ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент, заступник декана факультету з навчально-методичної роботи факультету № 4 Харківський національний університет внутрішніх справ

Каланча Андрій Андрійович
курсант групи Ф4-202 факультету № 4
Харківський національний університет внутрішніх справ

Гельдт Станіслав Володимирович
курсант групи Ф4-302 факультету № 4
Харківський національний університет внутрішніх справ

В умовах стрімкого розвитку інформаційних технологій використання можливостей штучного інтелекту (ШІ) під час розв’язання завдань, пов’язаних із забезпеченням кібербезпеки, набуває актуальності та вимагає від фахівців, задіяних у даних процесах, наявності теоретичних знань та практичних навичок для вмілого застосування спеціалізованого програмного забезпечення, що спирається на використання технологій ШІ.

Штучний інтелект – це розділ комп'ютерної лінгвістики та інформатики, метою якого є формалізація проблем та завдань, які подібні до дій, виконуваних людиною [1].

Системи ШІ ітераційні та динамічні – основою їхнього «навчання» є досвід, отриманий на основі даних, наданих для аналізу. Аналіз даних, з іншого боку, є статичним процесом, який досліджує великі набори даних, щоб зробити висновки про інформацію, яку вони містять, за допомогою спеціалізованих систем і програмного забезпечення [2].

Згідно із дослідженнями, опублікованими в MIT Sloan Management Review, три чверті генеральних директорів вважають, що ШІ дозволить їхній компанії ефективніше розвиватися, через що саме йому і надають перевагу (рис. 1).

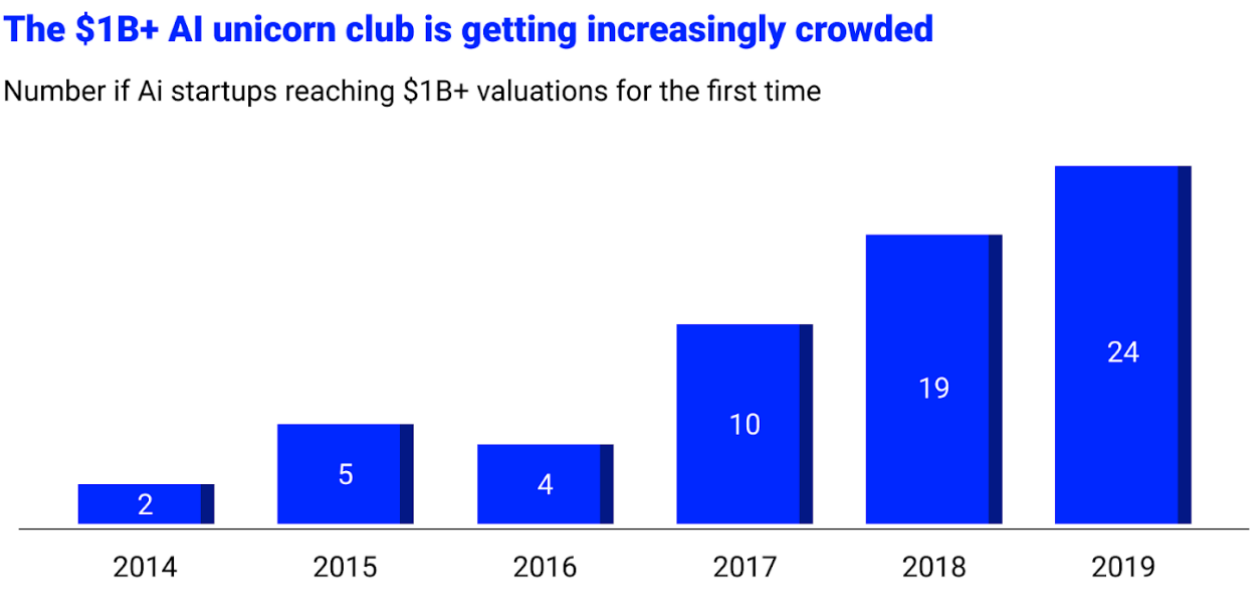

Рисунок 1 – Статистика використання ШІ у корпораціях

Спираючись на зазначені дані, стартапи 2017 року стали відправною точкою для популяризації штучного інтелекту у комерційних цілях, та 53 із них, станом на 2019 рік, були оцінені у більше ніж мільярд доларів.

Крім того, у 2019 році зросла кількість компаній ШІ, вартість яких перевищила мільярд доларів. Ними стали: розробник автономних роботів для доставки вантажів Nuro і аналітична компанія DataRobot. Усі десять нових компаній-мільярдерів розташовані в Китаї, Великобританії чи США. Такі венчурні інвестори, як Plug and Play Ventures, Accel і Lightspeed Ventures, були одними з лідерів інвестування в штучний інтелект у 2019 році [3].

Оскільки ШІ може бути реалізований для різнопланових задач, так як представляє собою інструмент, що здатен самостійно навчатися у необхідному середовищі, було створено подібне рішення і для сфери кібербезпеки. Таке рішення має наступні аспекти:

1) виявлення можливої загрози;
2) реагування на кіберінциденти;
3) взаємодія із біометричними даними.

Ці можливості застосовуються у 4 основних напрямках.

Інвентаризація IT-активів – отримання повної точної інвентаризації всіх пристроїв, користувачів і програм із будь-яким доступом до інформаційних систем, у склад якої входять як категоризація, так і вимірювання критичності.

Викриття загроз – надання актуальних знань про глобальні та галузеві загрози для прийняття важливих рішень про пріоритетність атак на системи безпеки підприємства.

Прогнозування ризику зламу – враховуючи інвентаризацію IT-активів, виявлення загроз і ефективність засобів контролю, системи на основі ШІ можуть передбачити, де найімовірніше буде здійснено злам. Рекомендовані відомості, отримані в результаті аналізу за допомогою технологій ШІ, стануть в нагоді для

налаштування та вдосконалення елементів керування та процесів підвищення кіберстійкості організації.

Реагування на інциденти – надання системами на базі ШІ покращеного контексту для встановлення пріоритетів і реагування на сповіщення системи безпеки, для швидкого реагування на інциденти та виявлення першопричин, щоб пом'якшити вразливі місця та уникнути майбутніх проблем [2].

Готовими продуктами у цій сфері стали рішення наступних компаній.

IBM Security QRadar SIEM. Платформа, що складається з наступних продуктів:

1. IBM QRadar Advisor with Watson – додаток, що обробляє та проводить послідовні та ретельні розслідування повторюваних загроз центу безпеки.
2. IBM QRadar Incident Forensics – додаток, що відстежує та аналізує дії злочинців у кіберпросторі для глибокого розуміння зламу системи безпеки та реконструює дані, пов'язані з інцидентом безпеки.
3. IBM QRadar Data Store – додаток, що збирає, аналізує та зберігає великі обсяги даних щодо безпеки та проведених операцій.
4. IBM QRadar Data Synchronization App – додаток, який дає змогу легко, економічно та ефективно копіювати дані і файли конфігурації між основними або активними та вторинними розгортаннями QRadar для аварійного відновлення [4].

Платформа Balbix Security Cloud використовує спостереження та аналіз на базі штучного інтелекту для безперервного прогнозування ризиків у режимі реального часу, управління вразливістю на основі ризиків і проактивного контролю зламів. Платформа допомагає командам з кібербезпеки підвищити ефективність у багатьох напрямках роботи, які вони повинні виконувати, щоб підтримувати надійну безпеку – від підтримки систем у встановлених виправленнях до запобігання програм-вимагачів [5].

Використання технології штучного інтелекту з 2014 по 2019 роки стало у 12 разів більшим відповідно дослідженням MIT Sloan Management Review, що пов'язано з фізичною неможливістю фахівців з кібербезпеки постійно проводити повторний аналіз та ідентифікацію загроз із метою зменшення ризиків зламу та покращення стану кібербезпеки. У сфері безпеки штучний інтелект може визначати пріоритети ризиків, миттєво виявляти будь-яке шкідливе програмне забезпечення в мережі, керувати реагуванням на інциденти та виявляти вторгнення до їх початку, що є зручним, надійним та ефективним інструментом для фахівців з кібербезпеки.

Список літератури:

1. Вікіпедія. Штучний інтелект. URL: https://uk.wikipedia.org/wiki/Штучний_інтелект (дата звернення: 03.02.2023).
2. Balbix. Using Artificial Intelligence in Cybersecurity. URL: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ (дата звернення: 03.02.2023).

3. Ideamotive. 100 Artificial Intelligence Statistics For 2022: The Ultimate List. URL: https://www.ideamotive.co/blog/the-ultimate-list-of-artificial-intelligence-statistics (дата звернення: 03.02.2023).

4. IBM. IBM Security QRadar SEIM. URL: https://www.ibm.com/products/qradar-siem/addons#3071036 (дата звернення: 03.02.2023).

5. Balbix. Balbix Security Cloud. URL: https://www.balbix.com/product-overview/ (дата звернення: 03.02.2023).