УДК 004.8
DOI: https://doi.org/10.53920/ITS-2023-2-5

Олександр Іванович ГОЛУБЕНКО,
кандидат технічних наук, доцент,
т. в. о. завідувача кафедри комп'ютерних наук
та інженерії програмного забезпечення,
ЗВО «Міжнародний науково-технічний університет
імені академіка Юрія Бугая»
ORCID ID: 0000-0002-1776-5160
Андрій Вікторович ЛЕМЕШКО,
доктор філософії, доцент,
доцент кафедри комп'ютерної інженерії
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-8003-3168
Андрій Русланович ПОЛІЩУК,
магістр кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0009-0000-7965-6499
Максим Володимирович КУЗЬМЕНКО,
магістр кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0009-0009-8146-8038
Євген Олександрович ДЕГТЯРЬОВ,
магістр кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0009-0002-7219-9437

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Схема штучного інтелекту на ринку кібербезпеки допомагає організаціям контролювати, виявляти, повідомляти про кіберзагрози та протидіяти їм, щоб зберегти конфіденційність інформації. Зростаюча обізнаність людей, прогрес в інформаційних технологіях, модернізація розвідувальних і поліцейських рішень для роботи, а також збільшення обсягу знань, зібраних з численних джерел, вимагають використання надійних і вдосконалених рішень кібербезпеки в усіх згаданих галузях. Збільшення інтенсивності та складності кібератак акцентує увагу на потребі розвитку кіберсистем, підтриманих штучним інтелектом. Ростуть

численність та масштаб кіберінцидентів на глобальному рівні, що заставляє організації активізувати заходи захисту своєї інформації. Мотивація атак може бути різноманітною: від політичної конкуренції до крадіжки міжнародної інформації та радикальних ідеологічних мотивацій.

Ключові слова: *штучний інтелект, кібербезпека, комп'ютерна система, алгоритм, машинне навчання, інтернет речей, мережа, середовище.*

Oleksandr GOLUBENKO
Candidate of technical sciences, associate professor,
Temporary acting head of the Department
of Computer Science and Software Engineering,
IHE «Academician Yuri Bugay international science
and technical university»
Andrii LEMESHKO
Doctor of Philosophy, Associate Professor,
associate professor of the department of computer engineering,
State University of information and communication technologies
Andrii POLISHCHUK,
Maksym KUZMENKO,
Eugene DEGTYAREV
Masters of computer engineering department,
State University of information and communication technologies

RESEARCH ON THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

The AI framework in the cybersecurity market helps organizations monitor, detect, report, and counter cyber threats to preserve information privacy. The growing awareness of people, the progress in information technology, the modernization of intelligence and police work solutions, as well as the increase in the amount of knowledge collected from numerous sources, require the use of reliable and advanced cyber security solutions in all the mentioned industries. The increase in the intensity and complexity of cyber-attacks emphasizes the need for the development of cyber systems supported by artificial intelligence. The number and scale of cyber incidents at the global level are growing, forcing organizations to step up measures to protect their information. The motivation of the attacks can be diverse: from political competition to the theft of international information and radical ideological motivations.

Keywords: *artificial intelligence, cyber security, computer system, algorithm, machine learning, Internet of Things, network, environment.*

Постановка проблеми. Сучасний конкурентний бізнес, активно використовує інноваційний підхід до організації та провадження діяльності, заснований на технологіях штучного інтелекту. Ця технологія дозволяє електронним автоматизованим системам (комп'ютерам) не лише самостійно приймати управлінські рішення, але й виявляти, аналізувати та запобігати кібератакам у режимі реального часу. Штучний інтелект в кібербезпеці стає ключовим для автоматизації захисних механізмів та стратегічного управління ризиками. Водночас, незважаючи на потенційні переваги, існує необхідність ефективно протидіяти новим кіберзагрозам, що виникають у контексті цієї інноваційної динаміки.

Аналіз останніх досліджень і публікацій. Кібербезпека відноситься до комплексу заходів, спрямованих на захист електронних даних та систем. Аналогічно до закону Мура, який передбачає зменшення розмірів компонентів інтегральних схем із збільшенням їх продуктивності, кіберзлочинці постійно покращують ефективність своїх атак, витрачаючи на це все менше коштів з часом. Важливо зауважити, що основною метою більшості кібератак є фінансова вигода [1]. За різними джерелами та оцінками, світові витрати на кібербезпеку між 2016 та 2021 роками склали понад 1 трильйон доларів. Витрати на кібербезпеку з 2016 року вже зросли більш ніж на 40 відсотків.

Мета статті – дослідження застосування штучного інтелекту для покращення кібербезпеки.

Виклад основного матеріалу дослідження. Штучний інтелект – це система, створена на основі комп'ютерних технологій, яка намагається моделювати певні аспекти людського менталітету та функціонування. Ця система може взаємодіяти з навколишнім середовищем, наприклад, розпізнавати голос та перетворювати його на різні мови, наслідуючи при цьому людські здібності. Він базується на різних науках, таких як математика, інформатика та філософія, і його головною метою є створення систем, які можуть демонструвати певні аспекти людської інтелектуальної діяльності. Термін «штучний інтелект» часто використовується для опису систем, які здатні емалювати основні функції сприйняття та розуміння, що є характерними для людського мислення рисунок 1 [2].

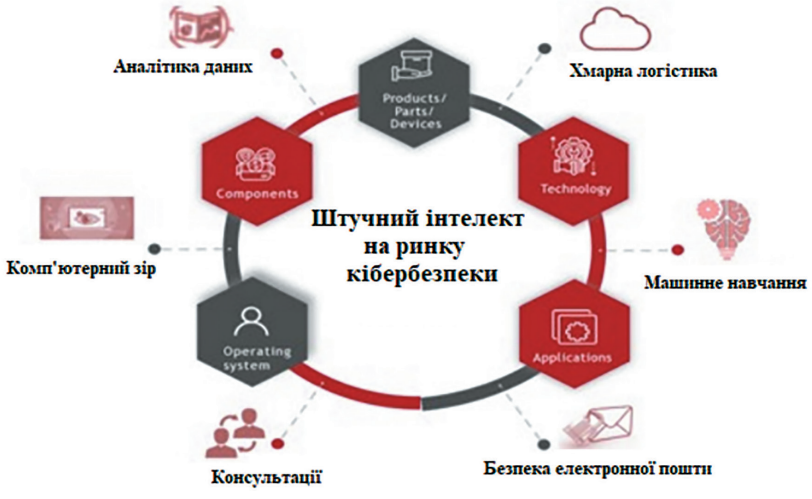

Рис. 1. Використання штучного інтелекту

Інтеграція штучного інтелекту у системи виявлення вторгнень (IDS) набуває великої актуальності. У роботі X. A. Larriva-Novo та співавторів [4] пропонуються алгоритми для покращення ефективності IDS, зокрема в контексті конкретних сценаріїв. Для цього проводиться категоризація наборів даних кібербезпеки, що дозволяє групувати їх у специфіковані категорії. В роботі розглядаються різні моделі нейронних мереж, такі як багатошарові та рекурентні, використовуються різноманітні функції активації та алгоритми навчання, щоб досягти оптимальної точності в залежності від характеристик бази даних.

Нарешті, результати були використані, щоб визначити, яка категорія набору даних про кібербезпеку є більш важливою для виявлення вторгнень і найбільш адекватної конфігурації алгоритму машинного навчання для мінімізації навантаження на обчислення. Існують також значні ризики для безпеки у взаємозв'язках, необхідних для використання певних переваг автоматизованих систем. У статті описана система виявлення вторгнень, заснована на концепціях некерованих автоматизованих систем.

Представлено модель машинного навчання безпеки на основі дерева (IntruD Tree), яка оцінює функцію безпеки на основі її

важливості та створює загальну модель виявлення вторгнень. Ця модель не тільки має точність прогнозування для непривабливих тестових випадків, вона також мінімізує комп'ютерну складність моделі, зменшуючи вимірювання функцій. Нарешті, набори даних кібербезпеки та вимірювання точності, використовуються для перевірки ефективності нашої моделі IntruDTree. Автори також порівнюють результати IntruDTree з різними традиційними, звичайними підходами машинного вчителя, такими як наївна система класифікації, логістична регресія, векторні системи підтримки та найвужчий сусід, щоб оцінити ефективність отриманої моделі безпеки.

У статті було запропоновано нейроморфний когнітивний обчислювальний підхід для системи виявлення вторгнень у мережу (IDS) кібербезпеки глибокого навчання (DL). Алгоритмічна потужність DL була поєднана зі швидкими та високоефективними нейроморфними процесорами кібербезпеки. Дані були пронумеровані для навчання за допомогою технік ретельного навчання без нагляду, які називаються автоматичним кодувальником під час процесу навчання (AE). Вагові коефіцієнти AE, створені для етапу навчання під керівництвом, використовуються як початкові вагові коефіцієнти для нейронних мереж. Остаточна вага перетворюється на дискретну вагу, синаптичну вагу та порогові значення для нервових клітин за допомогою дискретної факторизації векторів (DVF). Нарешті, згенеровані поперечні ваги, синаптичні ваги, пороги та витоки були зіставлені в поперечні смуги та нейрони. Під час контрольної точки, закодовані зразки перетворюються в центральну форму за допомогою гібридних методів кодування. Для реалізації та тестування використовували IBM Neurosynaptic Core Simulator (NSCS) і новий нейросинаптичний чіп True North. Для виявлення вторгнення в кібербезпеку нейроморфного чіпа результати тесту вказують на точність приблизно 90,12 відсотка. Крім того, автори переглянули запропоновану структуру не тільки для виявлення шкідливих пакетів, але й для класифікації цих типів атак і досягли точності 81,31%. Нейроморфна реалізація забезпечує дивовижну точність у виявленні та класифікації високопотужного виявлення мережевого вторгнення. Для виявлення вторгнення в кібербезпеку нейроморфного чіпа результати тесту вказують на точність приблизно 90,12 відсотка. Крім того, автори переглянули запропоновану структуру не тільки для виявлення

шкідливих пакетів, але й для класифікації цих типів атак і досягли точності 81,31%.

Нейроморфна реалізація забезпечує дивовижну точність у виявленні та класифікації високопотужного виявлення мережевого вторгнення. Для виявлення вторгнення в кібербезпеку нейроморфного чіпа результати тесту вказують на точність приблизно 90,12 відсотка. Крім того, автори переглянули запропоновану структуру не тільки для виявлення шкідливих пакетів, але й для класифікації цих типів атак і досягли точності 81,31%. Нейроморфна реалізація забезпечує дивовижну точність у виявленні та класифікації високопотужного виявлення мережевого вторгнення.

Технологія машинного навчання популярна в багатьох сферах, а технологія машинного навчання має багато застосувань для кібербезпеки. Приклади шкідливого програмного забезпечення включають аналіз шкідливого програмного забезпечення, зокрема виявлення зловмисного програмного забезпечення нульового дня, аналіз загроз, виявлення аномалій вторгнення та багато інших. У багатьох продуктах кібербезпеки вчені використовують виявлення машинного навчання через неефективність підходів на основі сигнатур у виявленні неденних атак або навіть незначних варіантів існуючих атак. У цьому [7] дослідженні, в якому машинне навчання є методом, автори обговорюють різні сфери кібербезпеки. Щоб маніпулювати навчанням і дослідженнями класифікації даних, автори також мають певний досвід несприятливої атаки на алгоритми машинного навчання, тому ці підходи не працюють.

Запобігання кібератакам і загрозам за допомогою ШІ. Штучний інтелект був лише різновидом комп'ютеризованої версії людського інтелекту. Те, як функціонує штучний інтелект, схоже на навчання, як це роблять люди, ітеративно знову і знову. Загроза ландшафту безсумнівно розвивається в цьому столітті. Кібер-зловмисники ґрунтуються виключно на фінансових стимулах. Але департамент знайшов новий спосіб запобігання атакам до того, як вони відбудуться, оскільки він більше не може залежати від старих звичайних методів. У цій статті [4] підкреслюється необхідність розвитку навичок кібербезпеки та те, як використання штучних нейронних мереж і алгоритмів машинного навчання може означати покращення навичок. Також включено огляд і визначення соціальної інженерії, роль, яку вона відіграє в мережі та кіберпограбуванні, а також причини та вплив на кіберзлочини.

Рекомендовано превентивні дії та потенційні рішення щодо загроз і вразливостей у соціальній інженерії, виходячи з висновків наведених у статті [5], вразливість залежить від поведінки людини, розумових імпульсів і психологічних схильностей, хоча технології допомагають зменшити вплив атак соціальної інженерії. Хоча література підтверджує інвестиційні ризики в організаційних освітніх таборах через чутливість соціальної інженерії, оптимістично можна сказати, що напади на соціальну інженерію можна зменшити.

Втрати мільярдів доларів спричинені кіберзлочинністю, збоями операційних систем, знищенням секретної інформації, порушенням безпеки мережі та секретності. Безпека комп'ютерних систем стала необхідною для мінімізації впливу та, імовірно, стримування кіберзлочинів у світлі цих злочинів, які здійснюються щодня. У статті наведена дискусія щодо останніх досягнень у використанні наборів даних кібербезпеки для оцінки систем виявлення вторгнень машинного навчання та інтелектуального аналізу даних. Встановлено, що сучасні стандарти кібербезпеки більше не є надійними, оскільки їхні бази даних більше не відповідають сучасним розробкам комп'ютерних технологій. Отже, у 2013 році було запропоновано новий набір даних ADFA Linux (ADFA-LD) для порівняння кібербезпеки, щоб відповідати поточним світовим досягненням у комп'ютерних технологіях для аналізу машинного навчання інтелектуального аналізу даних і систем виявлення вторгнень.

До ADFA-LD включено кращі визначення їхніх атрибутів. Дослідницьке співтовариство використає це дослідження, щоб відмовитися від поточних наборів даних порівняльного аналізу кібербезпеки та почати використовувати нещодавно впроваджений набір даних порівняльного аналізу для ефективної та систематичної оцінки комп'ютера та системи виявлення вторгнень інтелектуального аналізу даних.

Аналіз соціального та інтернет-трафіку важливий для ідентифікації та захисту від кіберзагроз. Розширені підходи до автоматизованого машинного навчання замінюють традиційні підходи, які повертаються до визначених вручну правил. Ця революція прискорюється завдяки масивним наборам даних, які забезпечують моделі машинного навчання з вищою ефективністю. У статті [8] аналізується нещодавнє аналітичне дослідження кібертрафіку

через соціальні мережі та Інтернет, використовуючи набір загальних принципів схожості, відношення та колективних індикацій у контексті моделі, керованої даними. Це не поодиноке бажання, а загальне використання різноманітних мереж і соціальних рухів пояснюється цим. Потоки також мають низку функцій, зокрема фіксований розмір і багато повідомлень між джерелом і одержувачем. Стаття представляє сучасну методологію дослідження та застосування в Інтернет-безпеці, керовані даними соціального та Інтернет-трафіку (DDCS). Підхід до DDCS включає три елементи: збір даних для кібербезпеки, розробку кібербезпеки та моделювання кібербезпеки. Також обговорюються виклики та майбутні шляхи.

Кібератаки становлять серйозну загрозу національній безпеці країні. Сьогодні зростає кількість шкідливих інструментів, які здійснюють численні кібератаки. Знання та інструменти для стримування та пом'якшення атак були заплановані для розвідки кіберзагроз (CTI) і порталу аналізу зловмисного програмного забезпечення. Однак поточні портали CTI та аналізи зловмисного програмного забезпечення звинувачують у надто швидкому реагуванні, оскільки вони залежать від попередніх кібератак для збору даних. Онлайн-форуми хакерів надають проактивному порталу CTI та шкідливих програм нове джерело інформації. Дослідження [8] показує AZ Safe Hacker Assets Portal. Цей веб-сайт збирає та аналізує шкідливі продукти із переважно невикористаних і багатих джерел даних онлайн-груп хакерів, використовуючи найсучасніші методи машинного навчання. У цьому документі обговорюється створення та розробка порталу активів AZ Safe Hacker. Автори також пропонують основні функції порталу, включаючи пошук активів, навігацію та завантаження, перегляд вихідного коду та аналітику порівняння коду, а також інтерактивну інформаційну панель CTI.

За останні десятиліття загрози кібербезпеці зросли. Експерти вважають, що існуючих заходів безпеки скоро буде недостатньо, щоб уникнути поширення більш складних і небезпечних кібератак. Останнім часом у складності кібербезпеки дедалі більше домінують підходи, запозичені зі штучного інтелекту (ШІ) для сприяння автоматизація. У цьому документі [2] дослідники надають короткий огляд і підказки щодо байєсівських програм кібербезпеки, щоб дозволити кількісну оцінку загроз для вищого аналізу ризиків і ситуаційної обізнаності.

Висновки та пропозиції. Оскільки кіберзлочини стають дедалі складнішими, підходи до кібербезпеки повинні бути більш надійними та розумними. Це дозволить механізмам захисту приймати рішення в режимі реального часу, щоб ефективно реагувати на складні атаки. Однак підходи штучного інтелекту до боротьби з кіберзлочинністю досі не класифіковані, що вимагає окремого дослідження.

Тому для ефективної боротьби з кіберзлочинністю, дослідники та практики повинні знати існуючі методи кібербезпеки та застосовувати штучний інтелект.

ЛІТЕРАТУРА

1. X. Chen et al., «Artificial intelligence-empowered path selection: *A survey of ant colony optimization for static and mobile sensor networks*». IEEE Access. Vol. 8. Pp. 71497 – 71511. 2020.

2. AI Forum of New Zealand and AsureQuality, «Artificial Intelligence for Agriculture in New Zealand». Pp. 40. 2019.

3. Y. Raban and A. Hauptman, «Foresight of cyber security threat drivers and affecting technologies». *Foresight*. Vol. 20. No. 4. Pp. 353 – 363, 2018, doi: 10.1108/FS-02- 2018-0020.

4. X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, and M. Sanz Rodrigo, *«Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies»*. IEEE Access. Vol. 8. Pp. 9005 – 9014. 2020.

5. J. Straub et al., *«CyberSecurity considerations for an interconnected self-driving car system of systems»*. 2017 12th Syst. Syst. Eng. Conf. SoSE 2017. 2017.

6. M. Z. Alom and T. M. Taha, *«Network intrusion detection for cyber security on neuromorphic computing system»*. Proc. Int. Jt. Conf. Neural Networks. Vol. 2017- May. Pp. 3830 – 3837. 2017.

7. K. Shaukat et al., «Performance comparison and current challenges of using machine learning techniques in cybersecurity». *Energies*. Vol. 13. No 10. 2020.

8. R. Coulter, Q. L. Han, L. Pan, J. Zhang, and Y. Xiang, «*Data-Driven Cyber Security in Perspective – Intelligent Traffic Analysis*». IEEE Trans. Cybern., Vol. 50. No 7. Pp. 3081 – 3093. 2020.

9. Fostolovych, V. «Modern tools of the business management system in the field of hotel and restaurant business». *Investytsii: praktyka ta dosvid*. Vol. 11 – 12. Pp. 18 – 25. 2022.

10. V. D. Soni, «Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA». SSRN Electron. J. Pp. 1–17. 2020.

11. N. Scarpato, N. D. Cilia, and M. Romano, *«Reachability Matrix Ontology: A Cybersecurity Ontology»* Appl. Artif. Intell., Vol. 33. No. 7. Pp. 643–655. 2019.

12. Y. Lu, *«Artificial intelligence: a survey on evolution, models, applications and future trends»*, J. Manag. Anal., Vol. 6, No. 1, pp. 1–29, 2019.

13. S. Mahdavifar and A. A. Ghorbani, «Application of deep learning to cybersecurity: A survey». *Neurocomputing*. Vol. 347. Pp. 149–176. 2019.

14. R. Calderon, «The Benefits of Artificial Intelligence in Cybersecurity» Econ. Crime Forensics Capstones. 36. 2021.

15. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень. К.: Маклаут, 2008. 444 с.

16. Глибовець М.М., Олецький О.В. Штучний інтелект: Підручн. для студ. вищ. навч. закладів, що навчаються за спец. «Компютерні науки» та «Прикладна математика». К.: Вид. дім «КМ Академія». 2012. 366 с.

17. Снитюк В.Є. Прогнозування. Моделі, методи, алгоритми. К.: Маклаут, 2018. 364 с.

REFERENCES

1. X. Chen et al., *«Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks»* IEEE Access. Vol. 8, Pp. 71497 – 71511. 2020.

2. AI Forum of New Zealand and AsureQuality, «Artificial Intelligence for Agriculture in New Zealand». P. 40. 2019.

3. Y. Raban and A. Hauptman, «Foresight of cyber security threat drivers and affecting technologies». *Foresight*. Vol. 20, No 4, Pp. 353 – 363. 2018. doi: 10.1108/FS-02- 2018-0020.

4. X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, and M. Sanz Rodrigo, *«Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies»* IEEE Access. Vol. 8. Pp. 9005 – 9014, 2020.

5. J. Straub et al., *«CyberSecurity considerations for an interconnected self-driving car system of systems»*. 2017 12th Syst. Syst. Eng. Conf. SoSE 2017. 2017.

6. M. Z. Alom and T. M. Taha, *«Network intrusion detection for cyber security on neuromorphic computing system»*. Proc. Int. Jt. Conf. Neural Networks. Vol. 2017- May. Pp. 3830 – 3837. 2017.

7. K. Shaukat et al., *«Performance comparison and current challenges of using machine learning techniques in cybersecurity»*. Energies. Vol. 13, No 10. 2020.

8. R. Coulter, Q. L. Han, L. Pan, J. Zhang, and Y. Xiang, *«Data-Driven Cyber Security in Perspective - Intelligent Traffic Analysis»* IEEE Trans. Cybern. Vol. 50. No 7. Pp. 3081–3093, 2020.

9. Fostolovych, V. «Modern tools of the business management system in the field of hotel and restaurant business». *Investytsii: praktyka ta dosvid*. Vol. 11 – 12. Pp. 18 – 25. 2022.

10. V. D. Soni, *«Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA»*. SSRN Electron. J. Pp. 1 – 17. 2020.

11. N. Scarpato, N. D. Cilia, and M. Romano, «*Reachability Matrix Ontology: A Cybersecurity Ontology»* Appl. Artif. Intell. Vol. 33. No. 7, Pp. 643 – 655, 2019.

12. Y. Lu, *«Artificial intelligence: a survey on evolution, models, applications and future trends»*. J. Manag. Anal., Vol. 6. No. 1, Pp. 1 – 29. 2019.

13. S. Mahdavifar and A. A. Ghorbani, «Application of deep learning to cybersecurity: A survey». *Neurocomputing*. Vol. 347, Pp. 149 – 176. 2019.

14. R. Calderon, «The Benefits of Artificial Intelligence in Cybersecurity». Econ. Crime Forensics Capstones. 36., 2021.

15. Hnatienko H.M., Snityuk V.E. Expert decision-making technologies. K.: Maklaut. 2008. 444 p.

16. Hlybovets M.M., Oletskyi O.V. Artificial intelligence: Manual. for students higher education institutions studying for special «Computer Science» and «Applied Mathematics». - K.: Ed. House «KM Academy». 2012. 366 p.

17. Snytyuk V.E. Prognostication. Models, methods, algorithms. - K.: Maklaut, 2018. 364 p.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 02.12.2023