ключових метрик і KPI гарантує відповідність ходу проєкту запланованим параметрам, а висока автоматизація дозволяє швидко впроваджувати зміни. Як результат, платформа розвивається стабільно та своєчасно масштабується відповідно до зростаючих вимог міського середовища. Зокрема, отримані результати мають практичне значення при розробці великих децентралізованих IT-систем, оскільки демонструють ефективність інтегрованого підходу в складних проектних умовах.

Список використаних джерел

1. Mohammed A. A., Benattou M., Benattou M., Ouzzif M. Smart cities services and solutions: a systematic review [Електронний ресурс] / A. A. Mohammed, M. Benattou, M. Benattou, M. Ouzzif // Sustainable Computing: Informatics and Systems. – 2024. – Т. 40. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2543925124000238 (дата звернення: 27.05.2025).
2. Cooper R. G. Winning at New Products: Creating Value Through Innovation / R. G. Cooper. – New York : Basic Books, 2017. – 448 с.
3. Ciancarini P., Giancarlo R., Grimaudo G. Digital transformation in the public administrations: a guided tour for computer scientists [Електронний ресурс] / P. Ciancarini, R. Giancarlo, G. Grimaudo // IEEE Access. – 2024. – Вип. 12 – С. 22841–22865. – Режим доступу: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10423006 (дата звернення: 27.05.2025).
4. Acebes F., González-Varona J. M., López-Paredes A., Pajares J. Beyond probability-impact matrices in project risk management: a quantitative methodology for risk prioritisation [Електронний ресурс] / F. Acebes, J. M. González-Varona, A. López-Paredes, J. Pajares // Humanities and Social Sciences Communications. – 2024. – Т. 11 – Art. 670. – Режим доступу: https://doi.org/10.1057/s41599-024-03180-5 (дата звернення: 27.05.2025).

ГОНКА ОЗБРОЄНЬ У КІБЕРБЕЗПЕЦІ: ПРОАКТИВНІ СТРАТЕГІЇ ЗАХИСТУ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Співак Вадим
асистент
кафедра економічної кібернетики,
комп’ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет, Україна

Сучасний кіберпростір перетворився на динамічну арену протистояння, де технологічний прогрес невпинно змінює правила гри. Штучний інтелект (ШІ) став однією з ключових технологій подвійного призначення, що одночасно надає потужні інструменти як для здійснення витончених кібератак, так і для розробки

інноваційних методів захисту. Це призвело до виникнення феномену, який можна охарактеризувати як "гонка озброєнь ШІ" в кібербезпеці – безперервний цикл розробки та впровадження все більш досконалих ШІ-технологій атакуючими сторонами та захисниками [1]. Актуальність цієї теми зумовлена стрімким зростанням кількості, складності та адаптивності ШІ-керованих кібератак, що ставлять під загрозу критичну інфраструктуру, корпоративні дані та приватність користувачів. Метою даної роботи є аналіз сучасної динаміки гонки озброєнь ШІ в кібербезпеці, виявлення ключових викликів, пов'язаних із цим процесом, та окреслення перспективних напрямків для розробки проактивних стратегій захисту. Основна теза полягає в тому, що для ефективної протидії зростаючій загрозі ШІ-керованих атак необхідна розробка та впровадження адаптивних, етично обґрунтованих та належним чином керованих ШІ-орієнтованих захисних механізмів.

Використання штучного інтелекту кіберзлочинцями значно підвищило рівень загроз, надавши їм можливості для автоматизації, масштабування та підвищення ефективності атак [3]. Одним із яскравих прикладів є фішинг на основі ШІ (AI-powered phishing), де зловмисники використовують алгоритми генерації природної мови для створення високоперсоналізованих та надзвичайно переконливих фішингових повідомлень, які важко відрізнити від легітимних [3].

Крім того, ШІ дозволяє створювати динамічні та адаптивні атаки, здатні аналізувати захисні механізми цільової системи та змінювати свою тактику в реальному часі для їх обходу [1]. Це включає автоматизоване виявлення вразливостей у програмному забезпеченні та мережевих конфігураціях, а також розробку та застосування експлойтів з мінімальним втручанням людини.

Особливе занепокоєння викликає концепція "Агентного ШІ" (Agentic AI), яку Gartner виділяє як одну з ключових технологічних тенденцій на 2025 рік [4]. Йдеться про автономні ШІ-системи, здатні самостійно планувати, координувати та здійснювати складні багатоетапні кібератаки, що значно ускладнює їх виявлення та нейтралізацію. Демократизація доступу до потужних ШІ-інструментів також сприяє зниженню порогу входу для кіберзлочинців, дозволяючи навіть менш кваліфікованим атакуючим здійснювати складні атаки, які раніше були доступні лише високоорганізованим групам.

Паралельно з використанням ШІ в атаках, він стає незамінним інструментом і для захисту. Штучний інтелект та машинне навчання (МН) є основою багатьох сучасних систем кібербезпеки, дозволяючи ефективніше протидіяти новим та невідомим загрозам [1].

Однією з ключових переваг ШІ в захисті є його здатність аналізувати величезні обсяги даних (наприклад, мережевий трафік, системні журнали, поведінкові патерни користувачів) для виявлення аномалій та прихованих ознак шкідливої активності, які можуть бути непомітними для традиційних сигнатурних методів.6 Це дозволяє виявляти атаки "нульового дня" та складні цілеспрямовані загрози (APT).

ШІ також використовується для прогнозування потенційних атак на основі аналізу поточних тенденцій та вразливостей, що дає можливість організаціям

завчасно вживати превентивних заходів. Автоматизоване реагування на інциденти за допомогою ШІ дозволяє значно скоротити час реакції на атаку, блокувати шкідливу активність та мінімізувати потенційні збитки. Спостерігається еволюція центрів управління безпекою (SOC), які все більше покладаються на процеси, керовані ШІ, для підвищення ефективності моніторингу та реагування [1]. Таким чином, ШІ-керований захист забезпечує вищу швидкість реакції, глибший аналіз та кращу адаптивність до постійно мінливого ландшафту загроз.

Безперервне вдосконалення ШІ-алгоритмів як атакуючими, так і захисниками, створює динамічну "гонку озброєнь", де кожна сторона намагається отримати технологічну перевагу [1]. Цей циклічний характер протистояння робить традиційні, статичні підходи до безпеки все менш ефективними. Організації стикаються з низкою серйозних викликів, що вимагають розробки комплексних та проактивних стратегій.

Технологічні виклики включають необхідність створення ШІ-систем захисту, які були б не тільки ефективними, але й надійними, стійкими до спроб обману (adversarial attacks) та забезпечували б достатній рівень прозорості та інтерпретованості своїх рішень (Explainable AI – XAI).

Етичні та управлінські виклики є не менш значущими. Необхідно розробити чіткі рамки та стандарти для відповідального використання ШІ в кібербезпеці, що запобігали б упередженості в алгоритмах (наприклад, дискримінаційне маркування певних груп користувачів), забезпечували б підзвітність у випадку помилок автономних ШІ-агентів та гарантували б довіру до таких систем [4].

Кадрові виклики пов'язані з гострим дефіцитом фахівців, які володіють необхідними компетенціями на перетині ШІ та кібербезпеки.

Для ефективної протидії в умовах "гонки озброєнь ШІ" необхідні стратегічні імперативи, спрямовані на проактивний захист:

- Інвестиції в дослідження та розробку: постійне фінансування створення передових ШІ-технологій для захисту, включаючи методи виявлення та протидії атакам, керованим ШІ.
- Впровадження принципів "Безпека через проектування" (Security by Design) та "Конфіденційність через проектування" (Privacy by Design): інтеграція вимог безпеки та конфіденційності на всіх етапах життєвого циклу ШІ-систем.
- Розвиток міжнародного співробітництва: обмін інформацією про нові загрози, найкращі практики та розробка спільних стандартів для безпечного використання ШІ.
- Підвищення рівня кіберграмотності: формування культури безпеки в організаціях та навчання персоналу методам розпізнавання та протидії ШІ-атакам, зокрема фішингу та соціальній інженерії [7].

Подальший прогрес у забезпеченні кібербезпеки в епоху ШІ вимагає цілеспрямованих досліджень у кількох ключових напрямках:

- Пояснюваний ШІ (XAI) в кібербезпеці: розробка методів, що дозволяють аналітикам безпеки розуміти, як ШІ-системи приймають рішення, для підвищення довіри та ефективності їх використання.

- Протидія дезінформації, керованій ШІ: створення технологій для виявлення та нейтралізації дезінформаційних кампаній, що використовують ШІ-згенерований контент (наприклад, діпфейки) для маніпуляції громадською думкою або підтримки кібератак [8].
- Управління та контроль автономних ШІ-агентів: дослідження моделей та протоколів для безпечного та контрольованого функціонування автономних ШІ-систем у кіберпросторі, включаючи механізми запобігання непередбачуваній поведінці.
- Масштабовані та доступні ШІ-рішення: розробка ефективних та економічно доцільних ШІ-інструментів для захисту організацій різного розміру, включаючи малий та середній бізнес.
- Федеративне навчання для обміну розвідданими: вивчення потенціалу технологій федеративного навчання для створення децентралізованих систем обміну інформацією про загрози без розкриття конфіденційних даних учасників.

Отже, "гонка озброєнь ШІ" є визначальною та невідворотною характеристикою сучасного ландшафту кібербезпеки. Зловмисники все активніше використовують можливості штучного інтелекту для створення більш складних, автоматизованих та руйнівних атак. У відповідь, захисники змушені також вдаватися до ШІ-технологій для розробки адаптивних та інтелектуальних систем оборони.

Ефективна протидія в цих умовах вимагає не просто реактивного нарощування технологічних потужностей, а комплексного, проактивного та етично обґрунтованого підходу. Це включає постійні інвестиції в дослідження та розробку передових захисних ШІ-систем, створення надійних механізмів управління та контролю за використанням ШІ, а також підготовку висококваліфікованих фахівців.

Ключовими аспектами успіху в цій "гонці озброєнь" стануть здатність до швидких інновацій, побудова довіри до ШІ-керованих систем безпеки, а також розвиток міжнародного співробітництва для спільної протидії глобальним кіберзагрозам. Лише такий багатогранний підхід дозволить забезпечити перевагу захисників та створити більш безпечний цифровий простір для суспільства та бізнесу в епоху тотального проникнення штучного інтелекту.

Список використаних джерел

1. EC-Council University. (2024). Emerging technologies driving the future of cybersecurity in 2025. Retrieved from https://www.eccu.edu.ua/blog/emerging-technologies-driving-the-future-of-cybersecurity-in-2025/
2. ENISA. (2025). ENISA Disinformation Alert. Retrieved from https://www.enisa.europa.eu/
3. Forrester. (2024). Forrester's Top 10 Emerging Technologies For 2025: Automation Evolves, Robots Rise, And Synthetic Data Steps Forward. Retrieved from https://www.forrester.com/technology/top-emerging-technologies/
4. Gartner. (2024). Top technology trends 2025. Retrieved from https://www.gartner.com/en/articles/top-technology-trends-2025

5. National CIO Review. (2024, March 16). Cybersecurity in 2025: The trends reshaping security strategies. Retrieved from https://nationalcioreview.com/articles-insights/cybersecurity-in-2025-the-trends-reshaping-security-strategies/
6. Otava. (2024). 2025 Trends in Edge Computing Security. Retrieved from https://www.otava.com/2025-trends-in-edge-computing-security/
7. Palo Alto Networks. (2024). Cybersecurity in 2025: How One Year Will Reshape the Industry. Retrieved from https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
8. Splunk. (2024). Cybersecurity Trends. Retrieved from https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html
9. Strobes.co. (2024). 10 Cybersecurity Trends to Watch in 2025 and How to Prepare. Retrieved from https://strobes.co/blog/10-cybersecurity-trends-to-watch-in-2025-and-how-to-prepare/

ІНФОРМАЦІЙНА БЕЗПЕКА В ІНТЕРНЕТІ: ЗАГРОЗИ, ЗАХИСТ, КУЛЬТУРА ТА ПРАВО

Деркач Тетяна
к.т.н., доцент
Гринюк Данило
здобувач вищої освіти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

У сучасному цифровому світі інтернет став невід'ємною частиною повсякденного життя. Він відкриває безліч можливостей – від спілкування та розваг до банківських операцій і дистанційної роботи. Однак поряд із перевагами виникають серйозні загрози, пов’язані з інформаційною безпекою. Уразливість персональних даних, шахрайство, віруси та атаки хакерів – усе це створює виклики, з якими стикається як окрема людина, так і суспільство в цілому. Інформаційна безпека – це сукупність заходів, спрямованих на захист інформації від несанкціонованого доступу, модифікації, знищення або розголошення. Вона охоплює не лише технічні аспекти, такі як шифрування чи захист від вірусів, а й організаційні та правові заходи.

Забезпечення інформаційної безпеки передбачає дотримання принципів конфіденційності, цілісності та доступності інформації [3].

Сучасна концепція інформаційної безпеки включає також питання етики в цифровому середовищі, дотримання прав користувачів на приватність, а також створення безпечного інформаційного простору для всіх учасників мережі.

Основні загрози в мережі. Сучасний Інтернет надає великі можливості, але водночас є джерелом численних кіберзагроз.

Шкідливе програмне забезпечення (віруси, трояни, програми-шпигуни) здатне збирати інформацію без відома користувача.