Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.16

Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи розвитку

Роман Пантюшенко
провідний науковий співробітник науково-випробувального відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, Повітрофлотський проспект, 28 Б, Київ, Україна
e-mail: prvm79@gmail.com
ORCID: 0000-0002-9301-9389

Юлія Чайка
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, Повітрофлотський проспект, 28 Б, Київ, Україна
e-mail: jul.seagull@gmail.com
ORCID: 0009-0002-4342-3313

Анотація. Актуальність дослідження обумовлена необхідністю ефективного захисту інформаційних систем в умовах постійно зростаючих кіберзагроз. У сучасному цифровому світі, де кібератаки стають все більш складними та поширеними, використання штучного інтелекту у сфері кібербезпеки є надзвичайно актуальним. Проблема кібербезпеки набуває все більшого значення і проведення відповідних досліджень є необхідним аспектом забезпечення безпеки у цифровому просторі.

У зв'язку із цим, пропонуємо статтю, у якій розглянуто роль штучного інтелекту, інновації, виклики та перспективи його розвитку у сфері кібербезпеки. Також досліджено використання штучного інтелекту для автоматизації процесів виявлення, аналізування та реагування на кіберзагрози і його практичну значущість для підвищення рівня безпеки в цифровому просторі та ефективність захисту від кіберзагроз.

Провідними підходами для цього дослідження є аналізування трендів та експертні оцінювання, що дозволяють комплексно розглянути напрями розвитку штучного інтелекту у сфері кібербезпеки, переваги та виклики його впровадження, а також потенційні можливості і загрози для інформаційної безпеки.

У статті розглянуто передові системи управління інформацією та подіями безпеки, які призначені для збирання, аналізування та реагування на кіберзагрози, та інші системи, що спрямовані на конкретні аспекти захисту та розширення можливостей автоматизації для підвищення рівня безпеки інформаційних систем.

Матеріали статті становлять теоретичну цінність для подальших наукових досліджень щодо використання штучного інтелекту у сфері кібербезпеки та відображають важливі риси його впливу на цю сферу. Це дослідження може сприяти не лише поглибленню розуміння теоретичних аспектів застосування штучного інтелекту в кібербезпеці, а й виявленню конкретних практичних застосувань та інновацій, що сприятимуть покращенню захисту від кіберзагроз у майбутньому.

Ключові слова: штучний інтелект, кіберпростір, великі дані, системи управління інформацією та подіями безпеки.

Вступ (Introduction)

Швидкий та нестримний розвиток цифрових технологій призвів до того, що кібербезпека стала однією з найбільш актуальних та нагальних проблем (Hryshchuk, Zhovnovatiuk, Nosova, 2019) нашого часу. У світі, де кіберзлочинність поширюється швидше, ніж будь-коли (Когут, 2022), захист від кібератак є пріоритетом для всіх організацій та осіб, що працюють в кіберпросторі. У цьому контексті штучний інтелект (далі – ШІ) набуває все більшої важливості та актуальності (Онищенко, Каланча, Гельдт, 2023) як інструмент для виявлення, протидії та запобігання кіберзагрозам.

У цій статті розглядаються роль та переваги використання ШІ в сфері кібербезпеки (Гуржій, 2023), а також виклики та перспективи подальшого розвитку.

Зосереджуючись на інноваційних методах та технологіях, проведено дослідження впливу ШІ на ефективність та надійність кібербезпеки, а також розглянуто можливості подальшого вдосконалення (Устименко, Олішевський, 2022) у цій сфері для забезпечення безпеки у цифровому просторі.

Методологічна основа (Methodological Framework)

У дослідженні розглядалися системи управління подіями інформаційної безпеки (Security Information and Event Management, далі – SIEM), призначені для збирання, аналізування та реагування на кіберзагрози (Юшко, Шевчук, 2020). Ці технології забезпечують моніторинг та аналіз подій в реальному часі, що виникають у мережах та інших компонентах інформаційних систем. Отримані дані було використано для визначення основних тенденцій, викликів та перспектив розвитку ШІ в кібербезпеці.

Для підвищення ефективності виявлення кіберзагроз у сучасних системах SIEM активно застосовуються ШІ. Використання ШІ сприяє автоматизації збирання, аналізування великих даних (Big Data, далі – ВД) та виявлення аномалій, що, у свою чергу, значно підвищує ефективність реагування на потенційні загрози. Підхід, що ґрунтується на використанні ШІ, дозволяє ефективно ідентифікувати незвичайні патерни у поведінці системи та користувачів, що можуть вказувати на потенційні загрози.

Отже, використання ШІ у SIEM системах сприяє підвищенню ефективності та швидкості виявлення кіберзагроз, а також скорочення часу реагування на інциденти, що, у свою чергу, підвищує загальний рівень кібербезпеки.

Результати і обговорення (Results and Discussions)

У сучасному світі, де кіберзагрози стають все більш складними та витонченими, використання ШІ у сфері кібербезпеки є надзвичайно важливим та необхідним. Інноваційні методи та технології, що ґрунтуються на використанні ШІ відіграють ключову роль у постійному удосконаленні захисту від кіберзагроз.

ШІ широко використовується у сфері кібербезпеки для автоматизації процесу виявлення та аналізування потенційних кіберзагроз, аналізування відомостей з журналів подій (event logs), виявлення аномалій у поведінці користувачів, розпізнавання нових та невідомих загроз і розроблення прогностичних моделей, що допомагають передбачати можливі атаки. Згідно з проведеними дослідженнями використання ШІ в кібербезпеці може скоротити час виявлення та відновлення після інциденту до 25% та зменшити кількість помилкових спрацьовувань тривог до 50%. Ці можливості дозволяють значно підвищити ефективність та швидкість реагування на кіберзагрози, забезпечуючи вищий рівень безпеки у цифровому просторі.

Прикладом використання ШІ у сфері кібербезпеки можуть бути SIEM системи, які інтегрують його у свою структуру для автоматизації аналізу ВД і виявлення потенційних

загроз та аномалій поведінки в мережі, забезпечуючи ефективне реагування на кіберінциденти та скорочуючи час реакції на них.

SIEM система – це комплексна інформаційно-аналітична інфраструктура, що об'єднує в собі програмне та апаратне забезпечення, мережеві рішення, методи управління та процеси, спрямовані на забезпечення безпеки інформаційних систем, і призначена для збирання, аналізування, виявлення та реагування на події безпеки, що виникають у комп'ютерних системах, мережах та програмних додатках.

Системи SIEM широко використовують ШІ для вирішення завдань з управління безпекою в кіберсфері, включаючи виявлення, аналізування та реагування на кіберзагрози. Це сприяє зменшенню помилкових тривог і підвищенню ефективності захисту інформаційних систем у сучасних умовах постійно зростаючих кіберзагроз.

У результаті проведених досліджень провідною світовою дослідницькою та консалтинговою компанією Gartner, Inc. було створено "Магічний квадрант" для систем SIEM, який є результатом аналізу ринку безпеки інформаційних технологій. Цей квадрант надає об'єктивне уявлення про лідерів у цій галузі (Inci, 2023) та допомагає вибрати найкращі технологічні рішення. На основі цього ідентифікуються низка провідних у цій галузі компаній, які варто розглядати, вибираючи системи SIEM, а саме:



Рисунок 1. Магічний квадрант для SIEM

1. Splunk Enterprise Security
2. IBM Security QRadar
3. LogRhythm
4. Securonix
5. Micro Focus ArcSight
6. RSA NetWitness Platform
7. Exabeam
8. Elastic
9. SolarWinds Security Event Manager
10. AT&T Cybersecurity (AlienVault)

На рис.2 показано інтерфейс системи SIEM IBM Security QRadar, який включає інтуїтивно зрозуміле користувацьке інтерфейсне середовище для моніторингу та аналізування подій безпеки. Цей інтерфейс надає операторам можливість відстежувати потоки даних, виявляти аномальні активності, аналізувати вразливості та реагувати на потенційні загрози в

реальному часі. Крім того, він може відображати звіти та статистику щодо заходів безпеки, допомагаючи адміністраторам ухвалювати обґрунтовані рішення щодо заходів з підвищення безпеки інформаційної інфраструктури.

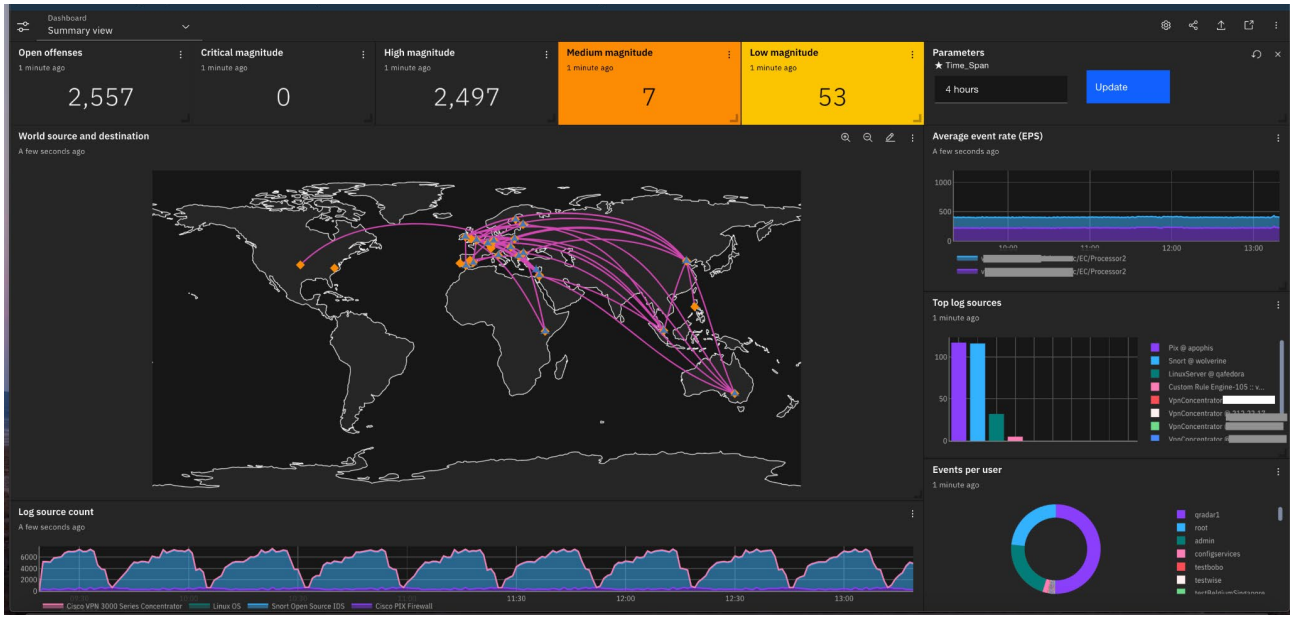


Рисунок 2. Інтерфейс SIEM системи IBM Security QRadar

На рис.3 відображено існуючі та прогнозовані витрати компаній світу на SIEM системи, що ілюструє стабільну тенденцію до збільшення фінансових вкладень у цей сегмент кібербезпеки, а також постійний попит на такі технологічні рішення.

Крім зазначених SIEM систем, є інші важливі інструменти кібербезпеки, які розширюють цей підхід до захисту та використовують ШІ для покращення безпеки інформаційних систем. Основною їхньою відмінністю є спрямованість на конкретні аспекти захисту та розширені можливості автоматизації для підвищення рівня безпеки інформаційних систем. Серед них можна виокремити:

Security Orchestration, Automation, and Response (SOAR). Це система, яка поєднує координацію, автоматизацію та реагування на події у сфері кібербезпеки, що сприяє підвищенню ефективності реагування на загрози та оптимізації процесів безпеки.

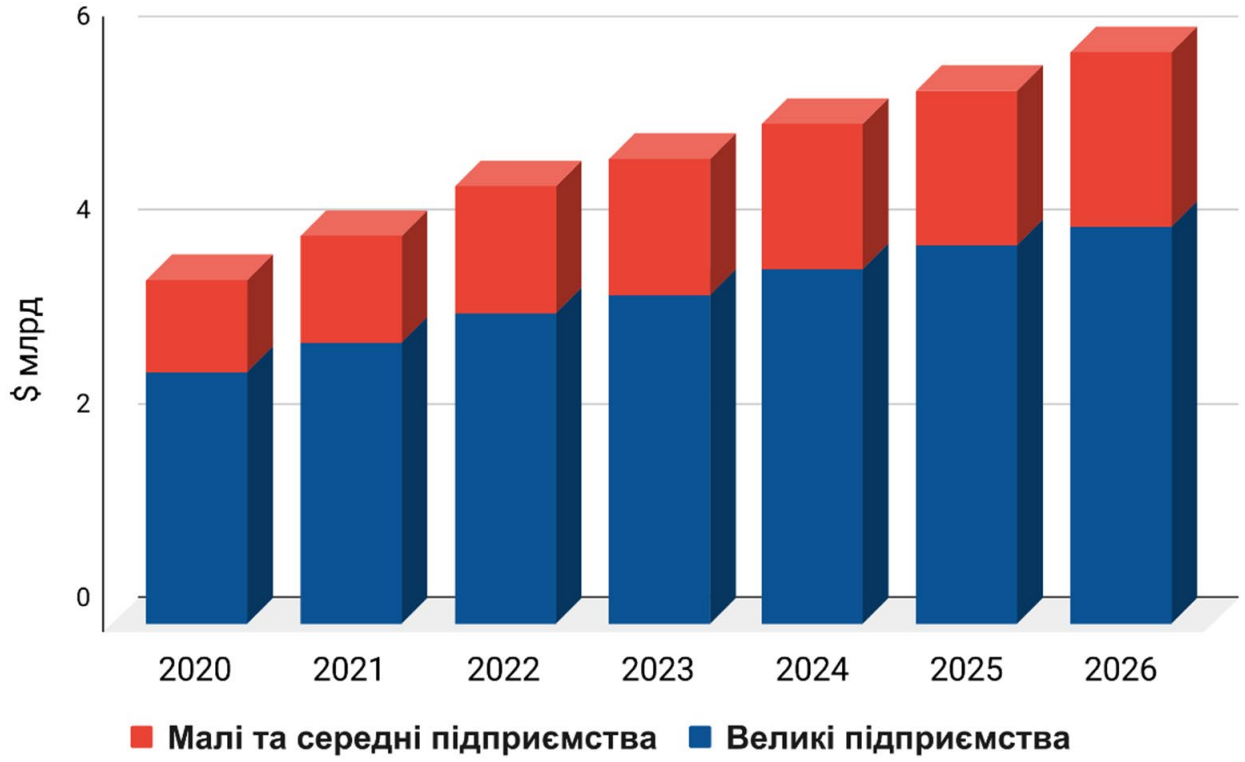


Рисунок 3. Існуючі та прогнозовані витрати підприємств на SIEM з 2020-го по 2026 роки

Endpoint Detection and Response (EDR). Це система захисту, спрямована на виявлення та реагування на загрози на рівні кінцевих точок у мережі, таких як комп'ютери, ноутбуки, сервери та інші пристрої, шляхом виявлення та аналізування аномальних активностей.

User and Entity Behavior Analytics (UEBA). Це система, яка використовується для аналізування поведінки користувачів та сутностей в інформаційних системах з метою виявлення аномалій у їхній активності для ідентифікації потенційних кіберзагроз.

Ці системи доповнюють можливості SIEM, розширюючи спектр інструментів для виявлення, аналізування та реагування на кіберзагрози в різних аспектах інформаційної безпеки. Вони розширюють можливості управління безпекою, надаючи додаткові функціональні можливості, такі як виявлення аномальних активностей в мережі, автоматизація рутинних процесів і застосування ШІ для виявлення складних загроз. Таке поєднання інструментів формує ефективну та розширену безпекову архітектуру, що забезпечує високий рівень захисту від кібератак у сучасному кіберпросторі.

Отже, розглянувши зазначені системи, можна дійти висновку, що використання ШІ широко застосовується та є необхідною складовою сучасних технологічних рішень у сфері кібербезпеки.

Незважаючи на переваги використання ШІ у сфері кібербезпеки, їхній розвиток супроводжується низкою викликів та складнощів, з якими ми потенційно можемо стикнутися у цій сфері. Розглянемо деякі з них.

Недостатня точність може призвести до недооцінювання або переоцінювання загроз, а також до збільшення кількості помилкових спрацьовувань тривог, що впливає на роботу аналітиків та загрожує ефективності системи.

Невизначеність в поведінці загроз ускладнює виявлення та протидію кіберзлочинцям,

які постійно розвивають нові методи та техніки для обходу захисту.

Брак доступу до відповідних даних може ускладнити навчання та знизити їхню ефективність, а зростання використання ШІ може призвести до залежності систем від його роботи, що збільшить їхню вразливість до атак.

Етичні питання та проблеми конфіденційності, зокрема у зв'язку зі збиранням та обробленням особистих даних користувачів, також потребують уваги та вирішення.

Розглядаючи роль ШІ у сфері кібербезпеки, важливо зауважити, що він відіграє двояку роль у майбутньому цієї галузі. З одного боку, він беззаперечно сприяє покращенню систем захисту, забезпечуючи більш ефективне виявлення атак та запобігання їм. З іншого боку, зростання кількості атак, для проведення яких використовується ШІ, а також проблеми, пов'язані з конфіденційністю, становлять серйозні виклики для кібербезпеки. У зв'язку із цим усі ці аспекти потребують уважного аналізування та розроблення відповідних стратегій для їх вирішення з метою забезпечення ефективної та надійної безпеки у кіберпросторі.

Перспективи розвитку у сфері кібербезпеки з використанням ШІ є багатообіцяючими. З розвитком технологій та постійним вдосконаленням їхнього рівня можна очікувати подальшого створення більш точних та швидких методів виявлення кіберзагроз, що сприятиме зростанню ефективності систем захисту.

Однією з головних перспектив є розвиток автономних систем інтелектуального захисту, які здатні адаптуватися до нових видів загроз та атак без прямого втручання операторів. Такі системи зможуть швидше та більш ефективно реагувати на зміни у кіберпросторі та запобігати потенційним атакам.

Іншою перспективою є посилення інтеграції ШІ з іншими технологіями кібербезпеки, такими як квантові обчислення та блокчейн. Це дозволить створити більш комплексні та надійні системи захисту, які зможуть ефективно реагувати на сучасні та майбутні виклики у кібербезпеці.

Крім того, важливою перспективою є розвиток стандартів та регулювань у сфері кібербезпеки, що стимулюватиме інновації та забезпечить високий рівень безпеки в інтернеті речей (IoT), хмарних сервісах та інших сучасних технологічних сферах.

Упровадження ШІ в діяльність Збройних Сил України відкриває перспективи для підвищення рівня їхньої готовності та ефективності застосування в умовах сучасних воєнних конфліктів. Ця інноваційна технологія дає можливість оптимізувати процеси планування та проведення військових операцій, забезпечуючи точність ухвалення відповідних рішень та миттєве реагування на різкі зміни оперативної обстановки. Також використання ШІ сприяє зміцненню кіберзахисту Збройних Сил України, захищаючи їхні важливі інформаційні ресурси від кібератак та забезпечуючи стабільність роботи військових комунікаційних систем. Крім того, завдяки застосуванню ШІ можна підвищити ефективність проведення кібернавчань та симуляції для підготовки військових до різних кризових ситуацій та кіберзагроз. Отже, використання ШІ у Збройних Силах України має потенціал підвищити їхню готовність та ефективність у сучасному воєнному середовищі.

Загалом, ШІ має потенціал перетворити підхід до кібербезпеки, забезпечуючи більш адаптивні, інтелектуальні та ефективні системи захисту, які здатні впоратися зі зростаючими загрозами у цифровому світі.

Висновок (Conclusion)

Розвиток ШІ у сфері кібербезпеки відкриває значний потенціал для підвищення ефективності захисту інформації як у цивільному, так і військовому секторах. Завдяки застосуванню ШІ можна виявляти, аналізувати та реагувати на кіберзагрози швидше та більш

ефективно, забезпечуючи високий рівень захисту від сучасних кібернападів. Інтеграція ШІ у кібербезпеку також підвищує безпеку та здатність реагувати на виклики сучасного цифрового середовища.

Отже, інтеграція ШІ у сфері кібербезпеки відкриває нові можливості для забезпечення ефективного та комплексного захисту від кіберзагроз у сучасному цифровому світі, що стає ключовим фактором у забезпеченні кібербезпеки в майбутньому.

Рекомендації (Recommendations)

Подальші дослідження доцільно спрямувати на підвищення ефективності застосування ШІ в кібербезпеці для точного виявлення та аналізування кіберзагроз, розробки адаптивних систем безпеки та вивчення можливостей прогнозування майбутніх загроз і розробки стратегій щодо запобігання їм.

Подяки (Acknowledgments)

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Hryshchuk, R., Zhovnovatiuk, R., & Nosova, H. (2019). Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. *Сучасні інформаційні технології у сфері безпеки та оборони, 36(3)*, 53–58.
2. Когут, Ю. І. (2022). *Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології)*. Консалтингова компанія “СІДКОН”.
3. Барабаш, О. В., Грищук, Р. В., Молодецька-Гринчук, К. В., & Молодецкая-Гринчук, К. В. (2018). *Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів*.
4. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global.
5. Онищенко, Ю. М., Каланча, А. А., & Гельдт, С. В. (2023, February). Застосування штучного інтелекту у сфері кібербезпеки. In *The 8th International scientific and practical conference “Trends, theories and ways of improving science”(February 28–March 03, 2023) Madrid, Spain. International Science Group. 2023.* 565 p. (p. 544).
6. ГУРЖІЙ, С. (2023). Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. *Інформація і право, 4 (47)*, 207–216.
7. ГОЛУБЕНКО, О. І., ЛЕМЕШКО, А. В., ПОЛІЩУК, А. Р., КУЗЬМЕНКО, М. В., & ДЕГТЯРЬОВ, Є. О. (2023). ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ. *ITSynergy*, *(2)*, 71–81.
8. Устименко, В. О., & Олішевський, І. Г. (2022). *Перспективи застосування технологій штучного інтелекту в сфері кібербезпеки*.
9. Опірський, І., Сусукайло, В., & Василишин, С. (2023). Дослідження можливостей використання чатботів зі штучним інтелектом для дослідження журналів подій. *Захист інформації, 24(4)*, 177–183.
10. Солдатова, М. О., Вітюк, А. Є., Мартинюк, А. С., & Чернобородюк, В. Д. (2022, April). ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ. In *The 9 th International scientific and practical conference “Innovations and prospects of world science”(April 28-30, 2022) Perfect Publishing, Vancouver, Canada. 2022.* 724 p. (p. 256).
11. Inci, S. (2023, 5 травня). The Best 10 SIEM Tools for 2023. *Medium*.

https://medium.com/@sedatinci1001/the-most-popular-10-siem-tools-b36f86d9fc7a
12. Юшко, А. В., & Шевчук, Р. П. (2020). *Аналіз систем управління подіями інформаційної безпеки*.

References

1. Hryshchuk, R., Zhovnovatiuk, R., & Nosova, H. (2019). Hybrid threats in cyberspace: factors influencing the nature of emergence. *Modern Information Technologies in the Sphere of Security and Defence, 36(3)*, 53–58.
2. Kohut, Y. I. (2022). *Cyberwarfare, cyberterrorism, cybercrime (concepts, strategies, technologies)*. Sidcon Consulting Company.
3. Barabash, O. V., Hryshchuk, R. V., Molodetska-Grynchuk, K. V., & Molodetska-Grynchuk, K. V. (2018). *Identification of threats to the information security of the state in the content of textual content of social Internet services*.
4. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global.
5. Onishchenko, Y. M., Kalancha, A. A., & Geldt, S. V. (2023, February). Application of artificial intelligence in the field of cybersecurity. In *The 8th International scientific and practical conference "Trends, theories and ways of improving science" (February 28–March 03, 2023) Madrid, Spain. International Science Group. 2023*. 565 p. (p. 544).
6. GURZHIY, S. (2023). Features of the use of artificial intelligence in cybersecurity issues. *Information and Law*, 4 (47), 207–216.
7. GOLUBENKO, O.I., LEMESHKO, A.V., POLISCHUK, A.R., KUZMENKO, M.V. & DEGTYAREV, E.O. (2023). RESEARCH OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY. *ITSynergy, (2)*, 71–81.
8. Ustymenko, V. O., & Olishevskyi, I. G. (2022). *Prospects for the application of artificial intelligence technologies in the field of cybersecurity*.
9. Opirskyi, I., Susukailo, V., & Vasylyshyn, S. (2023). Investigation of the possibilities of using artificial intelligence chatbots for the study of event logs. *Information Protection, 24(4)*, 177–183.
10. Soldatova, M. O., Vityuk, A. E., Martyniuk, A. S., & Chernoborodyuk, V. D. (2022, April). In *The 9th International scientific and practical conference "Innovations and prospects of world science" (April 28-30, 2022) Perfect Publishing, Vancouver, Canada. 2022.* 724 p. (p. 256).
11. Inci, S. (2023, 5 May). The Best 10 SIEM Tools for 2023. *Medium*. https://medium.com/@sedatinci1001/the-most-popular-10-siem-tools-b36f86d9fc7a
12. Yushko, A. V., & Shevchuk, R. P. (2020). *Analysis of information security event management systems*.

Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 2 No. 1 (2024)

Artificial Intelligence in the Sphere of Cybersecurity: Innovations, Challenges, and Development Prospects

Roman Pantiushenko
Leading Researcher of the Research and Testing Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: prvm79@gmail.com
ORCID: 0000-0002-9301-9389

Yuliia Chaika
Head of Research Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: jul.seagull@gmail.com
ORCID: 0009-0002-4342-3313

Abstract. The relevance of the study is due to the need for effective protection of information systems in the face of ever-growing cyber threats. In the modern digital world, where cyberattacks are becoming increasingly complex and widespread, the use of artificial intelligence in cybersecurity is extremely relevant. The problem of cybersecurity is becoming increasingly important and conducting relevant research is becoming a necessary aspect of ensuring security in the digital space.

In this context, we propose an article that examines the role of artificial intelligence, innovations, challenges, and prospects of its development in the sphere of cybersecurity. Additionally, it explores the utilization of artificial intelligence for automating processes of detecting, analysing, and responding to cyber threats, and its practical significance for enhancing security levels in the digital space and the effectiveness of cyber threat protection.

The main approaches for this study are trend analysis and expert assessments, which allow for a comprehensive review of the directions of artificial intelligence development in the field of cybersecurity, the benefits and challenges of its implementation, as well as potential opportunities and threats to information security.

The article discusses advanced security information and event management systems designed to collect, analyse and respond to cyber threats and other systems aimed at specific aspects of protection and expanding automation capabilities to improve the security level of information systems.

The materials of the article are of theoretical value for further scientific research on the use of artificial intelligence in the sphere of cybersecurity and reflect important features of its influence on this area. This research can contribute not only to deepening the understanding of the theoretical aspects of the use of artificial intelligence in cybersecurity but also to identifying specific practical applications and innovations that will help improve protection against cyber threats in the future.

Keywords: artificial intelligence, cyberspace, big data, Security Information and Event Management.