КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.379389
УДК 004.056.55:004.8

Лунгол Ольга Миколаївна
кандидат педагогічних наук, доцент,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Донецький державний університет внутрішніх справ, Кропивницький, Україна
ORCID ID: 0000-0001-8128-0072
olyalungol@gmail.com

ОГЛЯД МЕТОДІВ ТА СТРАТЕГІЙ КІБЕРБЕЗПЕКИ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. У сучасному світі інформаційні технології стрімко розвиваються, що призводить до зростання кількості та складності кіберзагроз, зокрема фішингу, шкідливого програмного забезпечення та атак з використанням соціальної інженерії. Зростання кількості та складності кіберзагроз створює нагальну потребу у вдосконаленні методів захисту інформаційних систем. Штучний інтелект (ШІ), особливо технології машинного навчання та глибокого навчання, демонструють значний потенціал у підвищенні рівня кібербезпеки. Ця стаття присвячена огляду сучасних методів та стратегій кібербезпеки, що базуються на застосуванні ШІ, а також оцінці їх ефективності у виявленні та протидії кіберзагрозам. Проаналізовано останні дослідження як вітчизняних, так і закордонних науковців, які акцентують увагу на здатності ШІ аналізувати великі обсяги даних, виявляти приховані закономірності, прогнозувати потенційні загрози та автоматизувати процеси реагування на інциденти. Висвітлено ключові напрямки досліджень, включаючи виявлення аномалій, моделювання загроз, автоматизацію процесів реагування на інциденти та забезпечення розуміння рішень, прийнятих системами ШІ. Особлива увага приділяється інтеграції ШІ в існуючі системи кібербезпеки та його здатності до адаптації у відповідь на нові загрози. Стаття також обговорює основні виклики та перспективи застосування ШІ у кібербезпеці, включаючи етичні та правові аспекти, такі як питання приватності, прозорості рішень та відповідальності за дії, здійснені на основі рішень ШІ-систем. Останні статистичні дані свідчать про стрімке зростання ринку засобів ШІ для забезпечення кібербезпеки, що підкреслює важливість і актуальність цієї теми у сучасних умовах. Результати аналізу підтверджують, що використання ШІ дозволяє автоматизувати процеси моніторингу, виявлення та реагування на загрози, що зменшує час реакції на інциденти та підвищує загальний рівень захисту інформаційних систем. Разом з тим, впровадження ШІ у кібербезпеку стикається з низкою викликів, таких як забезпечення прозорості рішень, прийнятих ШІ, а також захист від потенційних загроз, створених з використанням тих самих технологій. Дослідження цієї теми сприяє стратегічному розвитку та інноваціям у сфері кібербезпеки, надаючи дослідникам та фахівцям нові інструменти та методи для забезпечення безпеки інформаційних систем. Отже, з огляду на швидке зростання та еволюцію кіберзагроз, дослідження ролі ШІ в кібербезпеці є надзвичайно актуальним та важливим. Це дозволяє не тільки підвищити ефективність захисту, але й сприяє розвитку нових стратегій та технологій для протидії загрозам у цифрову епоху.

Ключові слова: штучний інтелект; кібербезпека; загрози; інформаційний простір.

ВСТУП

У сучасному світі інформаційні технології стрімко розвиваються, що призводить до зростання кількості та складності кіберзагроз. Це зумовлює необхідність вдосконалення методів захисту інформації. Останні роки характеризуються значним збільшенням кількості кіберзагроз, таких як фішинг, шкідливе програмне забезпечення та атаки з використанням соціальної інженерії. Кіберзлочинці застосовують дедалі

витонченіші методи, що вимагає впровадження нових технологій для ефективного захисту інформації.

Штучний інтелект (ШІ) став потужним інструментом для підвищення рівня кібербезпеки та планування і здійснення кібератак. Технології ШІ, зокрема машинне навчання та глибоке навчання, значно просунулися вперед і знайшли широке застосування у різних сферах, включаючи кібербезпеку. Здатність ШІ до аналізу великих обсягів даних та виявлення прихованих закономірностей робить його незамінним у боротьбі з кіберзагрозами.

Постановка проблеми. Збільшення кількості та складності кіберзагроз у сучасному світі створює нагальну потребу у вдосконаленні методів захисту інформації. Сучасні кіберзлочинці застосовують все більш складні та витончені методи, що викликає необхідність впровадження нових технологій для ефективного захисту інформаційних систем. У зв'язку з цим, виникає потреба у дослідженні можливостей використання ШІ для підвищення кібербезпеки.

Дослідження методів та стратегій кібербезпеки з використанням ШІ є актуальним та важливим напрямом у сучасних умовах зростання кількості кіберзагроз. Застосування технологій ШІ дозволяє значно підвищити ефективність захисту інформації, забезпечуючи швидке виявлення та протидію кіберзагрозам. Наукові дослідження у цій галузі є необхідними для розробки нових, більш ефективних методів захисту, що відповідатимуть сучасним викликам у сфері кібербезпеки.

Аналіз останніх досліджень і публікацій. На актуальність дослідження місця ШІ у кібербезпеці вказує низка наукових робіт як вітчизняних, так і зарубіжних науковців. Так, Магденко А. Р. [1], Бучацький І. О. [1] та Бондаренко І. О. [1] у своїх дослідженнях зазначають, що завдяки здатності аналізувати великі обсяги даних, виявляти вразливості в системах безпеки та прогнозувати потенційні кіберзагрози, ШІ стає ключовим інструментом у боротьбі із кіберзагрозами та захисті від кібератак. Вони також зазначають, що сучасні хакери та шахраї активно використовують ШІ для вдосконалення своїх атак, збільшуючи їх швидкість, масштаб та складність.

Товстуха Н. [2] вказує, що наразі близько 50% підприємств вже використовують комбінацію ШІ та інструментів машинного навчання, а понад 90% організацій планують запровадити такі інструменти у майбутньому. Устименко В. [3] та Олішевський І. [3] наводять статистичні дані, згідно з якими, за оцінкою MarketsandMarkets, ринок засобів ШІ для забезпечення кібербезпеки буде зростати на 23,3% щороку в період з 2019 до 2026 року, збільшуючись з 8,8 млрд до 38,2 млрд доларів США.

Каун Ю. [4] та Собчук О. [4] наводять результати дослідження вчених Університету Індіани, які виявили понад 200 вкрадених і зламаних відкритих мовних моделей, що пропонуються для хакерської діяльності. Це свідчать про зростаючу тенденцію використання ШІ для зловмисних цілей. Зокрема, створення дипфейків на основі цілком реалістичних та оманливих відео, які можуть мати значний вплив на громадську думку та хід подій. Зневажливі відео, підроблені документи та фейкові акаунти в соціальних мережах можуть бути використані для маніпулювання громадськістю, підриву довіри до інституцій та розпалювання соціальних заворушень.

Старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України Гуржій С. [5] зазначає, що алгоритм роботи системи захисту від кіберзагроз з використанням ШІ повинен працювати автономно та виконувати наступні дії: перевіряти мережі на наявність вразливостей з високою точністю; виявляти нові загрози в режимі реального часу; з високою ефективністю реалізовувати індивідуальні заходи з пом'якшення

наслідків, такі як автоматичне виправлення програмного забезпечення або блокування шкідливих IP-адрес.

Метою статті є огляд сучасних наукових досліджень вітчизняних й закордонних науковців щодо методів та стратегій кібербезпеки, що базуються на застосуванні ШІ, а також оцінка їх ефективності у виявленні та протидії кіберзагрозам.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Вітчизняні науковці Котенко Д. [6] та Хлапонін Ю. [6] виділяють ключову перевагу використання ШІ в кібербезпеці — це його здатність аналізувати великі обсяги даних для виявлення патернів та аномалій, які можуть свідчити про кіберзагрози. Ця здатність стає все більш важливою, оскільки обсяг даних, які генеруються та збираються, постійно зростає. Люди аналітики просто не в змозі впоратися з таким обсягом даних самостійно, тому ШІ є незамінним інструментом для виявлення кіберзагроз [6]. Здатність до аналізу великих обсягів даних для виявлення патернів та аномалій за допомогою ШІ в кібербезпеці можливо реалізувати за допомогою різноманітних засобів, включаючи: методи машинного навчання, аналіз поведінки користувачів, системи виявлення вторгнень (IDS), аналіз журналів подій (SIEM), технології Big Data. Систематизовану інформацію щодо перелічених методів представлено у табл. 1. [6] – [12].

Таблиця 1

Методи для аналізу великих обсягів даних у кібербезпеці за допомогою ШІ

Назва методу	Зміст методу	Характеристика	Зміст характеристики
Методи машинного навчання	Відіграє критичну роль у кібербезпеці, дозволяючи автоматизовано аналізувати великі обсяги даних та виявляти закономірності й аномалії, що можуть свідчити про кібератаки.	«Супервізоване» або «кероване» навчання (англ. Supervised Learning)	Використовується для класифікації даних, де система навчається на маркованих даних (наприклад, нормальні та аномальні дії) і потім застосовує цей досвід для нових даних. Приклади алгоритмів: логістична регресія, дерева рішень, SVM (Support Vector Machines).
		«Ненаглядне» або «некероване» навчання (англ. Unsupervised Learning)	Використовується для виявлення невідомих патернів у даних без попереднього маркування. Приклади алгоритмів: кластеризація (k-means, DBSCAN), алгоритми зниження розмірності (PCA, t-SNE).
		Глибоке навчання (англ. Deep Learning)	Включає використання нейронних мереж для складних завдань, таких як розпізнавання зображень або обробка природної мови. Рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN) є популярними методами для аналізу послідовних даних та зображень відповідно.

Аналіз поведінки користувачів (UBA)	User Behavior Analytics (UBA) використовує ШІ та ML (Machine Learning) для моніторингу та аналізу поведінки користувачів у реальному часі з метою виявлення аномалій, які можуть свідчити про внутрішні загрози або компрометацію облікових записів.	**Моніторинг дій**	Збирає дані про дії користувачів, включаючи логін, доступ до файлів, використання мережевих ресурсів та інші операції.
		Виявлення аномалій	Використовує моделі ML для порівняння поточної поведінки з історичними даними та виявлення відхилень, які можуть бути ознаками загрози.
		Адаптивність	Системи UBA можуть адаптуватися до змін у поведінці користувачів, забезпечуючи постійне оновлення моделей для більш точного виявлення загроз.
Системи виявлення вторгнень (IDS)	Intrusion Detection Systems (IDS) використовують ШІ для аналізу мережевого трафіку та виявлення підозрілих дій, які можуть свідчити про вторгнення.	**Мережеві IDS (NIDS)**	Моніторять мережевий трафік і аналізують пакети даних для виявлення аномалій. Застосовуються методи сигнатурного та евристичного аналізу.
		Хостові IDS (HIDS)	Моніторять активність на окремих пристроях, такі як журнали подій, цілісність файлів, системні виклики, для виявлення вторгнень.
		Гібридні системи	Комбінують NIDS та HIDS для більш комплексного підходу до виявлення загроз.
Аналіз журналів подій (SIEM)	Security Information and Event Management (SIEM) системи об'єднують та аналізують журнали подій з різних джерел для виявлення загроз і забезпечення відповідності вимогам безпеки.	Централізоване збирання даних	Збирають дані з мережевих пристроїв, серверів, додатків та інших джерел.
		Кореляція подій	Використовують алгоритми для кореляції подій з різних джерел, що дозволяє виявити складні атаки, які можуть бути непомітні при аналізі окремих подій.
		Робота в режимі реального часу	Забезпечують моніторинг у реальному часі та автоматичне реагування на виявлені загрози.
Технології Big Data	Технології Big Data дозволяють обробляти та аналізувати великі обсяги даних з високою швидкістю, що є критичним для виявлення та реагування на кіберзагрози.	Розподілена обробка	Використання платформ, таких як Hadoop та Apache Spark, для обробки великих обсягів даних у розподіленому середовищі.
		Аналіз у реальному часі	Використання технологій потокової обробки, таких як Apache Kafka, для аналізу даних у реальному часі.
		Інтеграція даних	Здатність інтегрувати дані з різних джерел, включаючи мережевий трафік, журнали подій, соціальні мережі та інші джерела.

Кожен із описаних методів має свої переваги та особливості, що робить їх важливими інструментами в арсеналі засобів кібербезпеки. Використання ШІ та машинного навчання дозволяє суттєво покращити виявлення загроз і реагування на них, забезпечуючи більш ефективний захист інформаційних систем у сучасному світі.

Серед закордонних досліджень за темою статті виділяємо роботи Саркер І. [13], Фурхад М. [13], Новрози Р. [13], Камачо Н. [14], Кузлу М. [15], Фэйр Ч. [15], Гюлер О. [15], Гупта М. [16], Акири К. [16], Арьял К. [16], Паркер Е. [16], Прахарадж Л. [16], Ясін А. [17], Мохамед Н. [18], Капуано Н. [19], Фенза Г. [19], Лоя В. [19], Станзіоне К. [19], Адевусі А. [20], Околі У. [20], Олорунсого Т. [20], Адага Е. [20], Дараоджимба Д. [20], Обі О. [20] та ін.

Перелічені роботи підкреслюють значний потенціал ШІ у підвищенні ефективності кібербезпеки. Основними напрямками досліджень є виявлення аномалій, моделювання загроз, автоматизація процесів реагування на інциденти та забезпечення розуміння рішень, прийнятих системами ШІ. Науковці акцентують увагу на важливості інтеграції ШІ в існуючі системи кібербезпеки для адаптації до наявних та нових загроз. Так, дослідження Саркера І. [13], Фурхада М. [13] та Новрози Р. [13] містять огляд застосування ШІ у кібербезпеці, акцентуючи увагу на моделюванні безпеки та можливих напрямках досліджень. Автори досліджують різні підходи до використання ШІ для підвищення ефективності кібербезпеки, аналізують поточні технології. Основні акценти зроблено на моделюванні загроз, виявленні аномалій та реагуванні на інциденти безпеки.

Камачо Н. [14] досліджує роль ШІ в сучасній кібербезпеці, зосереджуючи увагу на реагуванні на загрози у цифрову епоху. Автор детально аналізує, як технології ШІ можуть допомогти виявляти та протидіяти новим кіберзагрозам, обговорює переваги та виклики впровадження ШІ в системи кібербезпеки. Особлива увага приділяється інтеграції ШІ в існуючі системи та його здатності до адаптації у відповідь на нові загрози.

Кузлу М. [15], Фэйр Ч. [15] та Гюлер О. [15] демонструють результати дослідження ролі ШІ у забезпеченні кібербезпеки в контексті Інтернету речей (IoT). Вони розглядають специфічні виклики, пов’язані з безпекою IoT, і те, як ШІ може бути використаний для їх вирішення. Основні акценти зроблено на методах виявлення аномалій, прогнозуванні загроз та забезпеченні цілісності даних у мережах IoT.

Досить популярним за рівнем цитування у науковій спільності є колективне дослідження Гупти М., Акири К., Арьял К., Паркери Е. та Прахарадж Л. [16], які аналізують вплив генеративного ШІ, такого як ChatGPT, на кібербезпеку та приватність. Автори досліджують, як генеративні моделі можуть бути використані як для захисту, так і для здійснення кібератак. Вони обговорюють потенційні загрози та можливості, які надають ці технології, а також розглядають етичні аспекти та питання приватності.

Коло наукових інтересів Ясін А. [17] також пов’язане із парадигмальною зміною у кібербезпеці, спричиненою впровадженням ШІ для виявлення загроз та реагування на них. Науковець акцентує увагу на нових методах виявлення загроз, які базуються на машинному навчанні, та їхній здатності швидко адаптуватися до нових загроз. Автор роботи також розглядає питання автоматизації процесів реагування на інциденти.

Найновіші методи та підходи, які використовуються у сфері ШІ та ML для кібербезпеки, відображені у дослідженнях Мохамед Н. [18]. Науковець оцінює їхню ефективність і обмеження, а також робить акцент на міждисциплінарному підході та інтеграції різних технологій для покращення систем кібербезпеки.

Адевусі А., Околі У., Олорунсого Т., Адага Е., Дараоджимба Д. та Обі О. [20] досліджують специфічні виклики, пов’язані з захистом критичної інфраструктури, такі як енергетичні системи, транспорт та комунікації, і те, як ШІ може допомогти у

вирішенні цих питань. Вони розглядають конкретні приклади успішного впровадження ШІ та пропонують рекомендації для подальшого розвитку цієї галузі.

Отже, дослідження за темою статті є надзвичайно важливим з кількох ключових причин:

1. Зростання складності та обсягу кіберзагроз, оскільки з кожним роком кіберзагрози стають дедалі складнішими і частішими. Традиційні методи захисту вже не можуть ефективно протистояти новим, складним атакам. Штучний інтелект та машинне навчання здатні аналізувати великі обсяги даних, виявляти складні закономірності та адаптуватися до нових загроз швидше, ніж будь-які інші методи;

2. Застосування ШІ дозволяє автоматизувати багато аспектів кібербезпеки, від виявлення загроз до реагування на інциденти. Це значно підвищує ефективність та швидкість реагування, зменшуючи навантаження на людські ресурси та знижуючи ризик людських помилок;

3. Покращення точності та швидкості виявлення за рахунок аналізу аномальної поведінки в режимі реального часу. Це дозволяє зменшити кількість хибних спрацьовувань та підвищити загальний рівень безпеки;

4. ШІ-системи можуть постійно навчатися та адаптуватися до нових загроз, що дозволяє їм залишатися актуальними та ефективними навіть у швидкозмінному середовищі кібербезпеки;

5. Інтеграція ШІ з іншими сучасними технологіями, такими як IoT та Big Data, створює нові можливості для покращення кібербезпеки. Інтеграція дозволяє здійснювати більш детальний аналіз даних та розробляти комплексні захисні стратегії.

Дослідження за темою «Огляд методів та стратегій кібербезпеки засобами штучного інтелекту» також охоплює важливі етичні та правові аспекти, пов’язані з використанням ШІ в кібербезпеці: питання приватності, прозорості рішень та відповідальності за дії, здійснені на основі рішень ШІ-систем. Також, дослідження цієї теми сприятиме стратегічному розвитку та інноваціям у сфері кібербезпеки, надаючи дослідникам та фахівцям нові інструменти та методи для забезпечення безпеки інформаційних систем.

Отже, з огляду на швидке зростання та еволюцію кіберзагроз, дослідження ролі ШІ в кібербезпеці є надзвичайно актуальним та важливим. Це дозволяє не тільки підвищити ефективність захисту, але й сприяє розвитку нових стратегій та технологій для протидії загрозам у цифрову епоху. Останні статистичні дані свідчать про стрімке зростання ринку засобів ШІ для забезпечення кібербезпеки. Згідно з оцінками MarketsandMarkets [21], обсяг цього ринку з 2019 до 2026 року зростає на 23,3% щороку, збільшуючись з 8,8 млрд до 38,2 млрд доларів США. Цей ріст відображає збільшення інтересу до ШІ як інструменту для підвищення ефективності захисту інформаційних систем.

У звіті IBM X-Force Threat Intelligence Index [22] за 2023 рік зазначено, що 30% всіх кіберінцидентів пов’язані з використанням технологій штучного інтелекту та машинного навчання. IBM також повідомляє, що компанії, які використовують ШІ для забезпечення кібербезпеки, змогли скоротити час виявлення та реагування на інциденти на 27%.

За даними Gartner [23], до 2025 року 60% організацій будуть активно використовувати технології ШІ для виявлення та реагування на кіберзагрози. Gartner також зазначає, що компанії, які впроваджують ШІ у свої стратегії кібербезпеки, демонструють значне підвищення ефективності та точності виявлення загроз.

Statista [24] повідомляє, що у 2022 році обсяг інвестицій у технології ШІ для кібербезпеки становив близько 12,5 млрд доларів США. Очікується, що до 2025 року ці

інвестиції зростуть до 25 млрд доларів США. Цей ріст свідчить про важливість та актуальність технологій ШІ у сфері кібербезпеки.

Національний інститут стандартів і технологій США (NIST) [25] активно досліджує застосування ШІ у кібербезпеці. Вони публікують рекомендації та стандарти, які допомагають організаціям впроваджувати ефективні стратегії захисту з використанням технологій ШІ. NIST підкреслює важливість інтеграції ШІ у системи виявлення та реагування на загрози для підвищення загального рівня безпеки.

Отже, аналіз статистичних даних з різних офіційних джерел свідчить про значний потенціал та необхідність впровадження технологій ШІ у сферу кібербезпеки. ШІ дозволяє автоматизувати процеси моніторингу, виявлення та реагування на загрози, що зменшує час реакції на інциденти та підвищує загальний рівень захисту інформаційних систем. Інвестиції у технології ШІ для кібербезпеки продовжують зростати, що підкреслює важливість цих технологій у боротьбі з кіберзагрозами. Аналіз показує, що сучасні методи ШІ, такі як машинне навчання, глибоке навчання та аналіз великих даних, активно впроваджуються у системи кібербезпеки для автоматизації процесів моніторингу та реагування на загрози. Це дозволяє значно скоротити час реакції на інциденти та підвищити загальний рівень безпеки. Однак, незважаючи на значні досягнення, використання ШІ у кібербезпеці стикається з низкою викликів. Серед них — необхідність забезпечення прозорості рішень, прийнятих ШІ, а також захист від потенційних загроз, які можуть бути створені з використанням тих самих технологій ШІ. Наприклад, генеративні моделі, такі як GPT-3, можуть бути використані для створення більш складних фішингових атак або дезінформаційних кампаній.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження методів та стратегій кібербезпеки із застосуванням ШІ підтверджує значний потенціал цієї технології у боротьбі з кіберзагрозами. ШІ дозволяє ефективно аналізувати великі обсяги даних, виявляти складні закономірності та аномалії, що дає змогу швидше та точніше реагувати на наявні та можливі загрози. Завдяки здатності аналізувати великі обсяги даних у режимі реального часу, ШІ дозволяє значно підвищити точність і швидкість виявлення кіберзагроз, зменшуючи кількість хибних спрацьовувань та підвищуючи загальний рівень безпеки. Використання ШІ дозволяє автоматизувати багато аспектів кібербезпеки, що зменшує навантаження на людські ресурси та знижує ризик людських помилок. Даний процес особливо важливий у контексті швидкозмінного інформаційного середовища, де швидкість реакції на інциденти є критичною. Поєднання ШІ з IoT та Big Data створює нові можливості для покращення кібербезпеки. Інтеграція цих технологій дозволяє здійснювати більш детальний аналіз даних та розробляти комплексні захисні стратегії.

Незважаючи на значні досягнення, використання ШІ у кібербезпеці стикається з низкою викликів, таких як забезпечення прозорості рішень, прийнятих ШІ, а також захист від потенційних загроз, створених з використанням тих самих технологій. Використання ШІ у кібербезпеці порушує важливі питання приватності, прозорості рішень та відповідальності за дії, здійснені на основі рішень ШІ-систем. Важливо розробити етичні та правові стандарти для регулювання використання ШІ у цій сфері.

Подальші наукові дослідження у галузі використання ШІ для підвищення кібербезпеки є необхідними для розробки нових, ще більш ефективних методів захисту, що відповідатимуть сучасним викликам. Інвестиції у технології ШІ для кібербезпеки

продовжують зростати, що підкреслює важливість цих технологій у боротьбі з кіберзагрозами.

Отже, дослідження показало, що ШІ є потужним інструментом для підвищення рівня кібербезпеки. Використання ШІ дозволяє не тільки підвищити ефективність захисту, але й сприяє розвитку нових стратегій та технологій для протидії загрозам у цифрову епоху. Інтеграція ШІ у системи кібербезпеки є необхідною для адаптації до нових викликів та забезпечення безпеки інформаційних систем у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Магденко, А. Р., Бучацький, І. О., & Бондаренко, І. О. (2024). *Штучний інтелект: нова зброя у руках кіберзлочинців та шахраїв*. https://ir.lib.vntu.edu.ua//handle/123456789/42455
2. Товстуха, Н. А. (2023). Використання штучного інтелекту для покращення кібербезпеки: за та проти. *Комп'ютерні системи та мережні технології: XIII Міжнар. науково-практ. конф.*, 153–154.
3. Устименко, В. О., & Олішевський І. Г. (2022). Перспективи застосування технологій штучного інтелекту в сфері кібербезпеки. *Молодь: наука та інновації: мат. X Міжнар. науково-тех. Конф. студентів, аспірантів та молодих вчених,* 375–377.
4. Каун, Ю., & Собчук, О. (2024). Штучний інтелект як інструмент кібератак і кібербезпеки. *Міжнародна науково-практична конференція «Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем»,* 40–41.
5. Гуржій, С. В. (2024). Потенціал штучного інтелекту у сфері кібербезпеки. *Матеріали XLII-ої Міжнар. науково-практ. конф. «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку»,* 260–261.
6. Котенко, Д., & Хлапонін, Ю. (2024). Штучний інтелект у системах виявлення і запобігання кібератакам: перспективи та виклики. *Підводні технології: промислова та цивільна інженерія, 1(14),* 48–55. https://doi.org/10.32347/uwt.2024.14.1203
7. Субач, І. Ю., & Власенко, О. В. (2023). Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки, 4,* 82–92.
8. Савицька, Л., Коробейнікова, Т., Волос, О., & Тарновський, М. (2023). Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM. *Інформаційні технології та комп'ютерна інженерія, 58(3),* 22–32.
9. Коробейнікова, Т., & Цар, О. (2023). Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. *Grail of Science, 27,* 317–325.
10. Bondarenko, A., & Statsenko, V. (2024). Using artificial intelligence methods and models to improve expert intrusion detection systems. *Technical sciences, 333(2),* 99–106.
11. Цеба, К. Я. (2024). Огляд сучасних інструментів та технологій виявлення кіберзагроз. *Матеріали XV-ої Міжнародної науково-практичної конференції «Free and Open Source Software»*.
12. Бабкін, А. А., & Кудін, О. В. (2020). Огляд нейромережевих моделей систем виявлення вторгнень. *Вчені записки Таврійського національного університету ім. В.І. Вернадського. Серія: Технічні науки, 31(70),* 77–82.
13. Sarker, I. H., Furhad, M. H., Nowrozy, R. (2021). AI-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science, 2(3).*
14. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS), 3(1),* 143–154.
15. Kuzlu, M., Fair, C., Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things, 1(1),* 7–17.
16. Gupta, M., Akiri, C., Aryal, K., Parker, E., Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access, 11,* 80218–80245. https://doi.org/10.1109/ACCESS.2023.3300381
17. Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity, 7(12),* 25–43.
18. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering, 10(2).* https://doi.org/10.1080/23311916.2023.2272358

19. Capuano, N., Fenza, G., Loia, V., Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access, 10,* 93575–93600.
20. Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga. E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews, 21(1),* 2263–2275.
21. *MarketsandMarkets.* (n. d.). https://www.marketsandmarkets.com
22. *IBM X-Force Threat Intelligence Index.* (n. d.). https://www.ibm.com/reports/threat-intelligence
23. *Gartner.* (n. d.). https://www.gartner.com/en
24. *Statista.* (n. d.). https://www.statista.com
25. *National Institute of Standards and Technology (NIST).* (n. d.). https://www.nist.gov

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Olha Lunhol
PhD in Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of
Operational-search Activities and Information Security
Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-8128-0072
olyalungol@gmail.com

OVERVIEW OF CYBERSECURITY METHODS AND STRATEGIES USING ARTIFICIAL INTELLIGENCE

Abstract. In today's world, information technology is rapidly evolving, leading to an increase in both the number and complexity of cyber threats, including phishing, malware, and social engineering attacks. The growth in the quantity and sophistication of cyber threats creates an urgent need to improve methods for protecting information systems. Artificial Intelligence (AI), particularly machine learning and deep learning technologies, shows significant potential in enhancing cybersecurity. This article is dedicated to reviewing contemporary AI-based cybersecurity methods and strategies, as well as evaluating their effectiveness in detecting and countering cyber threats. The paper analyzes recent research by both domestic and international scientists, emphasizing AI's ability to analyze large volumes of data, uncover hidden patterns, predict potential threats, and automate incident response processes. It highlights key research directions, including anomaly detection, threat modeling, incident response automation, and ensuring the interpretability of decisions made by AI systems. Special attention is given to the integration of AI into existing cybersecurity systems and its capacity to adapt to new threats. The article also discusses the main challenges and prospects of applying AI in cybersecurity, including ethical and legal aspects such as privacy issues, decision transparency, and accountability for actions taken based on AI system decisions. Recent statistical data indicate a rapid growth in the market for AI-based cybersecurity tools, underscoring the importance and relevance of this topic in contemporary conditions. The analysis results confirm that using AI allows for automating monitoring, threat detection, and response processes, reducing incident response time and enhancing the overall protection level of information systems. At the same time, implementing AI in cybersecurity faces several challenges, such as ensuring the transparency of AI decisions and protecting against potential threats created using the same technologies. Research in this field promotes strategic development and innovation in cybersecurity, providing researchers and professionals with new tools and methods for ensuring information system security. Thus, given the rapid growth and evolution of cyber threats, studying the role of AI in cybersecurity is extremely relevant and important. It not only enhances protection efficiency but also fosters the development of new strategies and technologies to counter threats in the digital age.

Keywords: Artificial Intelligence; cyber security; threats; information space.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Magdenko, A. R., Buchatskyi, I. O., & Bondarenko, I. O. (2024). *Artificial intelligence: a new weapon in the hands of cybercriminals and fraudsters.* https://ir.lib.vntu.edu.ua//handle/123456789/42455.
2. Tovstukha, N. A. (2023). Using artificial intelligence to improve cybersecurity: pros and cons. *Computer systems and network technologies: XIII International Scientific and Practical Conference,* 153–154.
3. Ustymenko, V. O., & Olishevskyi, I. G. (2022). Prospects for the application of artificial intelligence technologies in the field of cybersecurity. *Youth: science and innovations: mat. X Internat. scientific and technical conf. of students, graduate students and young scientists,* 375–377.
4. Kaun, Y., & Sobchuk, O. (2024). Artificial intelligence as a tool for cyberattacks and cybersecurity. *International scientific and practical conference "Problems of computer science, software modeling and security of digital systems",* 40–41.

5. Gurzhiy, S. V. (2024). The potential of artificial intelligence in the field of cybersecurity. *Proceedings of the XLIIth International Scientific and Practical Conference "Modern Aspects of Modernization of Science: State, Problems, Development Trends",* 260–261.
6. Kotenko, D., & Khlaponin, Y. (2024). Artificial Intelligence in Cyber Attack Detection and Prevention Systems: Prospects and Challenges. *Underwater technologies: industrial and civil engineering, 1(14),* 48–55. https://doi.org/10.32347/uwt.2024.14.1203
7. Subach, I. Y., & Vlasenko, O. V. (2023). Architecture of an intelligent SIEM system for detecting cyber incidents in databases of information and communication systems for military purposes. *Systems and technologies of communication, informatization and cybersecurity, 4,* 82–92.
8. Savytska, L., Korobeynikova, T., Volos, O., & Tarnovskyi, M. (2023). Method and means of monitoring security in a computer network by means of SIEM. *Information technology and computer engineering, 58(3),* 22–32.
9. Korobeynikova, T., & Tsar, O. (2023). Analysis of modern open systems for intrusion detection and prevention. *Grail of Science, 27,* 317–325.
10. Bondarenko, A., & Statsenko, V. (2024). Using artificial intelligence methods and models to improve expert intrusion detection systems. *Technical sciences, 333(2),* 99–106.
11. Tseba, K. Y. (2024). An overview of modern tools and technologies for detecting cyber threats. *Proceedings of the XVth International Scientific and Practical Conference "Free and Open Source Software".*
12. Babkin, A. A., & Kudin, O. V. (2020). An overview of neural network models of intrusion detection systems. *Scientific Notes of the V.I. Vernadsky Taurida National University. Series: Technical Sciences, 31(70),* 77–82.
13. Sarker, I. H., Furhad, M. H., Nowrozy, R. (2021). AI-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science, 2(3).*
14. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS), 3(1),* 143–154.
15. Kuzlu, M., Fair, C., Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things, 1(1),* 7–17.
16. Gupta, M., Akiri, C., Aryal, K., Parker, E., Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access, 11,* 80218–80245. https://doi.org/10.1109/ACCESS.2023.3300381
17. Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity, 7(12),* 25–43.
18. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering, 10(2).* https://doi.org/10.1080/23311916.2023.2272358
19. Capuano, N., Fenza, G., Loia, V., Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access, 10,* 93575–93600.
20. Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga. E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews, 21(1),* 2263–2275.
21. *MarketsandMarkets.* (n. d.). https://www.marketsandmarkets.com
22. *IBM X-Force Threat Intelligence Index.* (n. d.). https://www.ibm.com/reports/threat-intelligence
23. *Gartner.* (n. d.). https://www.gartner.com/en
24. *Statista.* (n. d.). https://www.statista.com
25. *National Institute of Standards and Technology (NIST).* (n. d.). https://www.nist.gov