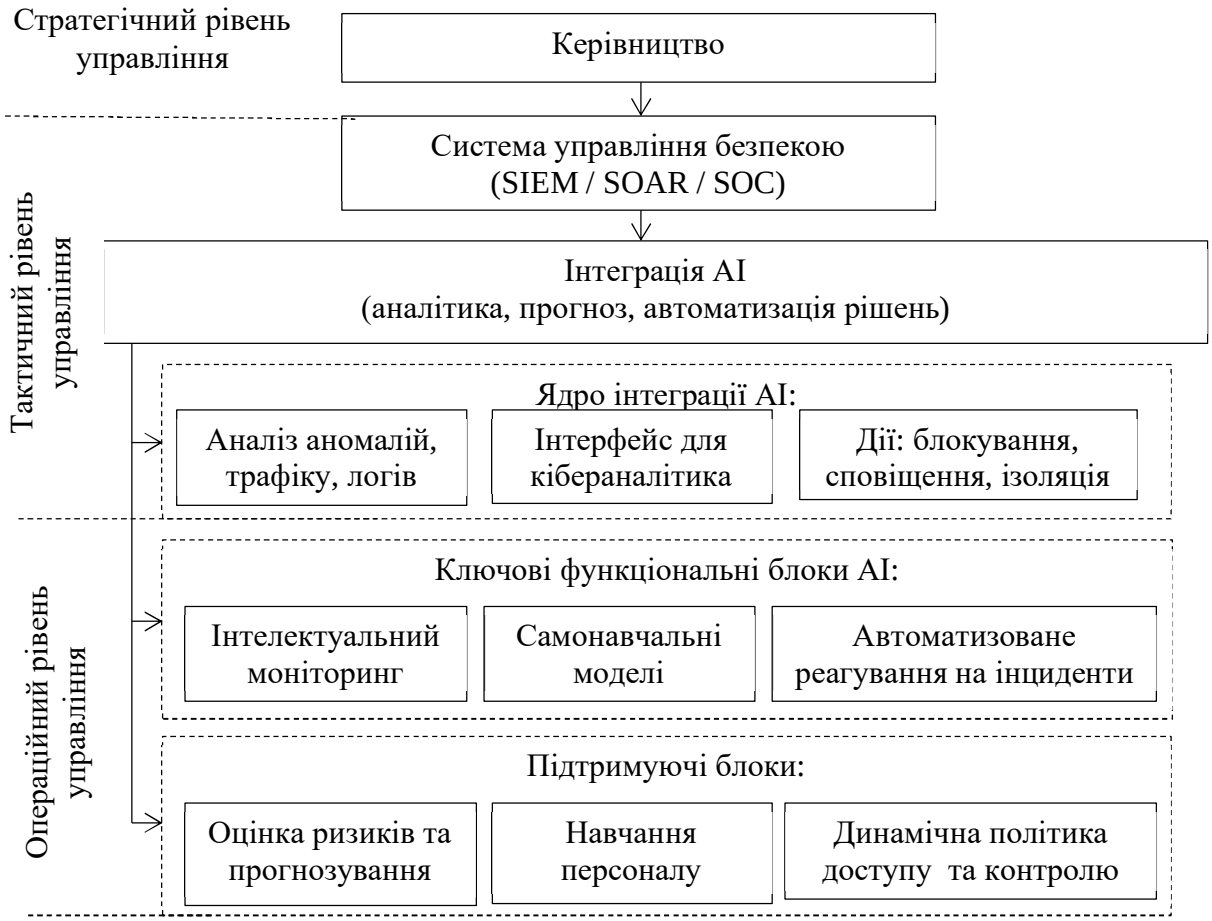

Рис. 3. Концепція інтеграції AI у систему управління кібербезпекою в організації

Джерело: авторська розробка

Ключову роль у виявленні, аналізі та знешкодженні загроз в реальному часі відіграє концепція інтеграції штучного інтелекту в системи мережевої безпеки, що передбачає створення багатошарової оборонної системи. Інтеграція AI на стратегічному рівні починається з визначення основних політик конфіденційності, пріоритетів захисту та інвестицій у впровадження нових технологій. Через використання таких систем безпеки, як SIEM (моніторинг та кореляція) та SOAR (автоматизація реагування) відбувається прийняття цих рішень, що сприяє ефективному впровадженню AI [19].

Створення такої гнучкої та адаптивної архітектури має на меті ефективно протидіяти загрозам. В основі цієї системи лежить штучний інтелект, який покращу. як оперативний, так і стратегічний рівень захисту організації. Впровадження штучного інтелекту в кібербезпеку - це не лише інноваційний прорив у цифровій сфері, а й управлінська еволюція, яка надає організаціям змогу діяти на випередження.

Висновки. Отже, в зазначеній статті було проаналізовано, як штучний інтелект інтегрується в системи кібербезпеки організацій, враховуючи сучасні виклики, зокрема гібридні загрози. Виявилося, що ці загрози є складним поєднанням кібернетичних атак і інформаційно-психологічного впливу, що значно ускладнює їх виявлення традиційними методами. У відповідь на це була розроблена концепція інтегрованої системи безпеки, яка, будучи частиною управління інформаційними ризиками, забезпечує комплексний підхід до моніторингу та оперативного реагування на кіберзагрози.

Перспективним напрямком для подальших досліджень є інтеграція технологій штучного інтелекту в системи кібербезпеки. Це відкриває нові можливості для підвищення рівня захисту інформаційних ресурсів організацій у світі глобальної цифровізації.

Список використаних джерел

1. Скіцько О., Складанний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. Том 2 №22. С. 6–18. DOI: https://doi.org/10.28925/2663-4023.2023.22.618.

2. Шостак Л.В., Федонюк А.А., Помазун О.О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Цифрова економіка та економічна безпека*. 2024. Випуск 3(12). С.121-125. DOI: https://doi.org/10.32782/dees.12-22.

3. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. 2022. № 44. DOI: https://doi.org/10.3278

2/2524-0072/2022-44-21.

4. Zavrazhnyi K., Kulyk A. Modern business cybersecurity challenges and the role of artificial intelligence in countering threats. *Економічний вісник НТУУ «Київський політехнічний інститут»*. 2024. № 30. С.81-86. DOI: https://doi.org/10.20535/2307-5651.30.2024.313042.

5. Хряпинський А.П. Якісно-інноваційні підходи до визначення сутності гібридної війни та гібридних загроз. *Суспільство та національні інтереси*. 2025. 1(9). С. 641-650. URL:https://doi.org/10.52058/3041-1572-2025-1(9)-641-650 (дата звернення: 28.05.2025).

6. Климаш М., Бальковський Н., Шпур О. Гібридна модель виявлення мережевих аномалій з використанням машинного навчання. *Інфокомунікаційні технології та електронна інженерія*. 2025. Вип. 5. № 1. С. 1–14. URL:https://science.lpnu.ua/sites/default/files/journal-paper/2025/apr/38730/paper1klimashbalkovskiyshpur.pdf (дата звернення: 28.05.2025).

7. Лявинець Г. М., Роглєв Й. Й., Бортнічук О. В. Режим детекції аномалій і загроз у великих даних підприємств готельно-ресторанної галузі. *Економіка та суспільство*. 2024. Випуск # 70. DOI: https://doi.org/10.32782/2524-0072/2024-70-29.

8. Schmitt M. Securing the digital world: protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*. 2023. vol. 36. DOI: https://doi.org/10.1016/j.jii.2023.100520.

9. Marwan O. Integrative Approaches in Cybersecurity, Artificial Intelligence, and Data Management: A Comprehensive Review and Analysis. URL:https://arxiv.org/pdf/2408.05888 (дата звернення: 28.05.2025).

10. Hudson J. Artificial Intelligence and Cybersecurity Integration: Modern Database Techniques for Securing AI Models. 2024. URL:https://www.researchgate.net/profiles.pdf (дата звернення: 28.05.2025).

11. Marron D. G., Martinez S. I.- L., Valadez L. A.-S., Ceron A. G. Integration of artificial intelligence techniques and intrusion detection systems in anomaly detection for data networks. *South Florida Journal of Development*. 2024. v.5, n.12. p.1-9. DOI: 10.46932/sfjdv5n12-047.

12. Хряпинський А. П. Перспективні напрями інформаційної політики для протидії гібридним загрозам. *Державне будівництво*. 2024. № 2 (36). С. 322–334. DOI: https://doi.org/10.26565/1992-2337-2024-2-22.

13. Бусол. О.Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. №4. С. 6-15. DOI 10.37749/2308-9636-2020-4(208)-1.

14. Грищук Р.В., Жовноватюк Р.М., Носова Г.Д. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. *Modern Information Technologies in the Sphere of Security and Defence*. 2019. № 3(36). С. 52-58. DOI:10.33099/2311-7249/2019-36-3-53-58.

15. Яненкова І. Г. Штучний інтелект у сфері кібербезпеки: виклики, регулювання, впливи. *Наукові тренди постіндустріального суспільства*. 2025. С.40-49. DOI 10.62731/mcnd-21.03.2025.001.

16. Нульовий день. URL:https://www.vpnunlimited.com/ua/help/cybersecurity/zero-day? (дата звернення: 28.05.2025).

17. Петляк Н. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. *International Scientific-technical journal «Measuring and computing devices in technological processes»*. 2025. Issue 1. С. 180-186. URL:https://doi.org/10.31891/2219-9365-2025-81-21 (дата звернення: 28.05.2025).

18. Одрехівський М., Дарміць Р., Жежуха В. Інтелектуальні інформаційні системи моніторингу компетентностей управлінців інноваційних підприємств. Фінансово-кредитна діяльність: проблеми теорії та практики. 2022. Том 5(46). С.222-238 DOI: 10.55643/fcaptp.5.46.2022.3884.

19. SecOps SOAR: Ключовий елемент сучасної кібербезпеки.

URL:https://itcluster.lviv.ua/secops-soar-klyuchovyj-element-suchasnoyi-kiberbezpeky/ (дата звернення: 28.05.2025).

 ISSN 3041-2129