УДК 004.42:005.8
DOI https://doi.org/10.32782/IT/2025-1-2

Володимир БОГОМ'Я
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0003-4403-3130*

Валентин ГАЛУНЬКО
доктор філософії в галузі права, доцент кафедри адміністративного права, інтелектуальної власності та цивільно-парових дисциплін, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-8133-6766*

Бібліографічний опис статті: Богом'я, В., Галунько, В. (2025). Захист програмного забезпечення роль штучного інтелекту в епоху кіберзагроз. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 13–17, doi: https://doi.org/10.32782/IT/2025-1-2

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ЕПОХУ КІБЕРЗАГРОЗ

Мета роботи. *Дослідження ролі штучного інтелекту в кібербезпеці, зокрема його впливу на захист програмного забезпечення в умовах зростання кіберзагроз. Приділяється увага до людського фактору, який є однією з основних причин кіберінцидентів, а також розглянуто етичні, правові та технічні аспекти інтеграції штучного інтелекту в системи кібербезпеки.*

Методологія. *В основу дослідження покладено системний підхід, що передбачає аналіз наукових досліджень, проведених вітчизняними та міжнародними дослідниками в галузі кібербезпеки та штучного інтелекту. Методи порівняльного аналізу були використані для оцінки ефективності різних технологій, таких як машинне навчання, нейронні мережі та обробка природної мови. Статистичні дані та прогнози щодо витрат на інформаційну безпеку взяті з міжнародних джерел, таких як Statista.*

Наукова новизна. *Полягає в комплексному аналізі ролі штучного інтелекту в безпеці програмного забезпечення в контексті сучасних кіберзагроз. Визначення потенціалу штучного інтелекту для компенсації людського фактору, який може спричиняти кіберінциденти. Наголошується на необхідності розробки нових стратегій, що поєднують технічні, правові та освітні заходи для ефективного використання штучного інтелекту у сфері кібербезпеки. Визначено ключові виклики, серед яких вразливість штучного інтелекту до атак, етичні дилеми та необхідність забезпечення прозорості процесів прийняття рішень.*

Висновки. *Штучний інтелект є потужним інструментом для підвищення ефективності кібербезпеки, оскільки він може автоматизувати процес виявлення, аналізу та реагування на загрози. Використання машинного навчання, нейронних мереж та алгоритмів обробки природної мови може значно підвищити рівень безпеки програмного забезпечення; автоматизуючи рутинні завдання та аналізуючи великі обсяги даних, штучний інтелект може компенсувати людський фактор, який є однією з основних причин кіберінцидентів. Ефективність штучного інтелекту залежить від якості даних, алгоритмів та інтеграції з існуючими системами. Для подальшого вдосконалення необхідно розробляти адаптивні системи, здатні безперервно навчатися та оновлюватися. Використання штучного інтелекту в кібербезпеці вимагає комплексного підходу, який враховує технічні, правові та етичні аспекти. Отже, необхідно забезпечити прозорість процесів прийняття рішень, захистити конфіденційність даних і запобігти зловживанню технологіями. Сферами, де очікуються подальші дослідження, є розробка нових стратегій і технологій для протидії сучасним кіберзагрозам та інтеграція штучного інтелекту з інноваційними інфраструктурами, такими як Інтернет речей (IoT) і великі дані (Big Data).*

Ключові слова: *адаптивні системи, захист, кібербезпека, кіберзагрози, програмне забезпечення, штучний інтелект.*

Volodymyr BOHOMYA
Doctor of Technical Sciences, Professor, Professor at the Department of Cyber Security, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, bog2603@ukr.net
***ORCID:** 0000-0003-4403-3130*

Valentyn HALUNKO
PhD in Law, Associate Professor at the Department of Administrative Law, Intellectual Property and Civil-Law Disciplines, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, valentinvalentin0987@gmail.com
***ORCID:** 0000-0002-8133-6766*

To cite this article: Bohomya, V., Halunko, V. (2025). Zakhyst prohramnoho zabezpechennia rol shtuchnoho intelektu v epokhu kiberzahroz [Software protection the role of artificial intelligence in the age of cyber threats]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 13–17, doi: https://doi.org/10.32782/IT/2025-1-2

SOFTWARE PROTECTION THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE AGE OF CYBER THREATS

Objective. *To study the role of artificial intelligence in cybersecurity, in particular, its impact on software protection in the face of growing cyber threats. Attention is paid to the human factor, which is one of the main causes of cyber incidents, and the ethical, legal and technical aspects of integrating artificial intelligence into cybersecurity systems are considered.*

Methodology. *The study is based on a systematic approach that involves the analysis of scientific research conducted by domestic and international researchers in the field of cybersecurity and artificial intelligence. Comparative analysis methods were used to assess the effectiveness of various technologies, such as machine learning, neural networks, and natural language processing. Statistics and forecasts on information security costs were taken from international sources such as Statista.*

Scientific novelty. *It consists in a comprehensive analysis of the role of artificial intelligence in software security in the context of modern cyber threats. Determining the potential of artificial intelligence to compensate for the human factor that can cause cyber incidents. The author emphasizes the need to develop new strategies that combine technical, legal and educational measures for the effective use of artificial intelligence in the field of cybersecurity. The key challenges are identified, including the vulnerability of artificial intelligence to attacks, ethical dilemmas, and the need to ensure transparency in decision-making processes.*

Conclusions. *Artificial intelligence is a powerful tool for improving cybersecurity efficiency, as it can automate the process of detecting, analyzing, and responding to threats. The use of machine learning, neural networks, and natural language processing algorithms can significantly improve software security; by automating routine tasks and analyzing large amounts of data, artificial intelligence can compensate for the human factor, which is one of the main causes of cyber incidents. The effectiveness of artificial intelligence depends on the quality of data, algorithms, and integration with existing systems. For further improvement, it is necessary to develop adaptive systems that can continuously learn and update. The use of artificial intelligence in cybersecurity requires a comprehensive approach that takes into account technical, legal, and ethical aspects. Thus, it is necessary to ensure transparency of decision-making processes, protect data privacy, and prevent misuse of technology. Areas where further research is expected include the development of new strategies and technologies to counter modern cyber threats and the integration of AI with innovative infrastructures such as the Internet of Things (IoT) and Big Data.*

Key words: *adaptive systems, artificial intelligence, cyber threats, cybersecurity, protection, software.*

Актуальність проблеми. Кіберзагрози стають все більш складними та поширеними забезпечення кібербезпеки є одним із актуальних питань сьогодення. Зростання кількості кібератак, таких як фішинг, шкідливе програмне забезпечення та атаки соціальної інженерії, вимагає нових підходів до захисту інформаційних систем захисту програмного забезпечення. Штучний інтелект може стати важливим інструментом у протидії цим загрозам завдяки в своїй здатності швидко аналізувати великі обсяги даних, виявляти аномалії та автоматизувати процеси реагування.

Поряд з перевагами, використання штучного інтелекту в кібербезпеці також створює нові виклики, такі як вразливість до атак, етичні та правові питання, а також необхідність забезпечення прозорості рішень. Це робить інтеграцію штучного інтелекту в кібербезпеку надзвичайно важливою, оскільки вона вимагає комплексного підходу, що враховує технічні, правові та соціальні аспекти в цілому.

Аналіз останніх досліджень і публікацій. Дослідження базується на працях вітчизняних науковців: Р. О. Іваненко, А. А. Кісь, О. М. Лунгол, В. А. Савченко, В. В. Симонова, О. Д. Шаповаленко, О. Б. Ящика.

Метою статті. Є дослідження і значення штучного інтелекту в кібербезпеці, захисту програмного забезпечення, проаналізувати здатність штучного інтелекту протидіяти кіберзагрозам та визначено основні виклики і перспективи використання штучного інтелекту в захисті програмного забезпечення та інформаційних систем.

Виклад основних положень. Підходи значення штучного інтелекту в захисту програмного забезпечення кіберзагрози в нашому житті не представити масштабністю значення його використання, будь-то на основі визначених позитивних цілей, чи в корисливих зі злим умислом з метою завдавати шкоди програмному забезпеченню. Тому, штучний інтелект є частиною важливості ролі в кібербезпеці. Потрібно також, враховувати людський фактор в забезпечені кібербезпеки програмного забезпечення, тобто штучний інтелект допоможе оцінювати помилки чим, і забезпечить можливість визначити певні ризики ефективно запобігати та вирішення масштабних загроз.

Штучний інтелект – це широкий термін, який описує процес надання машинам можливості використовувати міркування і логіку для вирішення проблем, імітуючи людський інтелект. Штучний інтелект в кібербезпеці базується на тому ж принципі і використовує швидкість і обчислювальну потужність штучний інтелект для створення протоколів кібербезпеки, які передбачають, ідентифікують і пом'якшують загрози. На людські помилки припадає понад 80 % кіберінцидентів, і штучний інтелект може заповнити цю прогалину, автоматизуючи завдання і розпізнаючи закономірності, невидимі для людського ока (Корпоративна кібербезпека, 2025).

Наприклад, алгоритми машинного навчання можуть класифікувати зловмисні електронні атаки та виявляти схожі характеристики, про які працівники можуть не знати. Такі інструменти, як обробка природної мови, можуть виявляти спроби фішингу та шкідливе програмне забезпечення, витягуючи ключові слова. Продуктивний штучний інтелект перетинається з кібербезпекою, аналізуючи і навчаючись на великих обсягах даних, виявляючи закономірності і приймаючи обґрунтовані рішення про те, як реагувати на потенційні загрози. Хоча він може вирішити лише деякі проблеми кібербезпеки. Штучний інтелект відіграє важливу роль у підтримці ініціатив з кібербезпеки та дотриманні нормативних вимог. Переваги використання штучного інтелекту для кібербезпеки З розвитком технологій штучний інтелект дедалі ширше застосовується у сфері кібербезпеки може допомогти організаціям швидко та ефективно виявляти загрози та управляти ними (Корпоративна кібербезпека, 2025).

Наприклад витрати на інформаційну безпеку та управління ризиками має таку статистику на платформі даних бізнес-аналітики з великою колекцією статистичних даних Statista про витрати на інформаційну безпеку та управління ризиками в усьому світі у 2024 та 2028 роках. Згідно з цим, глобальні витрати на інформаційну безпеку та управління ризиками становитимуть 210 мільярдів доларів а, що до 2028 року витрати на інформаційну безпеку та управління ризиками перевищать 310 мільярдів доларів (Information security and risk management spending worldwide in 2024 and 2028, 2025).

Отже, зростання витрат на інформаційну безпеку та управління ризиками підкреслює важливість інтеграції штучного інтелекту для ефективного протидіяння масштабним загрозам. Таким чином, штучний інтелект стане невід'ємною частиною сучасних підходів до кібербезпеки.

У глобальному середовищі, що характеризується постійно зростаючою кількістю кібератак, потреба в більш ефективних практиках та обізнаності щодо кібербезпеки. Про це свідчить значне зростання світової індустрії програмного забезпечення для забезпечення безпеки в останні роки. Кіберзлочинність швидко стає одним з найнебезпечніших і найшкідливіших злочинів. Інформаційна безпека стала фундаментальним елементом як для бізнесу, так і для приватних (Security software – statistics & Facts, 2025).

На думку Савченка В.А. та Шаповаленка О.Д. застосування технологій штучного інтелекту в кібербезпеці підкреслює актуальність використання штучного інтелекту для захисту інформації в умовах відсутності загальних концепцій застосування в цій сфері. Особлива увага приділяється машинному навчанню, нейронним мережам та обробці природної мови, підкреслюючи їх потенціал для аналізу даних, виявлення аномалій та автоматизації процесів безпеки. Подальші дослідження цих технологій в контексті адаптивних програмних систем безпеки можуть призвести до розробки більш ефективних способів протидії сучасним кіберзагрозам, враховуючи необхідність безперервного навчання та адаптації систем штучного інтелекту (Савченко, Шаповаленко, 2020).

Авторка Лунгол О.М. зосереджує огляд методів для аналізу великих обсягів даних у кібербезпеці за допомогою штучного інтелекту. Увагу на зростаючій складності кіберзагроз, таких як фішинг, шкідливе програмне забезпечення та атаки соціальної інженерії, які вимагають використання нових технологій для ефективного захисту інформаційних систем. Зокрема, машинне навчання та глибоке навчання демонструють великий потенціал у виявленні аномалій, прогнозуванні загроз та автоматизації

процесів реагування на інциденти. Ключові сфери, розглянуті в цьому дослідженні, включають аналіз великих даних, моделювання загроз, інтеграцію штучного інтелекту з Інтернетом речей і великими даними, а також етичні та правові аспекти використання штучного інтелекту в кібербезпеці. Однак використання штучного інтелекту також стикається з такими проблемами, як забезпечення прозорості рішень і захист від зловживань цими технологіями. Підкреслюючи, що штучного інтелекту є потужним інструментом для підвищення ефективності кібербезпеки, але для розробки нових стратегій і технологій протидії загрозам у цифрову епоху необхідні додаткові дослідження (Лунгол, 2024).

Отже, штучний інтелект відіграє важливу роль у сучасній кібербезпеці, дозволяючи автоматизувати виявлення загроз та реагування на них. Однак для ефективного та безпечного використання необхідно враховувати етичні, правові та технічні міркування.

Ящика О. Б., Сімонова В. В. та Іваненка Р. О. проаналізували забезпечення кібербезпеки в еру штучного інтелекту та технологічних підходів і стратегій захисту інформації та проаналізовано Стратегію кібербезпеки України, схвалену Указом Президента України від 26 серпня 2021 р. (Верховна Рада України, 2025). Підкреслюючи, що з одного боку, значно покращує якість життя за рахунок автоматизації рутинних завдань та надає нові можливості для інновацій, але, з іншого боку, створює нові ризики для інформаційної безпеки. Та, викликає занепокоєння щодо конфіденційності даних, оскільки технологія може стати інструментом для швидких і масштабних кібератак. Основні загрози пов'язані з системними вразливостями, вторгненням у приватне життя та різними видами атак. Вони пропонують використовувати інструменти на основі штучного інтелекту для автоматизації рутинних завдань з кібербезпеки, звільняючи таким чином час експертів для вирішення більш складних проблем. Однак для ефективного використання необхідно запровадити нове законодавство, яке б регулювало його функціонування та забезпечувало прозорість у прийнятті рішень системами штучного інтелекту (Ящик, Симонов, Іваненко, 2024).

Отже, потенціал штучного інтелекту може бути використаний для підвищення кібербезпеки, але для цього потрібен комплексний підхід до захисту інформації.

Авторка Кісь А. А. розглядає проблеми безпеки комп'ютерних систем при використанні штучного інтелекту зазначає, що штучний інтелект, хоча й має великий потенціал але, і сам створює нові ризики для кібербезпеки, зокрема через вразливість до атак підробки даних, вірусів та дій хакерів. Для захисту систем штучного інтелекту запропоновано практики, такі як захист даних, використання безпечних алгоритмів, моніторинг, контроль доступу та підготовка до кібератак. Штучний інтелект має як позитивний вплив, покращуючи кібербезпеку, так і негативний, посилюючи загрози. Оскільки штучний інтелект пронизує всі галузі людського життя, для кожного вкрай важливо знати про ризики безпеки та найкращі методи їх усунення чи мінімізації вважає автор з чим можна частково погодитись, що дійсно сам штучний інтелект може стати загрозою для кібербезпеки (Кісь, 2023).

Висновки. Штучний інтелект може стати важливим інструментом у боротьбі з кіберзагрозами завдяки своїй здатності автоматизувати процес виявлення, аналізу та реагування на загрози. Використання машинного навчання, нейронних мереж та алгоритмів обробки природної мови значно підвищує рівень безпеки програмного забезпечення, дозволяючи ефективно виявляти аномалії, класифікувати зловмисні атаки та прогнозувати потенційні ризики.

Штучний інтелект може допомогти компенсувати людський фактор, який є причиною кіберінцидентів. Завдяки автоматизації рутинних завдань та аналізу великих обсягів даних можна мінімізувати людські помилки та досягти швидшого і точнішого реагування на загрози.

Однак, незважаючи на значні переваги штучного інтелекту, він не є панацеєю від усіх проблем кібербезпеки, оскільки його ефективність залежить від якості даних, алгоритмів та інтеграції з існуючими системами. Зокрема, важливо розробляти адаптивні системи, здатні постійно навчатися та оновлюватися відповідно до загроз, що динамічно змінюються.

Крім того, слід враховувати етичні, правові та технічні аспекти використання штучного інтелекту, такі як забезпечення прозорості у прийнятті рішень, захист конфіденційності даних і запобігання зловживанню такими технологіями. В чому є перспективність досліджувати надалі цю тематику.

ЛІТЕРАТУРА:

1. Кісь А. А. Безпека комп'ютерних систем при використанні технологій штучного інтелекту. *Scientific Collection "InterConf"*. 2023. № 162. С. 246–248. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/4066

2. Корпоративна кібербезпека: Роль ШІ у захисті даних. *BDO Copyright*. 2025. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection

3. Лунгол О. М. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Науковий журнал*. 2024. № 1(25). С. 379–389. DOI: https://doi.org/10.28925/2663-4023.2024.25.379389

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України; Стратегія від 26.08.2021 № 447/2021. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/447/2021

5. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації*. 2020. № 4(44). С. 6–11. DOI: https://doi.org/10.31673/2409-7292.2020.040611

6. Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації. *БізнесІнформ*. 2024. № 1. С. 81–86. DOI: https://doi.org/10.32983/2222-4459-2024-1-81-86

7. Information security and risk management spending worldwide in 2024 and 2028. *Statista*. 2025. URL: https://www.statista.com/statistics/1345127/information-risk-management-security-spending-worldwide/#statisticContainer

8. Security software – statistics & Facts. *Statista*. 2025. URL: https://www.statista.com/topics/2208/security-software/#topicOverview

REFERENCES:

1. Kis, A. A. (2023). Bezpeka kompiuternykh system pry vykorystanni tekhnolohii shtuchnoho intelektu [Safety of computer systems when using artificial intelligence technologies]. *Scientific Collection "InterConf"*, 162, 246–248. Retrieved from: https://archive.interconf.center/index.php/conference-proceeding/article/view/4066 [in Ukrainian].

2. Korporatyvna kiberbezpeka: Rol ShI u zakhysti danykh [Corporate cybersecurity: The role of AI in data protection]. (2025). *BDO Copyright*. Retrieved from: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection [in Ukrainian].

3. Lunhol, O. M. (2024). Ohliad metodiv ta stratehii kiberbezpeky zasobamy shtuchnoho intelektu [Review of methods and strategies of cybersecurity using artificial intelligence]. *Naukovyi Zhurnal*, 1(25), 379–389. https://doi.org/10.28925/2663-4023.2024.25.379389 [in Ukrainian].

4. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy; Stratehiia vid 26.08.2021 № 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine»: Decree of the President of Ukraine; Strategy dated August 26, 2021 No. 447/2021]. (2025). Baza danykh "Zakonodavstvo Ukrainy" / Verkhovna Rada Ukrainy. Retrieved from: https://zakon.rada.gov.ua/go/447/2021 [in Ukrainian].

5. Savchenko, V. A., & Shapovalenko, O. D. (2020). Osnovni napriamy zastosuvannia tekhnolohii shtuchnoho intelektu u kiberbezpetsi [Main directions of application of artificial intelligence technologies in cybersecurity]. *Suchasnyi Zakhyst Informatsii*, 4(44), 6–11. https://doi.org/10.31673/2409-7292.2020.040611 [in Ukrainian].

6. Yashchyk, O. B., Symonov, V. V., & Ivanenko, R. O. (2024). Zabezpechennia kiberbezpeky v eru shtuchnoho intelektu: analiz tekhnolohichnykh pidkhodiv ta stratehii dlia zakhystu informatsii [Ensuring cybersecurity in the era of artificial intelligence: Analysis of technological approaches and strategies for information protection]. *BiznesInform*, 1, 81–86. https://doi.org/10.32983/2222-4459-2024-1-81-86 [in Ukrainian].

7. Information security and risk management spending worldwide in 2024 and 2028. (2025). *Statista*. Retrieved from: https://www.statista.com/statistics/1345127/information-risk-management-security-spending-worldwide/#statisticContainer

8. Security software – statistics & facts. (2025). *Statista*. Retrieved from: https://www.statista.com/topics/2208/security-software/#topicOverview