Секція 1

ДОСЛІДЖЕННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА КІБЕРБЕЗПЕКУ ВЕБ-ЗАСТОСУНКІВ

Момот О. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В.Я.

Актуальність дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків проявляється у декількох аспектах. Штучний інтелект стає все більш поширеним у різних сферах, включаючи медицину, фінанси, транспорт, комунікації та інші. Застосування штучного інтелекту вимагає глибокого розуміння потенційних загроз для кібербезпеки веб-застосунків, щоб забезпечити їх безпеку та захист від можливих атак. Впровадження штучного інтелекту в кіберзлочинність може призвести до виникнення нових видів атак та методів обхіду захисту [1]. Атаки, які використовують штучний інтелект, можуть бути складнішими для виявлення та захисту, що ставить під загрозу безпеку веб- застосунків та приватність користувачів [2]. Штучний інтелект може використовуватися для аналізу великих обсягів персональних даних, що створює ризик порушення приватності та можливість зловживання цими даними. Захист персональних даних веб-застосунків від штучного інтелекту стає важливою задачею для забезпечення конфіденційності та довіри користувачів. Залежно від типу застосунку, штучний інтелект може бути використаний як інструмент для посилення кібербезпеки або для здійснення шкідливих дій [3]. Це ставить виклик перед розробниками та кібербезпековими експертами для розробки нових стратегій захисту, адаптивних систем та методів виявлення атак, що використовують штучний інтелект. Враховуючи ці аспекти, дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків є актуальним завданням, що допомагає розуміти та адаптуватися до швидкого розвитку технологій, забезпечуючи безпеку, приватність та довіру в онлайн середовищі.

Метою є дослідження впливу штучного інтелекту на кібербезпеку веб-застосунків для розуміння загроз та розробки відповідних стратегій захисту, а також визначення основних проблем та викликів, пов'язаних з впливом штучного інтелекту на кібербезпеку веб-застосунків.

Основні положення. Штучний інтелект може використовуватися як засіб для покращення кібербезпеки веб-застосунків. Однак, він також може бути використаний зловмисниками для здійснення атак та обходу систем захисту, що ставить під загрозу безпеку веб-застосунків. Використання штучного інтелекту може створити нові види загроз для веб- застосунків. Крім того, штучний інтелект може використовуватися для генерації шкідливого коду, фішингу, соціального інжинірингу та інших атак, які

мають великий потенціал завдати шкоди веб-застосункам та користувачам. Для захисту веб-застосунків від впливу штучного інтелекту необхідно розробляти ефективні та адаптивні захисні механізми. Це може включати використання штучного інтелекту для виявлення та відповіді на атаки, розробку алгоритмів виявлення вразливостей та захисту, застосування аналізу поведінки для виявлення аномальних, шифрування та аутентифікації для забезпечення конфіденційності та цілісності даних, а також навчання на основі даних для адаптивного захисту. Впровадження штучного інтелекту в кібербезпеку вимагає врахування етичних та правових аспектів. Наприклад, необхідно уникати дискримінації та недостатньої прозорості в процесі використання штучного інтелекту. Також важливо розробляти стандарти та нормативи, які регулюють використання штучного інтелекту в кібербезпеці, забезпечуючи ефективність та безпеку веб- застосунків [3].

Висновки. Штучний інтелект має значний вплив на кібербезпеку веб-застосунків, вносячи як позитивні, так і негативні аспекти. Забезпечення кібербезпеки веб-застосунків є постійним завданням, яке вимагає постійного моніторингу, аналізу та оновлення захисних механізмів. Впровадження штучного інтелекту в кібербезпеку потребує балансу між використанням його для поліпшення захисту та захисту від нових видів атак, а також урахування етичних та правових аспектів.

Список літератури

1. Herping S. (2019). Securing Artificial Intelligence – Part I. *stiftung-nv*. URL – https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf (дата звернення: 12.06.2023);
2. Pupillo L., Fantin S., Ferreira A., Polito C. (2021). Artificial Intelligence and Cybersecurity. CEPS Task Force Report. *Ceps*. URL – https://www.ceps.eu/wp-content/uploads/ 2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf (дата звернення: 01.06.2023);
3. Hartmann K., Steup C. (2020). Hacking the AI – the Next Generation of Hijacked Systems. In 12 International Conference on Cyber Conflict (CyCon). *doi.org*. URL – https://doi.org/10.23919/CyCon49761.2020.9131724 (дата звернення: 12.06.2023).

Відомості про авторів

Момот Олег Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.o.momot@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu