Анна КРИНИЧНА
викладачка кафедри спеціальних
дисциплін та професійної підготовки
КННІ Донецького державного
університету внутрішніх справ

Андрій СОЛОМАХА
викладачка кафедри спеціальних
дисциплін та професійної підготовки
КННІ Донецького державного
університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ: СУЧАСНІ СПОСОБИ ЗАБЕЗПЕЧЕННЯ

Кожна сучасна соціально активна людина в Україні використовує мобільні пристрої та користується інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку. Де розвиваються нові суспільні відносини, там з'являється й злочинність. Відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів (і це не враховуючи класичні правопорушення з використанням комп'ютерної техніки, а також рівня латентності такої злочинності) [8].

На початку XXI століття злодій - це не обов'язково холоднокровна озброєна людина. Інформаційна революція призвела до того, що злодієм може виявитися звичайний студент із ноутбуком та доступом до мережі.

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 (Artificial Intelligence - AI) розуміється як здатність автоматичних систем брати на себе функції людини, вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів. Будь-який інтелект спирається на діяльність. Багато хто вважає, що впровадження штучного інтелекту в технології кібербезпеки стане свого роду революцією і станеться це набагато раніше, ніж можна було б припустити. Насправді ж в майбутньому нас, швидше за все, чекають лише поступові поліпшення в цій галузі. Але навіть ці кроки на шляху до абсолютної автономності все ж далеко виходять за рамки наших можливостей в минулому. Незабаром штучний інтелект на основі машинного навчання стане потужним

інструментом забезпечення кібербезпеки. У цій сфері, як і інших галузях, участь людини давно вважається важливим, незамінним елементом. І хоча в даний час кібербезпека, як і раніше, багато в чому залежить від роботи фахівців, у вирішенні певних завдань машини поступово починають нас випереджати [2, с. 341].

В останні роки штучний інтелект (ШІ) став найважливішим інструментом посилення роботи людських команд з інформаційної безпеки. ШІ забезпечує настільки необхідний аналіз та виявлення загроз, які фахівці з кібербезпеки можуть використовувати для зниження ризику злому та підвищення рівня безпеки, оскільки люди вже не можуть адекватно захистити динамічну корпоративну поверхню атаки. 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 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.

З огляду на гостру нестачу досвідчених фахівців щодо забезпечення безпеки і величезні обсяги даних, з якими доводиться працювати організаціям, багато компаній вже використовують можливості штучного інтелекту (ШІ) для забезпечення кібербезпеки або планують зробити це.

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 а, згідно з поглядами військових фахівців, стає четвертим театром воєнних дій.

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 ІТ-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 ІТ-активів, виявлення загроз і ефективність засобів контролю, системи на основі ШІ можуть передбачити, де найімовірніше буде здійснено злам.

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.

Отже, інтелектуальні системи позбавлені недоліків людського фактора: вони працюють швидше і помиляються значно рідше людей. ШІ дозволяє практично повністю виключити людей з процесів забезпечення захисту і залишає їм допоміжні функції моніторингу та корекції.

Список використаних джерел

1. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системноструктурний аналіз) / В. М. Бутузов ; Рада нац. безпеки і оборони України, Міжвід. н.-д. центр з пробл. боротьби з організованою злочинністю. Київ. : КИТ, 2010. 405 с
2. Девтеров Ілля Володимирович Соціалізація людини у кіберпросторі / І. В. Девтеров ; Мво освіти і науки, молоді та спорту України, Нац. техн. ун-т України "Київ. політехн. ін-т". Київ. : НТУУ "КПІ", 2012. 357 с. Бібліогр.: с. 335–357
3. Закон України: Про основні засади забезпечення кібербезпеки України / Законодавство України. 2018.
4. Кларк Дж., Джейкоб Дж. (2018). ШІ та кібербезпека: загрози та рішення. Журнал кібербезпеки, 4(1), С. 1-14.
5. Курбан Олександр Васильович Сучасні інформаційні війни у мережевому он-лайн просторі: навч. посіб. / О. В. Курбан. Київ, 2016. С.56–57.
6. Основні напрями застосування технологій штучного інтелекту у кібербезпеці/Савченко В. А [Доповідь]. 2020-5с.
7. Опірський І.Р., С.І. Василишин, В.А. Сусукайло Розслідування кіберзлочинів за допомогою прийому у хмарному середовищі. Безпека інформації, 27(1). 2021. С. 13-20
8. «ШІ та кібербезпека: майбутнє кіберзахисту» [Електронний ресурс]. Режим доступу до ресурсу: https://www.forbes.com/sites/andrewrossow/2021/06/01/ai-and-cybersecurity-the-future-of-cyber-de-fense/
9. Федотов Олег Олексійович Викриття злочинів у сфері комп'ютерних технологій як різновид боротьби з тероризмом / О. А. Федотов; Нац. акад. внутр. справ. Львів: Вид-во Львів. політехніки, 2014. 219 с. Бібліогр.: с. 186–217.