УДК 004.056.5 DOI: 10.63978/3083-6476.2025.3.3.08

Лисецький Юрій Михайлович
доктор технічних наук, доцент
професор кафедри
Воєнна академія імені Євгенія Березняка
Київ, Україна
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ

Анотація. *Розглянуто ретроспективу виникнення і розвитку штучного інтелекту. Наведено, що справжній прорив у використанні штучного інтелекту почався 2010 року з розвитком машинного навчання та глибоких нейромереж. Проаналізовано можливості штучного інтелекту як перспективної технології для використання у сфері кібербезпеки. Показано, що технології штучного інтелекту мають потенціал принести абсолютно нові можливості, зокрема трансформувати кібербезпеку, а їхнє застосування матиме значний вплив у сфері безпеки й оборони.*

Ключові слова: *штучний інтелект, технології, кіберзагрози, кібербезпека, аналіз, прогнозування, моніторинг, ідентифікація, шифрування.*

Yurii Lysetsyi
Doctor of Engineering Sciences, associate professor
professor of the department
Yevhenii Bereznyak Military Academy
Kyiv, Ukraine
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Abstract. *The article is devoted to researching the possibilities of using artificial intelligence in cybersecurity. The idea of creating artificial intelligence emerged in the mid-20th century. Alan Turing, one of the most famous English mathematicians, logicians, and cryptographers, was the first to conduct significant research in the field he called machine intelligence. The term "artificial intelligence" was officially introduced in 1956 at a conference at Dartmouth College, where a group of scientists discussed the potential for creating machines capable of performing tasks that require human intelligence. Practical steps in the creation of artificial intelligence were taken in the mid-20th century, when the first computers appeared. A real breakthrough in the use of artificial intelligence began in 2010 with the development of machine learning and deep neural networks, known as deep learning. Digitalization, Big Data, and the ability to process large amounts of data have provided a powerful resource for machine learning. Using large data sets and powerful computing resources, neural networks have begun to achieve incredible results in areas such as natural language processing, image recognition, data analysis, and more. Artificial intelligence is also actively used to address cybersecurity issues at many levels. Artificial intelligence plays a key role in predicting cyber threats thanks to its ability to process large amounts of data and identify complex patterns of behavior; can improve network monitoring through automation and increased data analysis accuracy; can significantly improve identification and access to information systems in many ways. Artificial intelligence opens up new horizons in cybersecurity, but at the same time, it can create serious threats, including attack automation, improved phishing attacks, use in deepfakes, data manipulation, and the creation of new types of vulnerabilities. Therefore, the key to protecting against these threats is the development of comprehensive cybersecurity strategies that involve the use of artificial intelligence as an effective protection tool.*

Keywords: *artificial intelligence, technology, cyber threats, cybersecurity, analysis, forecasting, monitoring, identification, encryption.*

Вступ

Постановка проблеми. Ідеї створення штучного інтелекту (ШІ) виникли в середині XX ст. Алан Тюрінг – один із найвідоміших англійських математиків, логіків і криптографів – був першим, хто здійснив істотні дослідження в галузі, яку він називав машинним інтелектом (англ. Machine Intelligence) [1]. У 1950 році Тюрінг опублікував статтю “Computing Machinery and Intelligence”, у якій запропонував експеримент “Тюрінга” як критерій інтелектуальної поведінки машин [2].

Офіційно термін “штучний інтелект” було запроваджено у 1956 році на конференції в Дартмутському коледжі, де група вчених, зокрема Джон Маккарті та Марвін Мінський, обговорювали потенціал створення машин, здатних виконувати завдання, що потребують людського інтелекту.

Практичні кроки зі створення ШІ було зроблено в середині XX ст., коли з’явилися перші комп’ютери. Вчені та інженери почали замислюватися над тим, як зробити комп’ютери розумнішими та здатними до автономного прийняття рішень.

Першим етапом стали досягнення в галузі логічного інтелекту. Було створено програмне забезпечення, здатне розв’язувати складні логічні задачі та робити логічні висновки. Наступним етапом стало створення експертних систем, здатних приймати складні рішення в певній сфері на основі знань, накопичених спеціалістами в цій галузі. Ці системи дали можливість автоматизувати вирішення багатьох задач, що призвело до суттєвого підвищення продуктивності та ефективності в різних сферах діяльності.

Наприкінці XX ст. та на початку XXI ст. спостерігався стрімкий розвиток у галузі ШІ. Еволюція комп’ютерних технологій, поява великих даних та розвиток машинного навчання сприяли створенню систем, здатних розпізнавати образи, обробляти природну мову та прогнозувати майбутні події. Ці нові технології застосовуються в багатьох сферах, зокрема в безпеці та оборони [3–7]. Зважаючи на це питання, дослідження можливостей використання ШІ в кібербезпеці є досить актуальним.

Аналіз останніх досліджень і публікацій. Застосування ШІ в різних сферах, зокрема у безпеці й обороні, а також у кібербезпеці, висвітлено в наукових працях як зарубіжних, так і вітчизняних дослідників [3–9]. Однак питання використання ШІ у сфері забезпечення кібербезпеки потребують подальших, більш системних досліджень.

Мета статті – проаналізувати можливості ШІ в контексті їхнього використання у сфері кібербезпеки.

Виклад основного матеріалу

З огляду на величезні обсяги даних, з якими доводиться працювати нині, переважна більшість організацій та установ, зокрема оборонного та безпекового сектору, вже використовує можливості ШІ для забезпечення кібербезпеки. За оцінкою MarketsandMarkets, у 2019-2026 рр. ринок засобів ШІ для забезпечення кібербезпеки зростатиме в середньому на 23,3 % за рік – з 8,8 до 38,2 млрд доларів (рис. 1). ШІ активно використовується для вирішення питань кібербезпеки на багатьох рівнях [7–9]. Сучасні системи ШІ здатні аналізувати більші обсяги даних швидше, ніж людина, і виявляти складні шаблони або аномалії, які можуть вказувати на потенційні загрози. ШІ застосовується також для підвищення ефективності захисту кінцевих точок, таких як антивіруси та фаєрволи, що дає змогу передбачати та блокувати атаки заздалегідь.

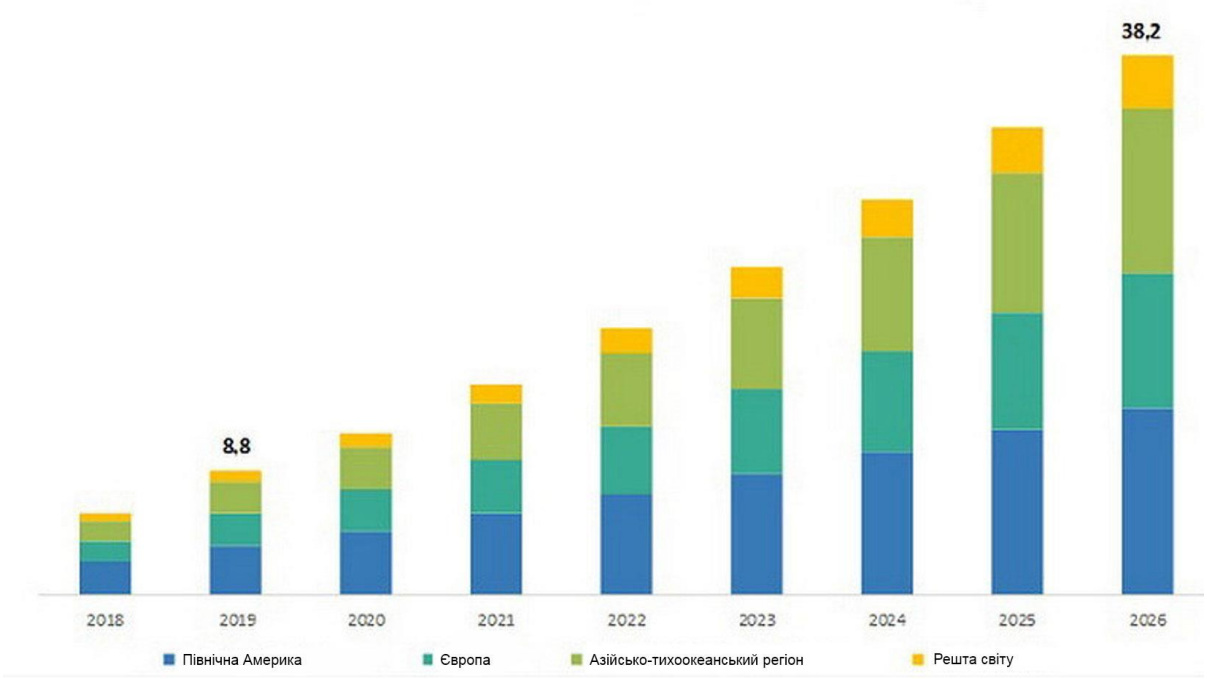

Рис. 1. Динаміка зростання ринку засобів ШІ для забезпечення кібербезпеки, млрд дол.

Основні напрямки застосування ШІ у сфері кібербезпеки:

прогнозування загроз (ідентифікація потенційних нових вразливостей та кібератак до того, як вони стануть серйозними проблемами);

автоматизація відповідей на інциденти (реагування ШІ на інциденти безпеки, що скорочує час на їх вирішення);

розумний моніторинг мережі (моніторинг мережевої активності та виявлення аномалій, які можуть свідчити про несанкціонований доступ чи вторгнення);

управління ідентифікацією та доступом (зміцнення систем управління доступом, що забезпечує можливість входу лише уповноваженим користувачам);

шифрування SSL/TLS (безпечні протоколи зв'язку, що використовують ШІ, допомагають забезпечити захист даних під час передачі).

Сьогодні ШІ є не просто зручним інструментом, а необхідною складовою ефективної системи захисту від кіберзагроз.

ШІ відіграє ключову роль у прогнозуванні кіберзагроз завдяки своїй здатності обробляти великі обсяги даних та виявляти складні зразки поведінки, що зазвичай неможливо в разі застосування традиційних аналітичних методів. У цьому процесі ШІ може допомагати, виконуючи такі функції:

аналіз даних у реальному часі (моніторинг та аналіз мережевого трафіку щодо аномальної поведінки, яка вказує на потенційні кіберзагрози);

автоматизація виявлення загроз (автоматизація процесів виявлення та класифікації загроз, що скорочує час реакції на інциденти безпеки);

підвищення точності прогнозів (завдяки машинному навчанню системи на базі ШІ можуть навчатися, вдосконалюватися через досвід атак та прогнозувати майбутні загрози);

виявлення невідомих загроз (ідентифікація нових кіберзагроз шляхом аналізу моделей поведінки, що мають відхилення від норми);

адаптація до нових загроз (здатність адаптуватися до змін у кіберзагрозах, постійно оновлюючи бази даних та методи захисту).

Використання ШІ не лише допомагає у прогнозуванні та виявленні кіберзагроз, а й сприяє забезпеченню більш адекватної та ефективної відповіді на кіберінциденти, зменшенню фальшивих спрацьовувань та зниженню витрат на захист інформаційних систем (ІС).

ШІ може допомогти у вирішенні таких питань:

швидке виявлення інцидентів (аналіз величезних обсягів даних у реальному часі та швидке виявлення аномалій, що вказують на потенційні кібератаки. Це дає можливість своєчасно реагувати на кіберзагрози);

класифікація та пріоритизація інцидентів (визначення ступеня небезпеки кіберінцидентів та пріоритизація відповіді з метою зосередження команди кібербезпеки на найкритичніших загрозах);

автоматизоване реагування (на відомі типи атак ШІ може автоматично відповідати такими діями, як ізоляція заражених ІС, блокування зловмисного трафіку або скидання паролів для мінімізації потенційних збитків);

адаптивне навчання (використовуючи машинне навчання, системи ШІ постійно вдосконалюються на прикладах з кожного кіберінциденту, підвищуючи здатність передбачати майбутні кіберзагрози та реагувати на них);

підтримка прийняття рішень (надання рекомендацій щодо оптимальних дій для відповіді на конкретні типи кіберзагроз, допомога аналітикам у прийнятті обґрунтованих рішень з питань кібербезпеки);

зменшення фальшивих спрацьовувань (завдяки точному аналізу даних ШІ може розрізняти легітимну діяльність від справжніх кіберзагроз, що зменшує кількість хибних тривог і підвищує продуктивність роботи команд кібербезпеки).

Застосування ШІ в автоматизації відповідей на інциденти кібербезпеки суттєво підвищує здатність організацій ефективно захищатися від кіберзагроз, скорочує час реакції на інциденти та забезпечує високий рівень захисту ІС.

ШІ може покращити моніторинг мереж за допомогою автоматизації та підвищення точності аналізу даних. Відзначимо кілька способів використання ШІ для розумного моніторингу мереж:

автоматизація виявлення аномалій (аналіз патернів мережевого трафіку в реальному часі та виявлення аномалій, що вказують на несанкціонований доступ або інші види кібератак. Це дає можливість швидше реагувати на потенційні загрози);

підвищення точності прогнозування (завдяки машинному навчанню ШІ може точніше прогнозувати потенційні кіберзагрози та аномалії в мережі, зменшуючи кількість хибнопозитивних спрацьовувань);

оптимізація пропускної здатності (аналіз патернів трафіку з метою оптимізації використання ресурсів мережі, підвищення її ефективності та зниження заторів);

ідентифікація та класифікація загроз (автоматична ідентифікація кіберзагроз та їх класифікація їх за типами на основі аналізу даних, що дає змогу виявляти потенційні ризики для мережі);

автоматизоване відновлення мережі після кіберінцидентів (автоматизація процесів відновлення мережі після кібератак, швидка ізоляція пошкоджених ІС та відновлення їхньої нормальної роботи);

безперервне навчання та адаптація (системи ШІ постійно “навчаються”, збільшуючи обсяг даних, що дає змогу адаптуватися до нових загроз та тактик кібератак).

Використання ШІ для розумного моніторингу мереж забезпечує глибший і точний аналіз даних, допомагаючи виявляти кіберзагрози та реагувати на них більш ефективно та з меншими витратами ресурсів.

ШІ може суттєво вдосконалити ідентифікацію та доступ до ІС за багатьма параметрами, зокрема:

розпізнавання облич (використання біометричних даних для розпізнавання осіб та надання доступу до ІС або приміщень);

аналіз поведінки користувачів (застосування алгоритмів машинного навчання для аналізу звичних дій користувачів допомагає ідентифікувати втручання, що можуть свідчити про неавторизований доступ);

автоматичне управління доступом (автоматизація процесів надання чи відкликання доступу, що базується на визначених критеріях, таких як рівень безпеки, час входу тощо);

виявлення шкідливого програмного забезпечення (виявлення та блокування шкідливого ПЗ, за допомогою якого зловмисники можуть намагатися отримати несанкціонований доступ до ІС);

посилення кіберзахисту (інтеграція ШІ в системи ідентифікації посилює кіберзахист, оскільки ШІ постійно навчається та адаптується до нових атак);

інтеграція з іншими системами (легка інтеграція ШІ з різними системами управління ідентифікацією та доступом (англ. Identity and Access Management – IAM) підвищує ефективність управління ідентифікацією).

Використання ШІ в системах управління ідентифікацією та доступом може надати організаціям та установам перевагу в швидкості, точності та ефективності захисту своїх ІС. ШІ може зіграти ключову роль у посиленні безпеки протоколів зв'язку, а саме від SSL/TLS, що використовують для шифрування даних під час їх передавання мережею. Він може це забезпечувати кількома способами:

виявлення аномалій (аналіз шаблонів мережевого трафіку з метою виявляння відхилень, які можуть вказувати на спроби злому системи шифрування або інші кібератаки);

автоматичне оновлення та підтримка (забезпечення актуальності протоколів, автоматизація оновлення криптографічних ключів та сертифікатів безпеки);

машинне навчання для прогнозування (застосування методів машинного навчання для прогнозування та виявлення потенційних зламів до того, як вони стануться, що дає можливість проактивно захищати ІС);

автоматизоване тестування безпеки (проведення комплексного тестування безпеки протоколів для виявлення слабких місць та вразливотей у шифруванні даних);

підтримка складних систем (забезпечення підтримання складних систем шифрування, які є надто важкими для ручного управління).

У використанні ШІ для підтримки безпечних протоколів зв'язку ключовим елементом є постійне вдосконалення технологій та адаптація до нових загроз, а також можливість масштабування, що є необхідною для захисту даних у сучасному цифровому світі.

ШІ відкриває нові горизонти у сфері кібербезпеки, але водночас може створювати й серйозні загрози [10]:

автоматизація атак (використання ШІ для створення і проведення швидких та ефективних кібератак, які важко виявляти та блокувати традиційними методами);

поліпшення фішингових атак (за допомогою ШІ фішингові атаки можуть стати більш переконливими, оскільки здатні імітувати патерни людського письма та поведінки);

використання у глибоких підробках (deepfake) (створення дуже реалістичних аудіо- та відеопідробок, що сприяють поширенню дезінформації та впливу на громадську думку або індивідуальні рішення);

маніпулювання даними (використання ШІ для маніпулювання даними або їх зміни без виявлення, що може мати серйозні наслідки для збереження цілісності інформації);

створення нових видів вразливостей (інтеграція ШІ в системи кібербезпеки може відкрити нові вразливості, які здатні використати зловмисники);

автономні кіберзброї (використання ШІ у створенні автономної кіберзброї може призвести до незворотних атак, які можуть бути запущені без людського втручання).

Отже, ключ до захисту від цих загроз – розробка комплексних стратегій кібербезпеки, які передбачають використання ШІ як ефективного інструменту захисту.

Висновки

Таким чином, справжній прорив у використанні ШІ розпочався 2010 року з розвитком машинного навчання та глибоких нейромереж. Цифровізація, BigData та можливість обробки великих обсягів даних забезпечили потужний ресурс для машинного навчання. Використовуючи значні набори даних та потужні обчислювальні ресурси, технології ШІ почали досягати вражаючих результатів у багатьох сферах, зокрема у сфері безпеки та оборони. Технології ШІ мають потенціал принести абсолютно нові можливості, трансформувати кібербезпеку та дати можливість розв'язувати проблеми, які раніше були недосяжними. Застосування технологій ШІ в сфері безпеки та оборони матиме особливо значний вплив вже в найближчій та середній перспективі.

Список літератури

1. Виникнення штучного інтелекту : історія та сучасність (ШІ). URL: https://catsite.com.ua/vynyknennya-shtuchnogo-intelektu-istoriya-ta-suchasnist-shi/#google_vignette (дата звернення: 02.09. 2025).
2. Turing A. M. Computing Machinery and Intelligence. *Mind.* 1950. № 49. С. 433-460.
3. Сфери застосування штучного інтелекту. URL: https://aiconference.com.ua/uk/news/oblasti-primeneniya-iskusstvennogo-intellekta-92253 (дата звернення: 02.09.2025).
4. 17 прикладів застосування штучного інтелекту у повсякденному житті. URL: https://futurenow.com.ua/5-prykladiv-shtuchnogo-intelektu-u-shhodennomu-zhytti/#google_vignette (дата звернення: 02.09.2025).
5. Кармазіна М. С. Використання штучного інтелекту в освіті та науковому аналізі. *Вісник воєнної розвідки.* 2024. № 77. С. 83–87.
6. Алексєєнко І. В., Дзядук Д. О., Кармазіна М. С., Лисецький Ю. М., Мокляк С. П., Смолянюк В. Ф., Ткач І. М. Штучний інтелект як чинник забезпечення національної безпеки : монографія / за заг. ред. С. П. Мокляка. Київ : ЛАТ&К, видавець Бихун В. Ю., 2025. 236 с.
7. Вплив штучного інтелекту на сферу кібербезпеки. URL: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/ (дата звернення: 10.03. 2024).
8. "Штучний інтелект не захистить, якщо не використовувати інтелект природний": як розвиток ШІ впливає на кібербезпеку. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 10.09.2025).
9. Лисецький Ю. М., Данченко О. І. Використання штучного інтелекту в сфері кібербезпеки. *Вісник воєнної розвідки*. 2025. № 86. С. 42–45.
10. Загрози та ризики використання штучного інтелекту. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520 (дата звернення: 12.09. 2025).