КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1139
УДК 004.056.5

Ільєнко Анна Вадимівна
кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0001-8565-1117
anna.ilienko@npp.nau.edu.ua

Кривокульська Ольга Олексіївна
старший викладач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0003-8518-6915
olha.kryvokulska@npp.kai.edu.ua

Яковенко Олеся Леонідівна
старший викладач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0003-2998-9767
olesia.yakovenko@npp.kai.edu.ua

Телющенко Валентина Анатоліївна
асистент кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0001-6026-5105
valentyna.teliushchenko@npp.kai.edu.ua

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ У КІБЕРБЕЗПЕЦІ: АНАЛІЗ ПОТЕНЦІАЛУ ТА ВИКЛИКІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. У статті здійснено системний аналіз можливостей та викликів застосування штучного інтелекту (ШІ) у сфері кібербезпеки. Обґрунтовано доцільність інтеграції ШІ-технологій у сучасні стратегії кіберзахисту в умовах зростання складності та інтенсивності кіберзагроз. Визначено основні напрями використання ШІ, зокрема автоматизацію виявлення аномалій, прогнозування кіберзагроз, прискорення реагування на інциденти та формування адаптивних систем захисту. Проаналізовано практичні кейси впровадження ШІ-рішень, що підтверджують підвищення точності детекції загроз і скорочення часу реагування. Окрему увагу приділено ризикам і вразливостям ШІ-орієнтованих систем, зокрема загрозам типу adversarial attacks та data poisoning, а також використанню ШІ зловмисниками для реалізації AI-асистованих атак. Розглянуто перспективи розвитку технологій ШІ у 2025–2026 роках, включаючи впровадження автономних інтелектуальних агентів (agentic AI) у центрах операційного кіберзахисту. Показано, що перехід до автономних моделей захисту потребує посилення контролю, застосування гібридних підходів (ШІ у поєднанні з експертним наглядом людини) та вдосконалення нормативно-етичних механізмів регулювання. Результати дослідження дозволяють сформувати комплексне бачення еволюції ШІ-орієнтованих систем кіберзахисту та обґрунтовують необхідність збалансованого поєднання технологічних можливостей і управління ризиками.

Ключові слова: штучний інтелект, кібербезпека, атаки, машинне навчання, виявлення аномалій, прогнозування кіберзагроз, алгоритми самонавчання, адаптивні системи захисту, кіберзахист, зловживання ШІ, кіберзагрози.

ВСТУП

Актуальність теми. У сучасних умовах інформаційні технології стали фундаментом цифровізації практично всіх сфер суспільного життя. Від бізнесу та державного

управління до медицини й наукових досліджень – інформаційні системи відіграють ключову роль у забезпеченні функціонування та сталого розвитку.

Загрози у кіберпросторі стають більш комплексними, швидкими та адаптивними, застосовуючи як вже відомі вразливості, так і нові, раніше невідомі. Це створює постійні ризики для різних сфер – комерційних структур, приватного бізнесу, об'єктів критичної інфраструктури, органів державної влади, фінансової та енергетичної галузей. Найбільшу уразливість мають масштабні мережеві системи, що використовують хмарні сервіси, дистанційний доступ та автоматизоване управління процесами.

Поширення нових методів атак, зокрема ботнет-кампаній, фішингових схем, атак на бази даних та складних DDoS-атак, свідчить про обмежену ефективність традиційних підходів до кіберзахисту в умовах постійної еволюції загроз. У цьому контексті особливого значення набуває застосування штучного інтелекту (ШІ), який має значний потенціал для прогнозування, виявлення та нейтралізації кіберзагроз. Завдяки здатності обробляти великі обсяги даних і навчатися на основі нової інформації, ШІ забезпечує можливість виявлення аномалій у режимі реального часу та адаптації до змін у кіберпросторі. Постійне вдосконалення зловмисниками методів обходу систем захисту зумовлює необхідність використання інтелектуальних алгоритмів для своєчасного виявлення та мінімізації наслідків атак. Динамічний характер кіберзагроз вимагає впровадження адаптивних технологій, здатних оперативно реагувати на зміни у характері атак і прогнозувати потенційні ризики. У цьому аспекті штучний інтелект розглядається як перспективний інструмент підвищення ефективності кіберзахисту, що забезпечує поєднання безпеки, гнучкості та адаптивності систем захисту.

Особливої актуальності зазначені питання набувають у контексті забезпечення кібербезпеки об'єктів критичної інфраструктури (КІ) та суб'єктів авіаційної діяльності, для яких порушення цілісності, доступності чи конфіденційності інформаційних систем може мати системні наслідки для національної безпеки, безпеки польотів та безперервності функціонування стратегічно важливих процесів [18]. Саме тому підвищення ефективності кіберзахисту має супроводжуватися переходом від суто технічних засобів реагування до комплексного ризик-орієнтованого підходу, у межах якого штучний інтелект використовується не лише для детекції інцидентів, а й для формалізованого оцінювання ризиків їх виникнення та поширення. Такий підхід забезпечує методичну основу для поєднання інтелектуальних технологій із міжнародно визнаними практиками управління кіберризиками. Якщо на операційному рівні ШІ забезпечує підвищення швидкості виявлення інцидентів та адаптивність засобів захисту, то на стратегічному рівні його застосування має бути інтегроване у формалізовану модель оцінювання ризиків, що враховує специфіку функціонування об'єктів критичної інфраструктури та суб'єктів авіаційної діяльності. Саме в межах ризик-орієнтованого підходу використання інтелектуальних алгоритмів набуває системного характеру, перетворюючись із інструменту детекції на інструмент підтримки управлінських рішень.

Управління кібербезпекою об'єктів критичної інфраструктури доцільно розглядати як безперервний ризик-орієнтований цикл, у якому вибір превентивних і реактивних заходів ґрунтується на формалізованій оцінці загроз, вразливостей, ймовірності їх реалізації та можливих наслідків для критичних сервісів. Методично це узгоджується з міжнародними підходами до оцінювання ризику, які передбачають ідентифікацію джерел загроз і умов уразливості, визначення ймовірності та масштабу впливу, а також підтримання актуальності оцінок у часі. Штучний інтелект надає інструментальну основу для кількісного оцінювання таких ризиків, оскільки дозволяє перетворювати дані

центрів моніторингу безпеки, інформацію про уразливості та результати кіберрозвідки на динамічні параметри аналітичних моделей.

Поєднання стандартизованих характеристик уразливостей із оцінками ймовірності їх експлуатації та критичності активів формує кількісний базис для пріоритизації заходів захисту. Для моделювання процесів виявлення та можливого поширення атак застосовуються ймовірнісні та стохастичні моделі, тоді як оцінювання можливих збитків і невизначеності може здійснюватися із використанням сценарного аналізу та статистичного моделювання. Отримані результати оцінювання мають бути прозорими, обґрунтованими та такими, що підлягають подальшому відстеженню, із їх інтеграцією до загального реєстру ризиків організації та узагальненням на рівні системи корпоративного управління ризиками. Водночас забезпечення достовірності прогнозних оцінок потребує перевірки відповідності модельних прогнозів реальним подіям і постійного контролю змін у вхідних даних, що можуть впливати на точність роботи інтелектуальних систем у динамічному кіберсередовищі.

Постановка проблеми. У сучасному цифровому середовищі спостерігається стійке зростання кількості та складності кіберзагроз, що створює ризики для безпеки інформаційних систем, мереж і даних. Особливу небезпеку становлять автоматизовані атаки, які використовують сучасні алгоритмічні підходи для обходу традиційних механізмів захисту. За таких умов класичні методи виявлення та протидії кібератакам виявляються недостатньо результативними, оскільки не забезпечують своєчасного реагування на нові й раніше невідомі загрози. Це зумовлює потребу у впровадженні інтелектуалізованих підходів до забезпечення кібербезпеки, зокрема на основі технологій штучного інтелекту.

Аналіз останніх досліджень і публікацій. Проблематика застосування штучного інтелекту у сфері кібербезпеки активно досліджується як у вітчизняних, так і в зарубіжних наукових працях. Значна увага приділяється аналізу можливостей машинного навчання, великих даних та адаптивних алгоритмів у виявленні й нейтралізації кіберзагроз, а також ризикам і вразливостям ШІ-орієнтованих систем.

У роботі Скіцька О. та співавторів [1] комплексно розглянуто загрози та ризики використання штучного інтелекту, зокрема проблеми прозорості алгоритмів, етичні виклики та можливість зловживання ШІ з боку кіберзлочинців. Автори наголошують на необхідності поєднання інтелектуальних технологій із людським контролем, що узгоджується з підходами, запропонованими в даному дослідженні.

Нормативно-стратегічні аспекти розвитку штучного інтелекту в Україні визначені в Концепції розвитку штучного інтелекту, затвердженій Кабінетом Міністрів України [2]. Документ підкреслює важливість впровадження ШІ в критичні сфери, зокрема кібербезпеку, та акцентує увагу на необхідності забезпечення надійності й безпеки інтелектуальних систем.

Теоретичні основи використання алгоритмів машинного навчання в контексті великих даних детально висвітлено в роботі Терещенка В. М. та Бугаьова А. Д. [3]. Автори демонструють, що поєднання ML та Big Data дозволяє ефективно виявляти приховані закономірності й аномалії у великих масивах інформації, що є ключовим для сучасних систем кіберзахисту.

Питання вразливостей ШІ-систем, зокрема adversarial attacks та data poisoning, розглянуті в дослідженні Неретіна О. та Харченка В. [4]. Автори доводять, що навіть незначна маніпуляція вхідними або тренувальними даними може призводити до критичного зниження ефективності систем захисту, що підтверджує актуальність аналізу ризиків, проведеного у цій статті.

Практичні приклади застосування штучного інтелекту в кібербезпеці наведені в матеріалах FireEye щодо інциденту SolarWinds [5], які демонструють ефективність поведінкового аналізу та раннього виявлення складних атак. Водночас аналітичні огляди CyberWitcher [6] фіксують тенденцію до активного використання ШІ самими зловмисниками, що призводить до зростання кількості AI-асистованих атак та ускладнює їх детекцію.

Освітньо-аналітичні матеріали Cisco Networking Academy [7] підкреслюють важливість інтеграції ШІ в сучасні стратегії кіберзахисту, зокрема у сферах автоматизованого реагування на інциденти та мережевого моніторингу.

Аналітичні звіти міжнародних компаній і дослідницьких агенцій доповнюють наукові підходи актуальними статистичними даними. За оцінками MarketsandMarkets [8], світовий ринок AI у кібербезпеці демонструє стійке експоненційне зростання у 2023-2028 роках. Дані Statista та Total Assure [9, 10] підтверджують стрімке збільшення кількості AI-асистованих атак, зокрема фішингових кампаній.

Практичну ефективність ШІ-рішень демонструють кейси компаній Darktrace, SentinelOne та Vectra AI [11, 12, 14], які підтверджують зниження часу реагування, підвищення точності виявлення загроз і скорочення кількості хибних спрацювань. Разом із тим, звіт IBM Security [13] наголошує на зростанні ризиків adversarial machine learning, що потребує комплексного підходу до захисту інтелектуальних систем.

Таким чином, аналіз наукових публікацій, нормативних документів і аналітичних звітів свідчить про високий потенціал штучного інтелекту в кібербезпеці за умови врахування його вразливостей і ризиків. Це обґрунтовує доцільність подальших досліджень, спрямованих на розроблення адаптивних та безпечних ШІ-орієнтованих систем захисту, що і є предметом даної роботи.

У межах цього дослідження методологія системного аналізу була використана для комплексного оцінювання ринку кібербезпеки в поєднанні з порівняльним вивченням функціональних архітектур адаптивного захисту. Перспективні оцінки на 2025-2026 рр. отримані на основі екстраполяції масивів даних міжнародних аналітичних агенцій. Достовірність викладених положень верифіковано за допомогою аналізу емпіричного досвіду подолання кіберінцидентів та експериментального моделювання вразливостей моделей машинного навчання до змагальних атак».

Мета статті. Метою статті є комплексний аналіз можливостей застосування технологій штучного інтелекту в системах кібербезпеки та ідентифікація основних викликів і ризиків їх практичного впровадження. Для досягнення поставленої мети визначено такі завдання: проаналізувати напрями використання ШІ для виявлення та нейтралізації кіберзагроз; окреслити ключові виклики та вразливості ШІ-орієнтованих систем; дослідити перспективи розвитку технологій ШІ у сфері кібербезпеки на 2025-2026 роки; розробити рекомендації щодо підвищення ефективності використання ШІ в системах кіберзахисту.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із перспективних рішень є впровадження штучного інтелекту, який дозволяє значно підвищити рівень автоматизації процесів виявлення атак, аналізу загроз та розробки активних стратегій захисту. Проте, разом із можливостями, застосування ШІ несе і нові виклики, включаючи питання прозорості алгоритмів, етичні аспекти, ризики зловживання технологією з боку кіберзлочинців, а також складнощі у її інтеграції в існуючі системи безпеки[1].

Зміни в середовищі кібератак – такі як зростання обсягів даних, підключення нових пристроїв до інтернету, перехід на хмарні технології та розвиток квантових обчислень – значно ускладнюють завдання забезпечення кібербезпеки. Усе це робить проблему захисту інформаційних систем все більш актуальною. Без застосування інтелектуальних технологій прогнозування та адаптивних систем нейтралізації атак буде важко встигати за новими викликами кіберпростору.

Крім того, в умовах динамічного розвитку кіберзагроз виникає необхідність у створенні гнучких, самонавчальних систем безпеки, здатних реагувати на нові типи атак, навіть якщо вони ще не були виявлені в ході навчання моделі. У цьому контексті ШІ може стати актуальним фактором для протидії кіберзагрозам[2].

ШІ здатний значно пришвидшити процес реагування на інциденти у сфері кібербезпеки. За допомогою алгоритмів автоматизації ШІ може самостійно блокувати дії, ізолювати зловмисні елементи з мережі або навіть проводити первинний аналіз інцидентів. Це дозволяє зменшити час реагування та забезпечити більшу ефективність.

ШІ дозволяє ефективно виявляти аномалії в мережевому трафіку, які можуть вказувати на кібератаки. Кіберзагрози генерують величезну кількість даних у вигляді журналів, мережевих пакетів, запитів до серверів тощо.

Аналіз великих даних дозволяє виявляти закономірності, кореляції та аномалії в цих масивах інформації[3].

Платформи аналізу великих даних, такі як Splunk або ElasticStack, використовують величезні обсяги даних для ідентифікації підозрілої поведінки в реальному часі. За допомогою аналізу попередніх даних про атаки можна визначити набір типових реакцій (шаблонів) які реалізуються у певній ситуації, які вказують на підготовку, або реалізацію загроз (наприклад, сканування портів перед атакою). Інструменти аналізу можуть інтегруватися з ThreatIntelligence платформами, щоб порівнювати активність мережі з відомими загрозами (чорні списки IP-адрес, шкідливі домени). Приклад застосування: компанії використовують Hadoop або ApacheSpark для обробки потокових даних у великих мережах. Наприклад, виявлення раптового сплеску трафіку на одному сервері може вказувати на DDoS-атаку.

Використання ML у кібербезпеці дозволяє:

- Виявлення несанкціонованого доступу.
- Виявлення фішингових атак.
- Ідентифікація шкідливого програмного забезпечення.

ML-алгоритми навчаються на нормальній поведінці користувачів і системи, дозволяючи розпізнавати незвичні, або підозрілі дії (наприклад, аномальна кількість запитів на сервер від одного IP-адреса). Завдяки обробці природної мови (NLP), ML-алгоритми аналізують електронні листи, URL-адреси та метадані для виявлення потенційно шкідливого вмісту. Наприклад, моделі можуть аналізувати текст електронних листів для виявлення ознак соціальної інженерії (емоційний тиск, прохання надати дані). ML моделі можуть класифікувати файли, процеси чи мережеву активність, як безпечні або шкідливі, використовуючи великі набори даних про раніше відомі атаки. Приклад застосування: системи, як-от Cylance або Darktrace, використовують машинне навчання для автоматизованого моніторингу та адаптації до нових загроз. Наприклад, якщо на сервер надходить новий тип шкідливого файлу, модель ML може розпізнати його поведінкові характеристики та заблокувати доступ.

Інтелектуальні системи здатні на основі аналізу даних передбачити можливість варіантів розвитку атаки, що дає можливість для активного реагування та запобігання кібератакам до їх фактичного здійснення. FireEye та SolarWinds у 2020 році FireEye

виявила аномальну поведінку, яка вказувала на скомпрометований програмний оновлення від SolarWinds. Хоча атака торкнулася багатьох організацій, її виявлення на ранньому етапі дало змогу зменшити масштаби збитків [5].

Поєднання технологій штучного інтелекту є логічним кроком для запобігання кібератакам. У багатьох випадках ці технології працюють разом:

1. Машинне навчання навчається на великих масивах даних (Big Data), щоб створювати моделі для прогнозування загроз.
2. Аналіз великих даних допомагає збирати та структурувати інформацію, яка використовується алгоритмами ML.
3. Виявлення аномалій служить для ідентифікації потенційних атак на основі відхилень від нормальної поведінки.

Наприклад, у захисті від фішингу ML моделі аналізують текст і метадані листів, Big Data використовується для аналізу великих обсягів таких повідомлень, а модулі Anomaly Detection виявляють незвичну поведінку у взаємодії з підозрілими сайтами.

Штучний інтелект суттєво розширює можливості сучасних систем кіберзахисту, зокрема в частині виявлення аномалій, автоматизованого реагування на інциденти та прогнозування потенційних атак. Використання алгоритмів машинного навчання дозволяє аналізувати мережевий трафік, поведінку користувачів і події в реальному часі, що значно скорочує час реагування на загрози.

Ефективність таких підходів підтверджується практичними прикладами впровадження. Зокрема, система Darktrace демонструє високі результати у виявленні аномалій у корпоративних мережах, а SentinelOne забезпечує автоматизований захист кінцевих пристроїв із суттєвим скороченням часу реагування на інциденти. Порівняльна характеристика основних систем виявлення аномалій на базі машинного навчання наведена в таблиці 1.

Таблиця 1

Порівняння систем виявлення аномалій на базі машинного навчання (2025-2026)

Система	Основні функції	Приклади застосування	Ефективність	Джерело
Darktrace	Виявлення аномалій, самонавчання	Фармацевтика, фінанси	Зниження помилкових спрацьовувань на 60%	[4]
SentinelOne	Захист ендпоінтів, автоматична відповідь	Корпоративні мережі	Скорочення часу реагування на 46%	[5]
Cylance	Виявлення шкідливого ПЗ	Промислові системи	Блокування до 99% загроз до активації	[6]
Vectra AI	Мережеве виявлення (NDR)	Охорона здоров'я	Точність виявлення до 95%	[7]

Зростаючий попит на подібні рішення підтверджується динамікою розвитку світового ринку AI у кібербезпеці. Як показано на рис. 1, у 2023-2026 роках спостерігається стійке експоненційне зростання обсягів цього ринку, що свідчить про зростаючу роль інтелектуальних систем захисту в сучасному кіберпросторі.

Дані, наведені в таблиці 1, демонструють ефективність сучасних систем кіберзахисту на базі машинного навчання, зокрема Darktrace, SentinelOne та Vectra AI, які забезпечують високу точність виявлення загроз і зниження кількості хибних спрацювань. Подальший розвиток і масштабування таких рішень безпосередньо корелює із загальносвітовими інвестиційними трендами у сфері штучного інтелекту.

Це підтверджується даними, наведеними на рис. 1, де спостерігається стійке експоненційне зростання ринку AI в кібербезпеці у 2023-2026 роках. Збільшення обсягів

ринку свідчить про зростаючий попит на адаптивні системи захисту, описані в таблиці 1, а також про їх практичну ефективність у реальних середовищах.

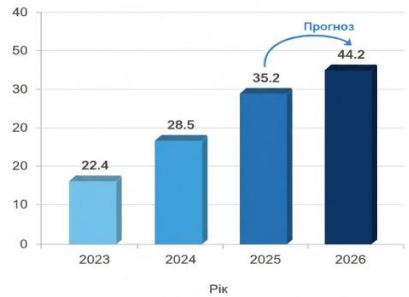

Рис. 1. Динаміка зростання світового ринку AI у сфері кібербезпеки у 2023-2026 рр., млрд дол. США.

Однак, ШІ-системи можуть мати власну вразливість [4]. Тенденції до використання штучного інтелекту для кіберзлочинів постійно розвиваються разом із вдосконаленням технологій. ШІ відкриває нові можливості для зловмисників, вони можуть маніпулювати даними, на основі яких відбувається навчання ШІ, що призводить до серйозних помилок у системах захисту [6].

Попри значні переваги, використання штучного інтелекту в кібербезпеці супроводжується низкою серйозних викликів. Однією з ключових проблем є вразливість моделей машинного навчання до adversarial attacks та атак типу data poisoning, які можуть призводити до суттєвого зниження точності виявлення загроз.

Додаткову загрозу становить активне використання штучного інтелекту самими зловмисниками. Як показано на рис. 2, у 2025 році кількість AI-асистованих кібератак зросла на 72% порівняно з 2024 роком. Особливо небезпечним є різке зростання AI-асистованого фішингу, динаміка якого наведена на рис. 3. У 2025 році рівень таких атак зріс більш ніж у 13 разів, що суттєво ускладнює їх виявлення традиційними методами.

Основні виклики та статистичні показники вразливостей ШІ в кібербезпеці узагальнено в таблиці 2. Аналіз наведених даних свідчить про необхідність комплексного підходу до захисту ШІ-моделей та постійного моніторингу їхньої надійності. Попри зростання ефективності AI-орієнтованих систем захисту, динаміка сучасних загроз демонструє зворотний тренд. Як показано на рис. 2, у 2025 році кількість AI-асистованих кібератак зросла на 72% порівняно з базовим рівнем 2024 року.

Таблиця 2

Основні виклики та вразливості застосування ШІ в кібербезпеці (2025–2026)

Виклик	Опис	Статистика	Потенційний вплив	Джерело
Adversarial attacks	Маніпуляція вхідними даними	Зниження точності на 22–27%	Пропуск загроз	[6]
Data poisoning	Отруєння тренувальних даних	0,001–3% даних → значне падіння точності	Довготривалі помилки моделей	[6]
AI-асистовані атаки	Використання ШІ зловмисниками	+72% атак у 2025 р.	Зростання успішності атак	[3]
AI-фішинг	Генеративні фішингові кампанії	+1265% у 2025 р.	Високий рівень компрометації	[3]
Agentic AI risks	Автономна непередбачувана поведінка	54% керівників вважають топ-ризиком	Масштабні інциденти	[7]

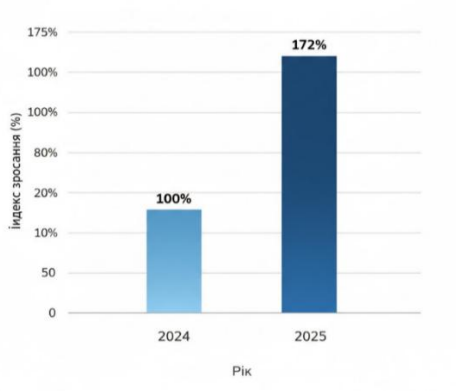

Рис. 2. Зростання кількості AI-асистованих кібератак у 2024-2025 рр.

Зазначене зростання безпосередньо пов'язане з викликами, наведеними в таблиці 2, зокрема з поширенням adversarial attacks та використанням ШІ зловмисниками. Таким чином, навіть за умов впровадження високоефективних систем захисту, кіберпростір залишається динамічним і вимагає постійного вдосконалення моделей безпеки.

Особливо критичним проявом зловживання штучним інтелектом є стрімке зростання AI-асистованого фішингу. Як видно з рис. 3, у 2025 році рівень таких атак зріс на 1265% порівняно з 2024 роком, що свідчить про кардинальну зміну характеру соціальної інженерії.

Ця тенденція корелює з даними таблиці 2, де AI-асистовані атаки визначені як один із ключових викликів кібербезпеки у 2025–2026 роках. Масштабне застосування генеративних моделей дозволяє зловмисникам створювати персоналізовані фішингові кампанії з високим рівнем правдоподібності, що значно підвищує їх успішність і знижує ефективність традиційних методів фільтрації.

Одним із найбільш критичних викликів 2025–2026 років стала зміна соціальної інженерії. Згідно з аналітичним звітом SlashNext "State of Phishing Report" [15], використання генеративного штучного інтелекту призвело до безпрецедентного сплеску AI-асистованого фішингу, рівень якого у 2025 році зріс на 1265% порівняно з базовим періодом 2024 року (див. Рис. 3). Таке зростання пояснюється здатністю великих мовних моделей генерувати персоналізовані повідомлення без граматичних помилок та з високим рівнем контекстуальної відповідності, що нівелює ефективність традиційних спам-фільтрів.

Паралельно з цим спостерігається інтенсифікація автоматизованих атак на мережеву інфраструктуру. За даними "IBM X-Force Threat Intelligence Index 2025" загальна кількість кібератак, де ШІ використовувався для автоматизації сканування вразливостей або адаптації шкідливого коду, зросла на 72%. Це підтверджує тезу про те, що зловмисники швидше адаптують інтелектуальні технології для масштабування своїх операцій [16].

Водночас розвиток технологій захисту демонструє оптимістичні прогнози. Відповідно до досліджень Gartner щодо стратегічних технологічних трендів до 2026 року рівень автоматизації в центрах операційного кіберзахисту (SOC) стрімко зростає. Очікується, що до кінця 2026 року до 80% рутинних завдань із детекції та первинного реагування на інциденти будуть виконуватися автономними агентами (Agentic AI). Це дозволить фахівцям зосередитися на стратегічному управлінні ризиками та розслідуванні складних цільових атак (APT) [17].

Динаміка інвестицій у цей сектор також залишається стабільною. За оцінками MarketsandMarkets світовий ринок AI у сфері кібербезпеки демонструє стійкий середньорічний темп зростання (CAGR) на рівні 22-26%, що підтверджує перехід організацій від реактивних до превентивних моделей захисту[8].

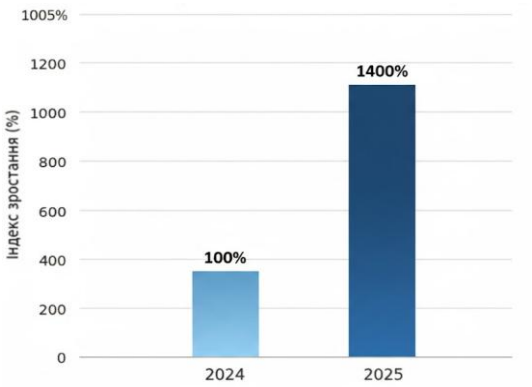

Рис. 3. Динаміка зростання AI-асистованого фішингу у 2024–2025 рр.

З огляду на зростання складності AI-асистованих атак та підвищення рівня автоматизації як засобів захисту, так і інструментів зловмисників, особливої ваги набуває системна оцінка ризиків поширення та своєчасного виявлення кіберзагроз у середовищах критичної інфраструктури та авіаційної галузі. Для таких об'єктів характерними є високий рівень взаємозалежності інформаційних, телекомунікаційних і технологічних систем, наявність сегментів операційних технологій (ОТ), а також жорсткі вимоги до безперервності функціонування. У цих умовах навіть локальний інцидент може мати каскадний характер, спричиняючи масштабні наслідки для безпеки польотів, енергозабезпечення, логістики або державного управління.

Застосування штучного інтелекту дозволяє перейти від фіксації факту інциденту до моделювання сценаріїв його можливого розвитку. Для оцінювання ризиків поширення атак доцільним є використання ймовірнісних моделей, зокрема байєсівських мереж та графів атак, які відображають можливі шляхи проникнення і горизонтального переміщення зловмисника в інфраструктурі. У таких моделях інтелектуальні алгоритми оновлюють ймовірності переходів між станами системи на основі поточної телеметрії центрів моніторингу безпеки. Для авіаційних інформаційних систем це може включати аналіз аномальної активності в сегментах управління польотними даними, сервісах бронювання або системах технічного обслуговування повітряних суден.

Оцінювання ймовірності реалізації вразливостей може базуватися на поєднанні стандартизованих технічних характеристик уразливостей із прогнозними моделями ймовірності їх експлуатації. Додатково для визначення можливого фінансового та операційного впливу інцидентів застосовуються сценарний аналіз і статистичне моделювання, зокрема методи Монте-Карло, що дозволяють врахувати невизначеність параметрів та отримати діапазон можливих збитків. У контексті критичної інфраструктури це створює підґрунтя для кількісного порівняння альтернативних стратегій захисту та обґрунтування інвестицій у засоби кібербезпеки.

Перевагою використання ШІ в оцінці ризиків є здатність інтегрувати різнорідні джерела даних, такі як мережеву телеметрію, журнали подій, дані про вразливості, результати кіберрозвідки - у єдину аналітичну модель, що забезпечує динамічне оновлення показників ризику в режимі реального часу. Для об'єктів КІ та авіаційних систем це дозволяє оперативно змінювати пріоритети реагування залежно від

критичності активів і поточної загрозової ситуації. Водночас обмеження пов'язані з можливістю викривлення результатів через некоректні або навмисно змінені дані, дрейф характеристик середовища функціонування та складність інтерпретації прогнозних оцінок. У разі помилкової калібрації моделей існує ризик недооцінки загроз, що в критичних системах може мати неприйнятні наслідки.

Узагальнюючи результати аналізу можливостей і викликів застосування штучного інтелекту в кібербезпеці, слід зазначити, що для авіаційної галузі та інших секторів критичної інфраструктури пріоритетним є впровадження гібридної моделі оцінювання ризиків, у межах якої інтелектуальні алгоритми здійснюють первинний аналіз, прогнозування розвитку інцидентів і моделювання сценаріїв поширення загроз, тоді як остаточні управлінські рішення приймаються з урахуванням експертної оцінки фахівців. Такий підхід забезпечує поєднання високої швидкості оброблення даних і здатності до адаптації з необхідним рівнем контролю, відповідальності та відповідності нормативним вимогам, що є критично важливим для систем із підвищеними вимогами до безпеки, безперервності функціонування та надійності.

Отже, наукова проблема інтеграції штучного інтелекту в системи кіберзахисту полягає не лише у розширенні функціональних можливостей детекції та реагування, а й у формуванні ефективних механізмів управління ризиками його застосування. Це передбачає комплексне поєднання технологічних інновацій, кількісних методів оцінювання ризиків поширення та виявлення кіберзагроз, організаційних процедур контролю й нормативного регулювання. Подальший розвиток інтелектуальних систем кіберзахисту, включаючи впровадження автономних агентів, має здійснюватися в логіці збалансованого підходу, де автоматизація процесів супроводжується забезпеченням прозорості моделей, їх підконтрольності та інтеграції результатів аналітики у загальну систему управління кіберризиками. Саме така синергія технологічних можливостей і системного ризик-орієнтованого управління визначає перспективний напрям еволюції сучасних стратегій кібербезпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведений аналіз наукових публікацій, нормативних документів та аналітичних звітів засвідчив, що сучасні дослідження переважно зосереджені або на прикладних аспектах використання штучного інтелекту в кібербезпеці, або на розгляді окремих вразливостей ШІ-систем. У межах даної роботи систематизовано взаємозв'язок між темпами впровадження інтелектуальних технологій захисту та динамікою AI-асистованих загроз у 2025-2026 роках, що дозволило виявити дисбаланс між швидкістю розвитку засобів оборони та еволюцією атак, зокрема у сфері генеративного фішингу. Наукова новизна полягає в уточненні класифікації викликів застосування ШІ шляхом виокремлення ризиків автономних («агентних») систем, поведінка яких може бути складною для прогнозування та контролю.

Узагальнення сучасних підходів показало, що машинне навчання, аналіз великих даних та автоматизоване виявлення аномалій формують основу адаптивних систем кіберзахисту, здатних підвищувати точність детекції та скорочувати час реагування. Водночас розширення застосування ШІ обумовлює необхідність системної оцінки ризиків його використання, зокрема в середовищах критичної інфраструктури та авіаційної галузі, де наслідки помилок або маніпуляцій можуть мати масштабний характер. Інтеграція інтелектуальних моделей у процеси управління ризиками має

супроводжуватися контролем якості даних, моніторингом стабільності моделей та формалізованим урахуванням невизначеності під час прийняття рішень.

Штучний інтелект слід розглядати як потужний інструмент підвищення ефективності сучасних стратегій кіберзахисту за умови його впровадження в межах гібридної моделі, що поєднує автоматизовану аналітику з експертним наглядом людини. Саме збалансоване поєднання технологічних можливостей, кількісної оцінки ризиків та системного управління безпекою забезпечує цілісність і стійкість ШІ-орієнтованих систем у динамічному кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M., & Vorokhob, M. (2023). Threats and risks of artificial intelligence use. *Cybersecurity: Education, Science, Technique, 2*(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
2. Cabinet of Ministers of Ukraine. (2020). *Concept of artificial intelligence development in Ukraine* (Order No. 1556-r, December 2, 2020). https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
3. V. M., & Bugaiov, A. D. (2018). Machine learning algorithms in the context of big data. *Artificial Intelligence, (3).*
4. Neretin, O., & Kharchenko, V. (2022). Cybersecurity of artificial intelligence systems: Analysis of vulnerabilities, attacks, and countermeasures. *Information Systems and Networks, (12).*
5. SOFTPROM. (2021, January 26). *FireEye CEO explains how the company detected a cyberattack.* https://softprom.com/ru/generalnyiy-direktor-fireeye-rasskazyivaet-o-tom-kak-kompaniya-obnarujila-kiberataku
6. CyberWitcher. (n.d.). *Trends in the use of AI for cybercrime.* https://hackyourmom.com/kibervijna/tendencziyi-u-vykorystanni-ai-dlya-kiberzlochyniv/
7. Education.ua. (2024). *Artificial intelligence and cybersecurity.* https://www.education.ua/blog/48113/
8. MarketsandMarkets. (2025–2028). *AI in cybersecurity market.* https://www.marketsandmarkets.com
9. Statista. (2025). *Artificial intelligence and cybersecurity statistics.* https://www.statista.com
10. Total Assure. (2026). *AI cybersecurity statistics in 2025.* https://www.totalassure.com
11. Darktrace. (2025). *AI and cyber defense case studies.* https://www.darktrace.com
12. SentinelOne. (2025). *Autonomous endpoint protection report.* https://www.sentinelone.com
13. IBM Security. (2025). *Adversarial machine learning risks.* https://www.ibm.com/security
14. Vectra AI. (2026). *Network detection and response report.* https://www.vectra.ai
15. SlashNext. (2024–2025). *State of phishing report 2024–2025.* https://slashnext.com/state-of-phishing-report/
16. IBM. (2025). *IBM X-Force threat intelligence index 2025.* https://www.ibm.com/reports/threat-intelligence
17. Gartner. (2025, October 20). *Gartner identifies the top strategic technology trends for 2026* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2025-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2026
18. Ilienko, A., Ilienko, S., Yakovenko, O., Halych, Y., & Pavlenko, V. (2024). Prospects for integration of artificial intelligence into cybersecurity systems. *Cybersecurity: Education, Science, Technique, 1*(25), 318–329. https://doi.org/10.28925/2663-4023.2024.25.318329

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Anna Ilienko
Candidate of Technical Sciences, Associate Professor, Head of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0001-8565-1117
anna.ilienko@npp. kai.edu.ua

Olha Kryvokulska
Senior Lecturer of the Cybersecurity Department
State University "Kyiv Aviation Institute",Kyiv, Ukraine
ORCID: 0009-0003-8518-6915
olha.kryvokulska@npp.kai.edu.ua

Olesia Yakovenko
Senior Lecturer of the Cybersecurity Department
State University "Kyiv Aviation Institute",Kyiv, Ukraine
ORCID: 0000-0003-2998-9767
olesia.yakovenko@npp.kai.edu.ua

Valentyna Teliushchenko
Assistant of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0001-6026-5105
valentyna.teliushchenko@npp. kai.edu.ua

INTELLIGENT TECHNOLOGIES IN CYBERSECURITY: ANALYSIS OF THE POTENTIAL AND CHALLENGES OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE

Abstract. The article provides a systematic analysis of the opportunities and challenges of applying artificial intelligence (AI) in the field of cybersecurity. The feasibility of integrating AI technologies into modern cyber defense strategies in the face of increasing complexity and intensity of cyber threats is substantiated. The main areas of AI use are identified, in particular, the automation of anomaly detection, forecasting cyber threats, accelerating incident response, and the formation of adaptive protection systems. Practical cases of implementing AI solutions are analyzed, which confirm the increase in the accuracy of threat detection and reduction of response time. Special attention is paid to the risks and vulnerabilities of AI-oriented systems, in particular, threats such as adversarial attacks and data poisoning, as well as the use of AI by attackers to implement AI-assisted attacks. The prospects for the development of AI technologies in 2025-2026 are considered, including the introduction of autonomous intelligent agents (agentic AI) in operational cyber defense centers. It is shown that the transition to autonomous protection models requires increased control, the use of hybrid approaches (AI combined with human expert supervision) and the improvement of regulatory and ethical mechanisms. The results of the study allow us to form a comprehensive vision of the evolution of AI-oriented cyber defense systems and justify the need for a balanced combination of technological capabilities and risk management.

Keywords: artificial intelligence, cyber security, attacks, machine learning, anomaly detection, cyber threat prediction, self-learning algorithms, adaptive defense systems, cyber defense, AI abuse, cyber threats.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M., & Vorokhob, M. (2023). Threats and risks of artificial intelligence use. *Cybersecurity: Education, Science, Technique, 2*(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
2. Cabinet of Ministers of Ukraine. (2020). *Concept of artificial intelligence development in Ukraine* (Order No. 1556-r, December 2, 2020). https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

3. V. M., & Bugaiov, A. D. (2018). Machine learning algorithms in the context of big data. *Artificial Intelligence, (3).*
4. Neretin, O., & Kharchenko, V. (2022). Cybersecurity of artificial intelligence systems: Analysis of vulnerabilities, attacks, and countermeasures. *Information Systems and Networks, (12).*
5. SOFTPROM. (2021, January 26). *FireEye CEO explains how the company detected a cyberattack.* https://softprom.com/ru/generalnyiy-direktor-fireeye-rasskazyivaet-o-tom-kak-kompaniya-obnarujila-kiberataku
6. CyberWitcher. (n.d.). *Trends in the use of AI for cybercrime.* https://hackyourmom.com/kibervijna/tendencziyi-u-vykorystanni-ai-dlya-kiberzlochyniv/
7. Education.ua. (2024). *Artificial intelligence and cybersecurity.* https://www.education.ua/blog/48113/
8. MarketsandMarkets. (2025–2028). *AI in cybersecurity market.* https://www.marketsandmarkets.com
9. Statista. (2025). *Artificial intelligence and cybersecurity statistics.* https://www.statista.com
10. Total Assure. (2026). *AI cybersecurity statistics in 2025.* https://www.totalassure.com
11. Darktrace. (2025). *AI and cyber defense case studies.* https://www.darktrace.com
12. SentinelOne. (2025). *Autonomous endpoint protection report.* https://www.sentinelone.com
13. IBM Security. (2025). *Adversarial machine learning risks.* https://www.ibm.com/security
14. Vectra AI. (2026). *Network detection and response report.* https://www.vectra.ai
15. SlashNext. (2024–2025). *State of phishing report 2024–2025.* https://slashnext.com/state-of-phishing-report/
16. IBM. (2025). *IBM X-Force threat intelligence index 2025*. https://www.ibm.com/reports/threat-intelligence
17. Gartner. (2025, October 20). *Gartner identifies the top strategic technology trends for 2026* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2025-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2026
18. Ilienko, A., Ilienko, S., Yakovenko, O., Halych, Y., & Pavlenko, V. (2024). Prospects for integration of artificial intelligence into cybersecurity systems. *Cybersecurity: Education, Science, Technique, 1*(25), 318–329. https://doi.org/10.28925/2663-4023.2024.25.318329

Отримано редакцією журналу / Received: 22.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26