УДК 004.81
DOI: 10.31673/2409-7292.2020.040611

Савченко В.А., Шаповаленко О.Д.

ОСНОВНІ НАПРЯМИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

У статті досліджуються ключові технології штучного інтелекту з метою застосування їх для забезпечення захисту інформації. Показано, що на даний час у кібербезпеці відсутня загальна концепція запровадження штучного інтелекту, не визначені найважливіші методи штучного інтелекту, які можуть бути використані у кібербезпеці, та не встановлено роль, яку можуть відігравати ці методи для захисту організацій у кіберпросторі. У якості ключової ідеї застосування засобів штучного інтелекту у кібербезпеці запропоновано використання технологій та методів, які полегшують виявлення та реагування на загрози, використовуючи набори статистичних даних про кібератаки. Пріоритетні сфери застосування штучного інтелекту – забезпечення безпеки мереж і захист даних.

Ключові слова: штучний інтелект, технологія, кібербезпека, машинне навчання, нейронна мережа

Вступ

На теперішній час термін “Штучний інтелект” (ШІ) вже надійно укорінився у повсякденному житті. І хоча пристроям з елементами штучного інтелекту все ще бракує можливостей зрозуміти проблему та знайти її рішення, то, коли йдеться про зменшення помилок в оперативних завданнях та пошук аномалій у різноманітних процесах, штучний інтелект випереджає людські здібності та компетентність. Штучний інтелект відіграє важливу роль у оцінці помилок, які можуть бути вчинені людьми. Передбачається, що у сфері кібербезпеки системи на основі штучного інтелекту зможуть захистити організації від Інтернет-загроз, визначати типи шкідливих програм, забезпечувати дотримування стандартів безпеки та допоможуть створити кращі стратегії запобігання атакам та відновлення після атак.

За оцінкою Gartner, витрати на системи інформаційної безпеки і управління ризиками у 2022-му році збільшаться до $ 174 млрд, з них приблизно $ 50 млрд будуть спрямовані на захист клієнтських систем. Продажі хмарних платформ і додатків для забезпечення безпеки виростуть до $ 1,63 млрд в 2023-му році, а систем забезпечення безпеки додатків до $ 4,5 млрд. Зростає і ринок послуг в області інформаційної безпеки, за останній рік він збільшився з $ 62 млрд до $ 66,9 млрд. Однак самі по собі гроші не можуть вирішити питання. Більшість фахівців з інформаційної безпеки сьогодні перевантажені аналізом журналів, запобіганням спроб злому, розслідуванням можливих випадків шахрайства і т. Д. Дефіцит кадрів великий, тому в індустрії безпеки все з більшою надією дивляться на рішення в області штучного інтелекту. За оцінкою Marketsand Markets, в 2019-2026 рр. зростання ринку засобів ШІ для забезпечення кібербезпеки буде рости в середньому на 23,3% в рік, з $ 8,8 млрд до $ 38,2 млрд (рис. 1) [1].

Формулювання проблеми

Незважаючи на уявлення щодо потенційних можливостей засобів штучного інтелекту їх застосування залишається переважно епізодичним та несистематизованим. На даний час у кібербезпеці відсутня загальна концепція запровадження штучного інтелекту, не визначені найважливіші методи штучного інтелекту, які можуть бути використані у кібербезпеці, та не встановлено роль, яку можуть відігравати ці методи (особливо, що стосується машинного навчання, дата-майнінгу, глибокого навчання та експертних систем) для захисту організацій у кіберпросторі. Відтак, **метою** даної роботи є аналіз та систематизація підходів щодо застосування основних технологій штучного інтелекту у сфері кібербезпеки.

Ключові технології штучного інтелекту

Штучний інтелект – це сукупність теоретичних та практичних підходів у галузі інформаційних технологій, які передбачають створення систем, що можуть функціонувати розумно та незалежно, подібно до механізму прийняття рішень у мозку людини. Завдяки ШІ машина зможе навчатися досвіду обробляючи великі обсяги даних та розпізнаючи шаблони у

них. Наприклад, Apple Siri, розпізнавання облич та самокерований автомобіль засновані на машинному навчанні та обробці природних мов, що є окремою галуззю ШІ. Крім того, ШІ включає багато суміжних областей та технологій, таких як машинне навчання, глибоке навчання, нейронні мережі, обробка природних мов та інші [2].

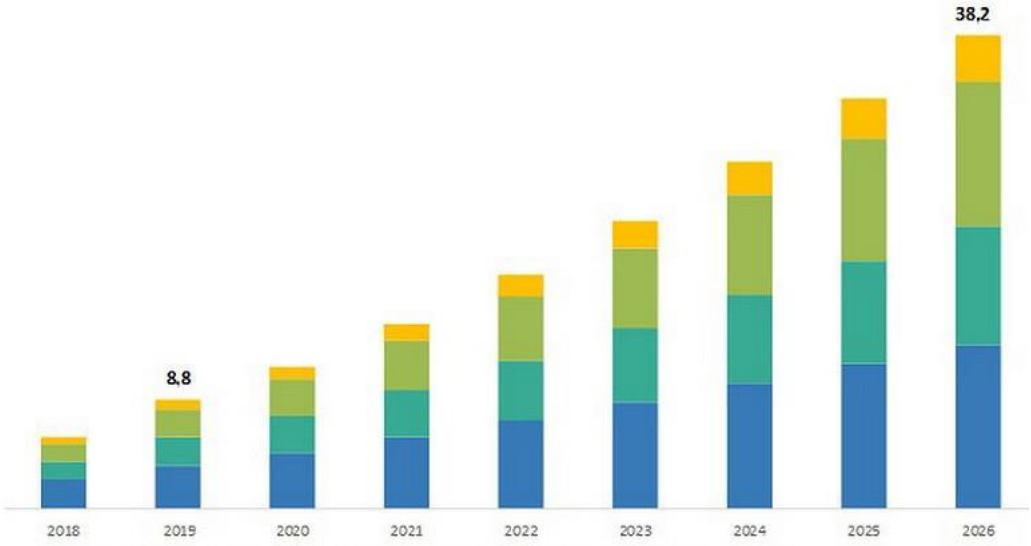

Рис. 1. Динаміка ринку засобів ШІ для кібербезпеки, $ млрд [1]

Для більш глибокого розуміння, систематизуємо основні напрямки досліджень у галузі штучного інтелекту, які реалізовані практично і якими ми користуємося майже щодня:

Машинне навчання – це множина технологій, які дозволяють комп'ютерам мислити за допомогою математичних алгоритмів на основі зібраних даних та конкретних інструкцій та правил [3]. Замість програмування комп'ютера на кожному кроці, цей підхід реалізує технології, які дозволяють йому поетапно вчитися на даних без інструкцій програміста [4]. Прикладом машинного навчання є віртуальні особисті помічники, які допомагають знаходити інформацію та дають вказівки щодо конкретних завдань, коли їх запитують через голос. Іншими прикладами є: відеоспостереження, яке відстежує незвичну поведінку, послуги соціальних медіа для зв'язку з "людьми, яких ви можете знати" на основі постійного самонавчання відповідно до уподобань людей.

Нейронні мережі (*Глибоке навчання*) являє собою подальший розвиток машинного навчання і є комп'ютерною моделлю, яка виконує завдання класифікації безпосередньо із зображень, тексту чи звуку. Ця модель реалізується з використанням широкого набору багатовимірних даних та багатошарової архітектури нейронної мережі. Глибоке навчання досягає точності розпізнавання при застосуванні більш складних моделей. Прикладами застосування цієї моделі у реальному житті є автоматизоване керування автомобілем, розпізнавання облич та знаків, промислова автоматизація та ін. [5,6].

Природна обробка мови, сукупність методів, які дозволяють машині аналізувати мову людини, зокрема у чат-ботах для програм підтримки клієнтів, використовують машинне навчання та обробку природної мови.

ШІ застосовує технології, які можна використовувати у багатьох галузях промисловості, таких як фінансові установи, освіта та охорона здоров'я. Зважаючи на вищевикладене цілком доцільним є потенційне використання методів ШІ для забезпечення кібербезпеки організацій та підприємств.

Потенційні можливості методів штучного інтелекту для застосування у сфері кібербезпеки

Без сумніву, величезний потенціал технологій штучного інтелекту може бути використаний для підвищення кібербезпеки. Кількість даних, що генеруються в сучасному

світі, постійно збільшується, при цьому інформація зберігається та передається у різній формі з використанням мережі Інтернет. Більше того, безпечна передача даних відіграє життєво важливу роль у боротьбі з кіберзлочинами, що досягається шляхом дотримання принципів кібербезпеки. З ростом прогресу в галузі інформаційних технологій кіберпростір перетворюється на полігон для вчинення різних кіберзлочинів [7] а, згідно з поглядами військових фахівців, стає четвертим (разом з сушею, морем, повітрям) театром воєнних дій.

Штучний інтелект у кібербезпеці – це достатньо широка область знань, яка потенційно може використовуватись в організаціях для зменшення ризиків та збільшення доходу, виявлення кіберзагроз та шахрайства. Відстежувати нові віруси та шкідливе програмне забезпечення стає все складніше і тому засоби на основі технологій штучного інтелекту здатні полегшити виявлення та реагування на загрози, використовуючи статистичні дані про кібератаки, щоб визначити найкращий перелік дій щодо протидії. ШІ може бути більш ефективним при виявленні шкідливого програмного забезпечення, ніж людина. ШІ впроваджується в організаціях з кількома рівнями безпеки, такими як Інформування про безпеку та Управління подіями і це допомагає поліпшити аналітикам безпеки виявлення будь-яких загроз усередині мережі організації [8].

Чим швидше можна виявити порушення цілісності даних, тим менші витрати на їх відновлення. Постійне збільшення часу на усунення порушень пов’язане зі збільшенням тяжкості зловмисних нападів, які зазнали більшість компаній. Автоматизація безпеки та інтелектуальні засоби, що забезпечують контроль у ситуаційному центрі безпеки, можуть допомогти поліпшити здатність організації зменшити збитки, спричинені порушеннями [9]. У рішеннях з кібербезпеки використовуються багато типів програм ШІ, зокрема SIEM системи, різноманітні фільтри спаму, засоби захищеної автентифікації користувачів та засоби прогнозування інцидентів злому. Ці програми навчаються за допомогою бази даних попередньої поведінки та можуть ідентифікувати кожну окрему поведінку як шкідливу чи ні. За даними компанії IBM, збитки від порушення даних у всьому світі будуть знижені, якщо організації застосовуватимуть автоматизовані рішення безпеки. Організації, які не застосовували автоматизацію безпеки, зазнали витрат на порушення, які були на 95 % вищими, ніж порушення в організаціях з повністю розгорнутою автоматизацією [10].

Експертні системи. Експертні системи є одним з найвідоміших інструментів штучного інтелекту і являють собою програмні пакети, які допомагають отримати відповіді на запити, які надає клієнт або надає інший пакет програм. Ці системи включають вміст знань, в якому знання експертів зберігаються в певній галузі застосування. Ці системи також включають механізм міркувань для доступу до відповідей з урахуванням наданої інформації та іншої додаткової інформації стосовно умов навколишнього середовища.

Експертна система програмується для пошуку відповідей на запити в певній області застосування, що відображаються або користувачем, або іншим продуктом. У кібербезпеці вони застосовуються для вибору заходів безпеки та визначення шляхів використання обмежених активів. Експертні системи безпеки допомагають персоналу організацій у боротьбі з кібератаками. Це здійснюється шляхом звірки логів атаки з базою знань у випадку, якщо це відомий процес, або її ігнорування, коли процес невідомий. У разі відсутності такої процедури в базі знань, експертна система використовує алгоритми механізму виведення та знаходить наближене рішення на основі досвіду [11].

Машинне навчання. Машинне навчання – це область штучного інтелекту, яка дозволяє комп’ютеру навчатись, використовуючи дані зразків (паттернів), не запрограмовані передбачити кожну можливу ситуацію. «Два найпоширеніші типи машинного навчання – це навчання з учителем та без учителя. Навчання з учителем використовується, коли доступний набір достовірно відомих екземплярів атак, зокрема, для вирішення проблем класифікації. Мета контрольованого навчання – навчити комп'ютер передбачати значення або точно класифікувати вхідний екземпляр атаки. Навчання без учителя використовується, коли набір достовірних даних недоступний. Кластеризація – це неконтрольована техніка навчання, яка приводить до подібних випадків групування в кластери. Кластеризація використовується для

виявлення закономірностей у даних. У деяких випадках кластеризація виконується для класифікації немаркованого набору даних та використання отриманого класифікованого набору даних для контрольованого навчання [12].

Оскільки загрози кібербезпеки постійно змінюються та розвиваються, необхідна автоматизована та негайна реакція. Отже, методи машинного навчання, особливо глибоке навчання, яке не обов'язково вимагає попереднього навчання або опори на попередні класифікації, надані експертами, можуть бути особливо життєво важливими при застосуванні підходів ШІ до кібербезпеки [13].

Нейронні мережі. Глибоке навчання. Відсутність великих масивів даних щодо кібератак є загальним викликом у дослідженнях з кібербезпеки. Часто це пояснюється вимогами щодо конфіденційності, коли компанії не бажають ділитися досвідом щодо атак, яких вони зазнали, але, разом з тим, база відомих загроз поступово все ж таки наповнюється, що дає можливість застосовувати методи глибокого навчання. Основою для таких методів є великі і часто незбалансовані набори даних, які часто використовуються для ручної кластеризації. У сфері кібербезпеки нейронна мережа може розрізнити, чи є документ шкідливим чи законним без будь-якого втручання людей. Ця технологія дозволяє виявляти шкідливі програми, демонструючи при цьому кращі результати у порівнянні з іншими методами [14].

Дата майнінг. Дата майнінг – це пошук суттєвих закономірностей та тенденцій у великій базі даних. Методологія аналізу даних спрямована на отримання цінної інформації та пошук прихованих закономірностей з величезної кількості баз даних, які не можуть бути виявлені статистичними методами. Це широка область досліджень, яка включає машинне навчання, бази даних, статистику, експертні системи, візуалізацію, високопродуктивні обчислення, нейронні мережі та методи представлення знань. Дата майнінг підтримується хостом, який фіксує дані різними способами (наприклад, кластеризація, класифікація, аналіз посилань, узагальнення, регресійні моделі та аналіз послідовностей) [15].

Основні приклади програм для дата майнінгу для кібербезпеки:

методи виявлення атипових видів діяльності.

аналіз посилань для відстеження вірусів.

класифікація та групування декількох кібератак на основі їх профілів.

прогнозування можливих майбутніх атак на основі отриманої інформації.

Інтелектуальні агенти. Інтелектуальний агент (ІА) – це автономна сутність, яка сканує датчики та стежить за доменами за допомогою виконавчих механізмів і координує свої дії для досягнення цілей. Інтелектуальний агент також може вивчати або використовувати інформацію для досягнення своїх цілей. Агенти можуть адаптуватися до реального часу, швидко пізнавати нові речі завдяки спілкуванню з навколишнім середовищем, а також мати можливість зберігання та відновлення моделей на основі пам'яті. Інтелектуальні агенти застосовуються, як правило, для захисту від атак типу “Відмова в обслуговуванні” (DoS/DDoS). Крім того, вони є ефективними при пошуку необхідної інформації у мережі, розподіленої обробки даних та ін.

Практика застосування ШІ у кібербезпеці. Ступінь зацікавленості служб інформаційної безпеки в штучному інтелекті залежить від галузі застосування. Консалтингова компанія Capgemini опублікувала результати опитування 850 керівників вищої ланки з 10 країн (Австралії, Великобританії, Німеччини, Індії, Італії, Іспанії, Нідерландів, США, Франції, Швеції). При цьому 20% респондентів займали пост IT-директора, 10% – керівника служби IT-безпеки. Компанії представляли сім сфер діяльності – виробництво споживчих товарів, ритейл, банківський сектор, страхування, автомобілебудування, ЖКГ та телекомунікації. За оцінкою Capgemini, якщо до 2019 г. лише кожна п'ята організація використовувала штучний інтелект для кібербезпеки, то 2020 році таких організацій вже понад 60%. Майже половина опитаних (48%) заявила, що бюджети на ШІ в області кібербезпеки збільшаться в 2021 фінансовому році в середньому на 29%. Пріоритетні варіанти використання ШІ для

кібербезпеки – забезпечення безпеки мережі і захист даних. Рішення інтернету речей поки відстають, але і з'явилися вони лише в останні роки (табл. 1) [1].

Таблиця 1

Рівень фінансування сфер застосування засобів штучного інтелекту

№	Сфера застосування засобів ШІ	Ступінь використання фінансів на захист, %
1.	Мережева безпека	75
2.	Безпека даних	71
3.	Безпека кінцевих точок	68
4.	Безпека систем ідентифікації	65
5.	Безпека додатків	64
6.	Хмарна безпека	59
7.	Безпека Інтернету речей	53

Висновки

Кількість атак на інформаційні системи зростає щороку високими темпами. При цьому атаки стають все більш витонченими, а збиток від них – усе вищим. До потенційних цілей тепер відносяться як мережева інфраструктура, так і пристрої інтернету речей та розумні домашні пристрої. «Класичні» засоби антивірусного боротьби вже не здатні впоратися з такими епідеміями, і на допомогу приходять рішення на базі штучного інтелекту.

Виглядаючи по-різному стосовно сучасних рішень з кібербезпеки, методи ШІ надійні та більш гнучкі і здатні покращувати системи захисту від все більшої кількості випереджаючих кіберзагроз. Разом з тим, незважаючи на інтенсивні зміни, які ШІ переніс у область кібербезпеки, відповідні системи ще не готові повністю адаптуватися до середовища, а також робити зміни у своєму стані. На сьогоднішній день ШІ ще не став основною панацеєю для безпеки. У той момент, коли людський інтелект має намір атакувати інтелектуальну систему безпеки, ця система зазнає збою. У той же час це не означає, що ми не повинні використовувати методи ШІ для захисту. Навпаки, ми повинні знати його обмеження та використовувати їх належним чином.

Перелік посилань

1. Почему искусственный интеллект все чаще принимают на кибервооружение? https://safe.cnews.ru/articles/2020-06-01_pochemu_iskusstvennyj_intellekt_vse
2. Kabbas A., Alharthi A, Munshi A. Artificial Intelligence Applications in Cybersecurity. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2, Fabruary 2020. 120-124.
3. Big data, artificial intelligence, machine learning and data protection. 2nd ed. [ebook] Information Commissioner's Office. (2017). https://ico.org.uk/media/fororganisations/documents/2013559/big-data-ai-ml-and-dataprotection.pdf.
4. Rupali M., Amit P. A Review Paper on General Concepts of “Artificial Intelligence and Machine Learning”. National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017) AGTI’s Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad Vol. 4, Special Issue 4, January 2017. 79-82.
5. Mathew A., Amudha P. and Sivakumari S. Deep Learning Techniques: An Overview. In book: Advanced Machine Learning Technologies and Applications. January 2021. https://www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview
6. Kumar S. H. and Tiwary R. K. Analysis of rankbrain algorithm using machine learning. (2017).
7. Bhatele, Kirti Raj and Harsh Shrivastava, and Neha Kumari. The Role of Artificial Intelligence in Cyber Security. In *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems.* edited by S. Geetha , and Asnath Victy Phamila, 170-192. Hershey, PA: IGI Global, 2019.
8. Intelligence, S. (2019). IBM QRadar Security Intelligence. [online] Ibm.com. Available at: https://www.ibm.com/security/security-intelligence/qradar [Accessed 6 Dec. 2019].

9. Nadine Wirkuttis and Hadas Klein. Artificial Intelligence in Cybersecurity. Cyber, Intelligence, and Security | Volume 1 | No. 1 | January 2017. 103-119.

10. Bob Sohval. A Deep Dive in Scoring Methodology. 2020 SecurityScorecard Inc. 26 p.

11. Arockia Panimalar.S1, Giri Pai.U2, Salman Khan.K. Artificial Intelligence Techniques for Cyber Security. International Research Journal of Engineering and Technology (IRJET). Volume: 05 Issue: 03 | Mar-2018. 122-124.

12. Al Musawi, Ahmad. (2018). Introduction to Machine Learning. https://www.researchgate.net/publication/323108787_Introduction_to_Machine_Learning

13. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cybersecurity. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.

14. Dipankar Dasgupta, Zahid Akhtar, Sajib Sen. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling & Simulation. September 2020.

15. M. Nikhil Kumar, K.V.S. Koushik, K. John Sundar. Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2018 IJSRCSEIT | Volume 3 | Issue 3. 162-167.

Надійшла: 07.10.2020 Рецензент: д.т.н., професор Вишнівський В.В.