*ISSN 2786-5371 print*
*ISSN 2786-538X online*
*Технології та інжиніринг, № 4(21), 2024*

***Інформаційні технології, електроніка, механічна та електрична інженерія***
***Information technologies, electronics, mechanical and electrical engineering***

*ttps://doi.org/10.30857/2786-5371.2024.4.8*

**УДК 004.89**

**ТРОФИМЕНКО О. Г., СОКОЛОВ А. В., ЧИКУНОВ П. О., АХМАМЕТЬЄВА Г. В., МАНАКОВ С. Ю.**
*Національний університет «Одеська юридична академія», Україна*

# ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ КІБЕРСФЕРІ

***Мета**. Аналіз ролі штучного інтелекту (ШІ) для забезпечення кібербезпеки військових мереж та можливості застосування ШІ у галузі кібербезпеки оборонної сфери.*

***Методика**. При проведенні дослідження були використані методи аналізу наукових та літературних джерел, інформаційного пошуку, порівняння та узагальнення.*

***Результати.** Проведено порівняння та аналіз наявної у відкритому доступі інформації про технології та інструменти кібербезпеки на основі ШІ. В результаті проведеного наукового аналізу встановлено, що інструменти ШІ відіграють важливу роль у виявленні та стримуванні загроз несанкціонованих вторгнень у систему безпеки військової мережі. З'ясовано, що ШІ наразі є необхідністю для кожної комп'ютерної системи та мережі. Використання технологій ШІ у формі інтелектуальних агентів є доволі ефективним інструментом для захисту від кібератак та оцінювання вразливостей і ризиків у кіберпросторі. Під час цілодобового потокового аналізу великих обсягів даних у режимі реального часу ШІ здатен визначати закономірності та надавати рекомендації щодо можливого усунення виявлених вразливостей. Програмне забезпечення для кіберзахисту на основі ШІ реагує на атаки, ізолюючи уражені системи.*

***Наукова новизна**. Проаналізовано та систематизовано сфери можливого застосування ШІ у військових кібероперацій. Розглянуто технології машинного та глибинного навчання, штучних нейронних мереж для ідентифікації та прогнозування кіберзагроз.*

***Практична значимість**. Отримані результати проведеного аналізу вказують на потужний потенціал використання інтелектуальних технологій та інструментів для військової галузі. Технології ШІ надає кібербезпековим командам гнучкість, масштабованість та можливість автоматизації виявлення загроз. Впровадження ШІ у кібербезпеку військової сфери здатне суттєво зменшити кіберризики, скоротити витрати й оптимізувати процеси виявлення, дослідження, реагування та моніторингу кіберзагроз у реальному часі. Робота сприяє інтенсифікації проактивного виявлення та аналізу потенційних кіберзагроз у поєднанні з діями реагування на інциденти та загрози у боротьбі з кіберзлочинністю. Зрештою, ці досягнення допоможуть нашому кібервійську бути краще підготовленим й оснащеним до викликів і ризиків сучасної війни.*

***Ключові слова:** штучний інтелект (ШІ); кібербезпека; ризики кіберзагроз; військова галузь; тестування; машинне навчання; глибоке навчання; нейронні мережі.*

**Вступ.** Через високий рівень ризиків витоків даних у військових та оборонних мережах важко переоцінити переваги застосування технологій штучного інтелекту (ШІ, Artificial Intelligence, AI) для кібербезпеки. Величезні обсяги розвідувальних даних з одного боку та небезпеки їх витоків з іншого зумовлюють високий рівень пріоритету кібербезпеки для армії та уряду будь-якої держави світу. Завдяки використанню систем ШІ полегшується збір, аналіз та класифікація великих обсягів даних. Штучний інтелект може відігравати важливу роль у профілактичних заходах для військових, щоб ідентифікувати та оцінювати зловмисне програмне забезпечення.

Проведений аналіз наявних досліджень свідчить про важливість дослідження можливих сфер застосування ШІ у військовій кібербезпеці, а повсюдне впровадження технологій ШІ потребує підвищеної уваги до цього напрямку, й відповідно, глибокого висвітлення питань потенційних переваг та ризиків впровадження ШІ в кібербезпеку оборонного сектора. Дослідження [1] вивчає людиноорієнтовану концепцію ШІ у військових кібероперацій, ілюструє способи встановлення пріоритетів залучення та взаємодії людини, людського розуміння, ефективного ухвалення рішень та етичних міркувань під час створення

та проведення військових кібероперацій. Стаття [2] досліджує можливий вплив ШІ на глобальну кібербезпеку. У роботі [3] відзначено, що інвестиції у розробку та впровадження ШІ та робототехніки у військову сферу дозволять зменшити ризики для життя людей і скоротити витрати. Автори цієї статті звертають увагу на те, що наразі сфери спостереження, розвідки та кібероперацій можуть ефективно функціонувати лише за допомогою ШІ. Автори статті [4] порівняли особливості військового ШІ, зосередженого на цілях стратегічної оборони, з цивільним ШІ. У роботі [5] дійшли висновку, що ШІ став незамінною інновацією для мережевої безпеки. Робота [6] називає національну безпеку та кібербезпеку одними з ключових сфер можливого застосування штучного інтелекту в армії, разом зі сферами транспорту, логістики та навчальної бойової підготовки.

**Визначення мети дослідження.** Основною метою даної роботи є аналіз ролі ШІ для забезпечення кібербезпеки військових мереж та можливості застосування ШІ у галузі кібербезпеки оборонної сфери.

**Результати дослідження.**

***1. ШІ для ідентифікації та прогнозування кіберзагроз.*** Інтелектуальний аналіз великих масивів текстових, графічних, аудіо та відео даних дозволяють виявляти потенційні терористичні загрози, формувати доказову базу підготовки правопорушень задля їх ефективного застосування у сфері безпеки.

Кваліфіковані зловмисники вишукують і винаходять нові способи та інструменти проникнення, щоб завдати серйозної шкоди. Вони здійснюють атаки й використовують різноманітні способи поширення шкідливого програмного забезпечення, яке може залишатися прихованими в системі тривалий час. Наразі кіберзлочинність викрадає приблизно 1% світового ВВП [7]. Кіберзагрози стрімко розвиваються, а тому застосування брандмауерів та антивірусного програмного забезпечення вже недостатньо [8]. Потрібні більш інтелектуальні інструменти на основі ШІ, які з часом тільки підвищують ефективність та точність виявлення загроз, покращують розуміння користувачами активних кіберзагроз, відкривають інноваційні шляхи розвитку для забезпечення кібербезпеки, у тому числі й заходи превентивного характеру [9].

Використання ШІ для виявлення й аналізу загроз не лише покращує точність і швидкість цих процесів, а й масштабує операції безпеки для ефективного керування зростаючим обсягом кіберзагроз. Завдяки аналізу наявних ретроспективних даних та поточних тенденцій, ШІ моделює прогнозну аналітику для передбачення потенційних порушень безпеки. ШІ здатен передбачити появу вразливості та запропонувати запобіжні заходи, що надає змогу організаціям усунути недоліки, перш ніж їх використають злочинці [10]. Тим самим ШІ покращує профілактичні заходи безпеки та посилює загальну кіберстійкість.

***2. Використання технологій ШІ в кібербезпеці.***

***Машинне навчання***. Використання машинного навчання (Machine Leaning, ML) у програмних продуктах безпеки дозволяє ідентифікувати та прогнозувати загрози до того, як вони вплинуть на військові мережі інтернету речей (IoT). Ідентифікація технічних та програмних інструментів для імплантації зловмисного програмного забезпечення та подальша нейтралізація кіберзагроз у військовій сфері за допомогою ML можлива ще до того, як зловмисне програмне забезпечення почне активуватися. ШІ та ML аналізують поведінку мережі, виявляють аномалії, розрізняючи законні транзакції від шахрайських [11]. ML використовується для пошуку й виявлення зловмисних сценаріїв, первинних заражень, визначення пріоритетів впливу та стримування загроз вторгнення в систему безпеки військової мережі. Алгоритми ШІ сканують та вивчають поведінку файлів та вміст електронних листів на ознаки фішингу, щоб виявити шаблони, схожі на зловмисне програмне

забезпечення. Загалом традиційне антивірусне програмне забезпечення покладається на відомі сигнатури шкідливих програм, а ШІ відстежує і вивчає дії зловмисного програмного забезпечення, щоб знайти навіть невідомі варіанти.

***Глибоке навчання***. ШІ використовує глибоке навчання (Deep Learning, DL) для виявлення складних загроз зловмисних програм, які оминають звичайні заходи безпеки. Глибоке навчання, яке імітує здатність людського мозку навчатися з великої кількості даних, використовується для виявлення складних закономірностей і аномалій, які зазвичай важко вловити традиційними методами. Це дозволяє запобігати та виявляти розширені постійні загрози (Advanced Persistent Threat, APT), інсайдерські загрози та обхідні атаки, які не помічають традиційні заходи безпеки [12]. Завдяки постійному навчанню алгоритми ШІ вдосконалюються і можуть відрізняти законні дії від потенційних загроз, зменшуючи хибні спрацьовування.. Це покращує аналіз загроз та зміцнює захист від нових загроз ще до того, як вони виникнуть. При цьому суттєвим є те, що системи виявлення загроз на основі ШІ обробляють величезні обсяги даних у реальному часі для виявлення загроз у мережах. Тим самим скорочується частка ручного аналізу, що прискорює виявлення та ефективне реагування на небезпеки.

***Штучні нейронні мережі***. Нейронні мережі мають широке застосування в галузі інформаційної безпеки. Вони можуть аналізувати шаблони мережевого трафіку, щоб виявляти загрози безпеці, зловмисне програмне забезпечення та несанкціоновані вторгнення. Вони здатні ідентифікувати незвичні шаблони в мережевих діях, активувати сповіщення системи безпеки, що дозволяє вживати профілактичні заходи. Нейронні мережі можна використовувати в процесах розпізнавання особи та автентифікації. Аналізуючи закономірності та відповідні ознаки ідентичності особи, ці методи можуть перевірити й визначити, чи є ця особа авторизованою, чи ні [13]. Тому нейронні мережі здатні ідентифікувати підозрілі моделі поведінки та тенденції у фінансових операціях, щоб виявляти шахрайство у фінансовій сфері, онлайн-платежах і банківських системах [14]. Також нейронні мережі можна використовувати в процесах шифрування та дешифрування інформації, позаяк вони можуть використовувати можливості глибокого навчання для розробки та ідентифікації складних алгоритмів шифрування та дешифрування [15]. Важливо відзначити, що в будь-якому домені безпеки використання нейронних мереж вимагає точності та повного розуміння загроз безпеці та можливих обмежень. Крім того, при використанні нейронних мереж у безпеці слід приділяти належну увагу збереженню конфіденційності даних.

***3. Інструменти ШІ для кібербезпеки.*** Отже, в системах виявлення вторгнень і системах безпеки можна використовувати різні технології ШІ та їх комбінації. Так, запропонована у травні 2024 року платформа Google Threat Intelligence для автоматизації аналізу кіберзагроз, завдяки використанню можливостей генеративного ШІ, поєднує та аналізує дані з різних джерел і здатна швидко виявляти та класифікувати загрози [16]. Іншими прикладами сучасних інструментів для виявлення кіберзагроз, які використовують технології ШІ є: Darktrace (https://darktrace.com), Cylance (https://login.cylance.com), Vectra AI (https://www.vectra.ai), SentinelOne (https://www.sentinelone.com), Cybereason (https://www.cybereason.com/), McAfee MVISION (https://www.mcafee.com/), FortiAI (https://www.fortinet.com/) тощо. Ці інструменти використовують дещо різні підходи, алгоритми та технології (ML, DL, прогнозну аналітику для виявлення загроз, реагування на інциденти та захисту конфіденційних даних у режимі реального часу.

Добре зарекомендувала себе синергічна взаємодія між платформою розширеного виявлення та реагування на інциденти безпеки (eXtended Detection and Response, XDR), операційним центром безпеки (Security Operations Center, SOC), зосередженим на управлінні загрозами і вразливостями, проактивному моніторингу інцидентів, та набором інструментів і

методів для дослідження подій, важливих для кібербезпеки (Security Information and Event Management, SIEM) [17]. Саме SIEM із використанням ШІ та машинного навчання дає змогу стандартизовано використовувати дані журналізації транзакцій з різних інструментів безпеки та забезпечує розширений моніторинг великих наборів даних шляхом збору й аналізу подій безпеки і контекстних джерел даних у реальному часі. Хмарна платформа XDR за допомогою ШІ оптимізує процеси виявлення, дослідження, реагування та моніторингу кіберзагроз у реальному часі. XDR враховує найдрібніші деталі, сприяючи виявленню раніше непомічених загроз. Завдяки використанню потужностей аналізу великих даних, XDR надає кібербезпековим командам гнучкість, масштабованість та можливість автоматизації виявлення загроз. Ці інструменти із застосуванням технологій ШІ допомагають інтенсифікувати проактивне виявлення та аналіз потенційних кіберзагроз у поєднанні з діями реагування на інциденти та загрози у боротьбі з кіберзлочинністю [18].

Системи ШІ в армії тісно взаємопов'язані з іншими системами і через це вразливі до кібератак. Зловмисне використання ШІ може завдати значної шкоди військовій інфраструктурі, персоналу та операціям. Крім того, кібератаки на основі ШІ складно виявити та запобігти їм. Тому інструменти кібербезпеки на основі ШІ наразі є необхідністю для кожної комп'ютерної системи та мережі. Їх використання є проактивним кроком реагування задля зменшення ризиків кіберзагроз і кіберзлочинів. Інтеграція інструментів ШІ в систему дозволяє автоматизувати процес виявлення ризиків витоків даних, захисту від розподілених атак на відмову в обслуговуванні (DDoS) та стримування загроз несанкціонованих вторгнень у систему безпеки військової мережі.

***4. Інтелектуальні методи автентифікації.*** Системи контролю доступу користувачів на основі ШІ пропонують надійні рішення автентифікації. Традиційні методи автентифікації, які використовують паролі, більш вразливі до злому через можливе повторне використання пароля у разі викрадення облікових даних. Донедавна двофакторна автентифікація була найкращим способом захисту профілів користувачів. Залучення до цього процесу ШІ дозволило сформувати нові рівні захисту для перевірки особи за допомогою розширених метаданих безпеки. Для автентифікації ШІ додатково враховує фактори біометрії та моделі поведінки користувачів, наприклад: динаміку натискання клавіш, розпізнавання обличчя та голосу. Тим самим поведінкова біометрія здатна забезпечити безпечну автентифікацію, навіть без пароля. Використання поведінкової біометрії, відбитків пальців та іншої контекстної інформації для розширеної багатофакторної автентифікації суттєво ускладнюють доступ неавторизованим користувачам, навіть у випадку викрадення облікових даних.

Загрози кібербезпеці бувають різних форм і розмірів. Хакери полюють за секретами як військових, так і приватних організацій. Використання технологій ШІ у формі інтелектуальних агентів є доволі ефективним інструментом для захисту від кібератак та оцінювання вразливостей і ризиків у кіберпросторі. Автоматизація на основі ШІ спрощує рутинні завдання логічного тестування відповідності законодавчим правилам і нормам кібербезпеки та захисту персональних даних, дозволяючи командам із кібербезпеки зосередитися на більш важливих справах, що допускає номінальне залучення до процесів із заміщенням осіб із числа військових. Оптимізація робочих процесів відбувається шляхом сповіщення та попередження персоналу відділу кібербезпеки про наявні виявлені невідповідності та ризики загроз [19]. Під час цілодобового потокового аналізу великих обсягів даних у режимі реального часу ШІ здатен визначати закономірності та надавати рекомендації щодо можливого усунення виявлених вразливостей. Програмне забезпечення для кіберзахисту на основі ШІ реагує на атаки, ізолюючи уражені системи. При цьому шляхом самостійного навчання та глибокого аналізу даних з часом ШІ зменшує похибку і пропонує більш точні способи боротьби з кіберзагрозами, розробляє розумні методи можливого

усунення складних загроз, підходи до трансформації й оптимізації традиційних методів захисту інформації.

**Висновки.** Проведене дослідження з'ясувало великий потенціал використання ШІ у військовій кібербезпеці. Наразі фахівці з кібербезпеки часто використовують ШІ як засіб захисту від різних форм атак. Системи безпеки на основі ШІ сканують на наявність зловмисного програмного забезпечення та ізолюють підозрілі файли або ж блокують доступ у разі несанкціонованих спроб зловмисників отримати конфіденційні дані. Це робить їх чудовим інструментом у виявленні нових, незнайомих штамів шкідливих програм, які традиційне антивірусне програмне забезпечення може пропустити. Тим самим ШІ допомагає експертам з кібербезпеки зменшити ризики злому та посилити безпеку шляхом аналізу та виявлення загроз.

Використання різних технологій ШІ дозволяє в режимі реального часу знаходити та класифікувати шаблони та аномалії, які можуть залишитися непоміченими людьми. Можливості ШІ до аналізу даних дозволяють моніторити поведінку пристроїв та виявляти потенційні загрози безпеці, навіть коли пристрої перебувають в офлайн-режимі. І хоча програмні системи кібербезпеки на базі ШІ мають певні ризики, проте партнерство між людьми та ШІ здатне створити більш безпечне майбутнє в діяльності військовослужбовців.

## References

1. Maathuis, C. (2024). Human-Centered AI in Military Cyber Operations. *International Conference on Cyber Warfare and Security*, Vol. 19, P. 121–128. DOI: https://doi.org/10.34190/iccws.19.1.1972.

2. Khalifa, E. (2021). Artificial Intelligence and Global Security. *International Affairs Forum* (IAF'21), P. 1–3. URL: https://www.researchgate.net/publication/356207786_Artificial_Intelligence_and_Global_Security.

3. Agarwala, N. (2023). Robots and Artificial Intelligence in the Military. *Obrana a strategie*, Vol. 23 (2), P. 083–100. DOI: https://doi.org/10.3849/1802-7199.23.2023.02.083-100.

4. Bansi, K., Shivam, P. (2023). Collision Between Military Artificial Intelligence and Civilian Artificial Intelligence. *OSR Journal of Computer Engineering* (IOSR-JCE), Vol. 25, Iss. 6, Ser. 1, P. 38–48, DOI: https://doi.org/1010.9790/0661-2506013848.

5. Ibrahim, A. (2024). Defense Disrupted: AI and ML Transforming Cybersecurity. URL: https://www.researchgate.net/publication/380152320_Defense_Disrupted_AI_and_ML_Transforming_Cybersecurity_AUTHORSIBRAHIM_A.

6. Rashid, A. B., Kausik, A. K., Sunny, A. H., Bappy, M. H. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. *International Journal of Intelligent Systems*, Vol. 2023, Article ID 8676366, P. 1–31, DOI: https://doi.org/10.1155/2023/8676366.

## Література

1. Maathuis C. Human-Centered AI in Military Cyber Operations. *International Conference on Cyber Warfare and Security*. 2024. Vol. 19. P. 121–128. DOI: https://doi.org/10.34190/iccws.19.1.1972.

2. Khalifa E. Artificial Intelligence and Global Security. *International Affairs Forum* (IAF'21). 2021. P. 1–3. URL: https://www.researchgate.net/publication/356207786_Artificial_Intelligence_and_Global_Security.

3. Agarwala N. Robots and Artificial Intelligence in the Military. *Obrana a strategie*. 2023. Vol. 23 (2). P. 083–100. DOI: https://doi.org/10.3849/1802-7199.23.2023.02.083-100.

4. Bansi K., Shivam P. Collision Between Military Artificial Intelligence and Civilian Artificial Intelligence. *OSR Journal of Computer Engineering* (IOSR-JCE). 2023. Vol. 25, Iss. 6, Ser. 1. P. 38–48. DOI: https://doi.org/10.9790/0661-2506013848.

5. Ibrahim A. Defense Disrupted: AI and ML Transforming Cybersecurity. 2024. URL: https://www.researchgate.net/publication/380152320_Defense_Disrupted_AI_and_ML_Transforming_Cybersecurity_AUTHORSIBRAHIM_A.

6. Rashid A. B., Kausik A. K., Sunny A. H., Bappy M. H. Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. *International Journal of Intelligent Systems*. 2023. Vol. 2023,

7. AI-Powered Cybersecurity: Top Use Cases in 2023. URL: https://hackernoon.com/ai-powered-cybersecurity-top-use-cases-in-2023.

8. Trofymenko, O. G., Prokop, Yu. V., Loginova, N. I., Zadereyko, O. V. (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu [Cybersecurity of Ukraine: analysis of the current situation]. *Zakhyst informatsii = Ukrainian Information Security Research Journal*, Vol. 21, No. 3, P. 150–157. DOI: https://doi.org/10.18372/2410-7840.21.13951 [in Ukrainian].

9. Roth, M. Artificial Intelligence in the Military – An Overview of Capabilities. URL: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

10. AI in Cybersecurity: Transforming Cyber Defense Mechanisms. URL: https://www.ppln.co/tpost/elo03cn2g1-ai-in-cybersecurity-transforming-cyber-d.

11. Trofymenko, O. G., Loginova, N. I., Manakov, S. Yu., Dubovoi, Ya. V. (2022). Kiberzahrozy v osvitnomu sektori [Cyberthreats in higher education]. *Kiberbezpeka: osvita, nauka, tekhnika = Cybersecurity: Education, Science, Technique*, Vol. 4 (16), P. 76–84, DOI: https://doi.org/10.28925/2663-4023.2022.16.7684, URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/365 [in Ukrainian].

12. Do Xuan, C., Dao, M. H. (2021). A novel approach for APT attack detection based on combined deep learning model. *Neural Comput & Applic*, Vol. 33, P. 13251–13264, DOI: https://doi.org/10.1007/s00521-021-05952-5.

13. Minuchehr, A. Neural Networks and Security. URL: https://www.linkedin.com/pulse/neural-networks-security-ali-minoo/

14. Soroor, M., Bijan, R. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, Vol. 240, P. 122–156. DOI: https://doi.org/10.1016/j.eswa.2023.122156.

15. Fu, Y., Fu, J., Wei, J. (2023). Encryption and Decryption Using Deep Neural Network. *Machine Learning and Artificial Intelligence*, Vol. 374, P. 9–15, DOI: https://doi.org/10.3233/FAIA230762.

16. Google Threat Intelligence. Actionable threat intelligence at Google scale. URL: https://cloud.google.com/security/products/threat-intelligence/?hl=en.

Article ID 8676366. P. 1–31. DOI: https://doi.org/10.1155/2023/8676366.

7. AI-Powered Cybersecurity: Top Use Cases in 2023. URL: https://hackernoon.com/ai-powered-cybersecurity-top-use-cases-in-2023.

8. Трофименко О. Г., Прокоп Ю. В., Логінова Н. І., Задерейко О. В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21. № 3. С. 150–157. DOI: https://doi.org/10.18372/2410-7840.21.13951.

9. Roth M. Artificial Intelligence in the Military – An Overview of Capabilities. URL: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

10. AI in Cybersecurity: Transforming Cyber Defense Mechanisms. URL: https://www.ppln.co/tpost/elo03cn2g1-ai-in-cybersecurity-transforming-cyber-d.

11. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Дубовой Я. В. Кіберзагрози в освітньому секторі. *Кібербезпека: освіта, наука, техніка*. 2022. № 4 (16). С. 76–84. DOI: https://doi.org/10.28925/2663-4023.2022.16.7684. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/365.

12. Do Xuan C., Dao M. H. A novel approach for APT attack detection based on combined deep learning model. *Neural Comput & Applic*. 2021. Vol. 33. P. 13251–13264. DOI: https://doi.org/10.1007/s00521-021-05952-5.

13. Minuchehr A. Neural Networks and Security. URL: https://www.linkedin.com/pulse/neural-networks-security-ali-minoo/

14. Soroor M., Bijan R. Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*. 2024. Vol. 240. P. 122–156. DOI: https://doi.org/10.1016/j.eswa.2023.122156.

15. Fu Y., Fu J., Wei J. Encryption and Decryption Using Deep Neural Network. *Machine Learning and Artificial Intelligence*. 2023. Vol. 374. P. 9–15. DOI: https://doi.org/10.3233/FAIA230762.

16. Google Threat Intelligence. Actionable threat intelligence at Google scale. URL: https://cloud.google.com/security/products/threat-intelligence/?hl=en.

17. Trofymenko, O. G., Kikh, Y. T. (2024). Vykorystannia shtuchnoho intelektu u viiskovyi tekhnolohiiakh [Application of artificial intelligence in military technologies]. *Informatsiine suspilstvo: problemy ta perspektyvy: mater. IKh vseukr. nauk.-prakt. konf. = 9th All-Ukrainian scientific and practical conference "Information society: problems and prospects"* (Odesa, May 24, 2024), P. 76–79, DOI: https://doi.org/10.32837/11300.27842 [in Ukrainian].

18. SIEM / XDR / SOAR Solutions for SOC. URL: https://nxgsecure.com/siem-xdr-soar-solutions-for-soc/

19. Trofymenko, O. G., Yaremchuk, M. V. (2023) Shtuchnyi intelekt u viiskovii sferi [Artificial intelligence in the military sphere]. *Kiberprostir v umovakh viiny ta hlobalnykh vyklykiv KhKhI stolittia: teoriia ta praktyka: mater. mizhnar. nauk.-prakt. konf. = International scientific and practical conference "Cyberspace in conditions of war and global challenges of the 21st century: theory and practice"* (Odesa, November 24, 2023), P. 144–148. DOI: https://doi.org/10.32837/11300.27179 [in Ukrainian].

17. Трофименко О. Г., Кіх Я. Т. Використання штучного інтелекту у військовий технологіях. *Інформаційне суспільство: проблеми та перспективи: матер. IX всеукр. наук.-практ. конф.* (24 травня 2024). Одеса, 2024. С. 76–79. DOI: https://doi.org/10.32837/11300.27842.

18. SIEM / XDR / SOAR Solutions for SOC. URL: https://nxgsecure.com/siem-xdr-soar-solutions-for-soc/

19. Трофименко О. Г., Яремчук М. В. Штучний інтелект у військовій сфері. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика: матер. міжнар. наук.-практ. конф*. (Одеса, 24 листопада 2023 р.). Одеса: НУ "ОЮА", 2023. С. 144–148. DOI: https://doi.org/10.32837/11300.27179.

***TROFYMENKO OLENA***
*PhD, Associate Professor,*
*Department of Information Technologies,*
*National University "Odessa Law Academy", Ukraine*
*https://orcid.org/0000-0001-7626-0886*
*Scopus Author ID: 57189319394*
*ResearcherID: AAE-5852-2021*
*E-mail: trofymenko@onua.edu.ua*

***SOKOLOV ARTEM***
*Doctor of Technical Sciences, Professor,*
*Department of Cyber Security,*
*National University "Odesa Law Academy", Ukraine*
*https://orcid.org/0000-0003-0283-7229*
*Scopus Author ID: 7402611956*
*E-mail: radiosquid@gmail.com*

***CHYKUNOV PAVLO***
*PhD, Associate Professor,*
*Department of Information Technologies, National University "Odesa Law Academy", Ukraine,*
*https://orcid.org/0000-0003-4959-7744*
*ResearcherID: D-2957-2019*
*E-mail: pavel@onua.edu.ua*

***AKHMAMETIEVA HANNA***
*PhD, Associate Professor,*
*Department of Cyber Security,*
*National University "Odesa Law Academy", Ukraine*
*https://orcid.org/0000-0002-0567-902X*
*Scopus Author ID: 57200117944*
*E-mail: anna.odessitka@gmail.com*

***MANAKOV SERHII***
*PhD, Associate Professor,*
*Department of Information Technologies,*
*National University "Odesa Law Academy", Ukraine,*
*https://orcid.org/0000-0001-5930-4592*
*Scopus Author ID: 57224370160*
*E-mail: manakov_serhii@onua.edu.ua*

**TROFYMENKO O. G., SOKOLOV A. V., CHYKUNOV P. O.,**
**AKHMAMETIEVA H. V., MANAKOV S. Yu.**
*National University "Odesa Law Academy", Ukraine*

## AI IN THE MILITARY CYBER DOMAIN

***Purpose***. *Analysis of the role of artificial intelligence (AI) in ensuring the cyber security of military networks and the possibility of applying AI in cybersecurity in defense.*

***Methodology***. *The research used methods of analysis of scientific and literary sources, information search, comparison, and generalization.*

***Findings***. *A comparison and analysis of publicly available information on AI-based cybersecurity technologies and tools was performed. As a result of the performed scientific analysis, it was established that AI tools play an important role in detecting and deterring threats of unauthorized intrusions into the security system of the military network. It has been found that AI is now a necessity for every computer system and network. The use of AI technologies in the form of intelligent agents is an effective tool for protecting against cyber attacks and assessing vulnerabilities and risks in cyberspace. During the 24/7 streaming analysis of large volumes of data in real-time, AI can identify patterns and provide recommendations for possible remediation of identified vulnerabilities. AI-powered cyber defense software responds to attacks by isolating affected systems.*

***Originality***. *Areas of possible application of AI in military cyber operations were analyzed and systematized. Technologies of machine and deep learning, and artificial neural networks for identification and prediction of cyber threats are considered.*

***Practical value***. *The obtained results of the performed analysis indicate the powerful potential of using intelligent technologies and tools for the military industry. AI technologies provide cybersecurity teams with flexibility, scalability, and the ability to automate threat detection. The implementation of AI in the cyber security of the military sphere can significantly reduce cyber risks, reduce costs, and optimize the processes of detection, research, response, and monitoring of cyber threats in real time. The paper contributes to the intensification of proactive detection and analysis of potential cyber threats in conjunction with incident and threat response activities in the fight against cybercrime. Ultimately, these advances will help our cyber military to be better prepared and equipped for the challenges and risks of modern warfare.*

***Keywords****: artificial intelligence (AI); cyber security; risks of cyber threats; military industry; testing; machine learning; deep learning; neural networks.*