АНАЛІЗ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА ЗАХИЩЕНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ

Назаренко Д.М.

Харківський Національний Університет
Радіоелектроніки, Україна.

E-mail: dmytro.nazarenko1@nure.ua

Abstract

In today's digital landscape, where cyber security threats are becoming increasingly complex and distinct, the use of Artificial Intelligence (AI) in cyber defense is becoming a key factor in determining information systems protection strategies. The application of AI in cyber security opens up new perspectives in detecting threats, adapting to evolving attacks, and increasing the effectiveness of cyber defense. The detailed impact of AI on the security of information systems is considered and innovative approaches that change the landscape of cyber security are highlighted.

На даний час в світі суспільний розвиток характеризується формуванням інформаційного суспільства. Зацікавленими у розвитку інформаційної безпеки є не тільки бізнес-структури, що активно застосовують нововведення у даній сфері, а й державні установи, для яких найголовнішим є питання національної безпеки [1, с. 20]. Одним з чинників, що сприяє забезпеченню інформаційної безпеки є застосування технологій штучного інтелекту. Адже штучний інтелект є одним з трендових напрямків, яким охоплені всі розвинуті країни світу.

Використання штучного інтелекту в інформаційній безпеці обумовлено насамперед двома чинниками:

• необхідністю оперативного реагування під час настання кіберінциденту;

• нестачею кваліфікованих спеціалістів з кіберзахисту [2, с.10]

У зв'язку з розвитком штучного інтелекту суттєво змінився підхід до захисту конфіденційності інформації, особливо в Інтернеті. З огляду на неперервний розвиток технологій штучного інтелекту, дедалі важливіше для людей та організацій розуміти, як можна використовувати цю технологію для захисту своїх даних та персональних даних.

Системи безпеки, які використовують штучний інтелект, у змозі виявляти та запобігати зловмисним діям, таким як крадіжки особистих даних, кібератаки і витоки інформації. Ці системи можуть виявляти надзвичайно підозрілу активність і сповіщати користувачів про потенційні загрози навіть до того, як вони стануть актуальними проблемами. Системи, що використовують штучний інтелект, також здатні виявляти та блокувати підозрілі електронні листи. Аналізуючи вхідні повідомлення за допомогою штучного інтелекту, ці системи у змозі виявляти шкідливі листи та запобігати їхньому доступу до користувача [3].

Системи, що базуються на штучному інтелекті, можуть також бути використані для виявлення та блокування шкідливого програмного забезпечення. При використанні штучного інтелекту при аналізі вхідного програмного забезпечення, ці системи у змозі виявляти шкідливе програмне забезпечення та забороняти йому доступ до користувача. Тому це дає змогу захистити користувачів від шкідливих програм, зловмисного програмного забезпечення та інших онлайн-загроз.

У кінці кінців, системи, що використовують штучний інтелект, у змозі виявляти та блокувати зловмисних користувачів. Аналізуючи поведінку користувачів за допомогою штучного інтелекту, ці системи можуть виявляти зловмисників і перешкоджати їхньому доступу до даних користувача. Тому це сприяє захисту користувачів від хакерів, зловмисників та інших онлайн-загроз.

Аналіз потенційних загроз штучного інтелекту для забезпечення конфіденційності особистих даних.

Непокоїть багатьох людей питання можливих загроз для захисту особистих даних, пов'язаних із розвитком штучного інтелекту. Штучний інтелект стає все більш складним і застосовується в різних сферах, від розпізнавання облич до аналізу даних. Незважаючи на те, що ця технологія може бути потужним інструментом для підприємств і організацій, вона також може використовуватися для незаконного збору та аналізу особистих даних без відома або згоди осіб. Це викликає серйозні питання про захист конфіденційності та приватності. З розвитком технології штучного інтелекту ускладнюється регулювання її використання та забезпечення захисту людей від можливих ризиків.

Однією з очевидних загроз, пов'язаних із штучним інтелектом, є можливість витоку даних. Штучний інтелект може використовуватися для доступу та аналізу великих обсягів інформації, включаючи особисті дані. Якщо ці дані не будуть належним чином захищені, зловмисники можуть отримати до них доступ і використовувати для злочинних цілей. Крім того, штучний інтелект може бути використаний для спрямування реклами чи інших повідомлень на конкретні особи, що може призвести до непотрібного або нав'язливого контакту.

Ще однією загрозою, пов'язаною із штучним інтелектом, є можлива упередженість. Алгоритми штучного інтелекту можуть бути налаштовані на користь певних груп або конкретних осіб, що може вести до дискримінації чи несправедливого ставлення. Це особливо важливо у випадках, коли йдеться про чутливі питання, такі як житло, працевлаштування чи медична допомога.

У кінці кінців, штучний інтелект може використовуватися для контролю за людьми та спостереження за їхньою активністю, що може призвести до відсутності приватності та можливого неправомірного використання особистої інформації.

Для підприємств і організацій надзвичайно важливо мати усвідомлення щодо можливих ризиків, пов'язаних із штучним інтелектом, і вживати заходів для захисту особистих даних. Тобто впровадження надійних заходів безпеки, таких як автентифікація та шифрування, а також етичне та відповідальне використання штучного інтелекту. Додатково люди повинні бути обізнані зі своїми правами та вживати заходів для захисту своїх власних даних.

Ризики, пов'язані із штучним інтелектом та захистом особистих даних, є реальними, і їхню важливість не слід недооцінювати. Надзвичайно важливо для забезпечення конфіденційності особистих даних, щоб окремі особи та організації різних форм власності усвідомлювали ці ризики та вживали відповідних заходів для захисту своїх даних, а також забезпечували відповідальне та етичне використання штучного інтелекту.

Аналіз рішень із захисту даних, що використовують штучний інтелект

Засоби захисту даних, які використовують штучний інтелект, стають все більш популярними серед компаній і організацій різних розмірів. Ці засоби використовують розширені алгоритми штучного інтелекту для виявлення та запобігання кібератакам, захисту конфіденційності даних і забезпечення безпеки систем. Незважаючи на багато переваг, які пропонують такі засоби захисту даних, використовуючи штучний інтелект, вони також мають свої потенційні недоліки, що повинні бути враховані.

Переваги рішень із захисту даних, що використовують штучний інтелект:

1. Підвищена точність. Засоби захисту даних, що використовують штучний інтелект, можуть виявляти та запобігати кібератакам з більшою точністю порівняно з традиційними методами безпеки. Алгоритми штучного інтелекту мають змогу швидко обробляти великі обсяги даних і виявляти шаблони, які можуть вказувати на можливу атаку. Тому це дає змогу організаціям залишатися сучасними і мати свої системи, які захищені від останніх загроз.

2. Підвищена ефективність. Засоби захисту даних, що використовують штучний інтелект, мають змогу автоматизувати багато складних і нудних завдань, що пов'язані із традиційними методами безпеки. Це може сприяти економії часу та коштів для організацій і зменшити ризик людських помилок.

3. Покращена видимість. Засоби захисту даних, які використовують штучний інтелект, забезпечують організаціям більш прозору картину стану інформаційної безпеки. Як результат, це допомагає їм виявляти можливі слабкі місця та приймати заходи для їх вирішення ще до того, як виникнуть проблеми.

Недоліки рішень із захисту даних, що використовують штучний інтелект:

1. Висока вартість. Впровадження та підтримка рішень для захисту даних на основі штучного інтелекту може вимагати значних витрат. Організаціям слід враховувати витрати на програмне забезпечення, обладнання та навчання, коли вони вирішують, чи варто інвестувати в такі рішення.

2. Складність. Управління рішеннями для захисту даних на основі штучного інтелекту може бути складним завданням. Організації та підприємства різних форма власності повинні бути впевненими, що вони мають необхідні ресурси та знання для ефективного використання та підтримки таких рішень.

3. Турбота про конфіденційність. Засоби захисту даних на основі штучного інтелекту можуть викликати хвилювання з приводу конфіденційності через можливість збору та зберігання значних обсягів конфіденційної інформації. Організації та підприємства повинні мати впевненість у застосуванні відповідних заходів безпеки для захисту цих даних від несанкціонованого доступу.

Отже, рішення для захисту даних, які використовують штучний інтелект, пропонують численні переваги для організацій, які мають намір підвищити рівень безпеки. Проте важливо враховувати можливі недоліки перед вкладанням коштів у такі рішення. Підприємствам та організаціям варто ретельно вивчити та проаналізувати всі плюси та мінуси, щоб визначити, чи відповідають рішення для захисту даних з використанням штучного інтелекту потребам.

*Л*ітература

1. Виловатых А.В. На пути к теории глобальной безопасности в условиях становления цифровой эпохи. Свободная мысль. 2020. № 4. С. 188–193.

2. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. Int. J. Cyber Warf. Terror. 2016. Vol. 6, pp. 1–16.

3. Применение технологий искусственного интеллекта в информационной безопасности. URL:https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-informationsecurity (дата звернення: 07.12.2021).