УДК 004.855

О.О. Щепінська
В.А. Гарнага

ЗАХИСТ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Вінницький національний технічний університет

Анотація

Розглянуто можливості використання штучного інтелекту (ШІ) для підвищення рівня безпеки мобільних операційних систем. Досліджено можливості ШІ для виявлення, аналізу та прогнозування кібератак, автоматизації реагування на інциденти та персоналізації захисту для окремих користувачів.

Ключові слова: Штучний інтелект (ШІ), мобільні операційні системи (ОС), кібербезпека , захист від кіберзагроз, прогнозування кібератак, автоматизація реагування на кібератаки , персоналізація захисту.

Abstract

The possibilities of using artificial intelligence (AI) to increase the level of security of mobile operating systems are considered. The possibilities of AI for detecting, analyzing and predicting cyberattacks, automating response to incidents and personalizing protection for individual users have been explored.

Keywords: Artificial intelligence (AI), mobile operating systems (OS), cyber security, protection against cyber threats, prediction of cyberattacks, automation of response to cyberattacks, personalization of protection.

Вступ

У сучасному світі мобільні пристрої є невід'ємною частиною нашого життя. Ми використовуємо їх для спілкування, роботи, розваг та зберігання особистої інформації. Це робить їх цінними мішенями для кіберзлочинців, які прагнуть отримати доступ до приватної інформації або завдати шкоди нашим пристроям. Традиційні методи захисту мобільних пристроїв, такі як антивірусне програмне забезпечення та брандмауери, не завжди є ефективними проти нових кібератак. Штучний інтелект (ШІ) пропонує нові та інноваційні способи вирішення цієї проблеми.

Результати дослідження

ШІ в сфері безпеки ОС - це велика кількість рішень, які об’єднують в собі аналітичні системи, відеонагляд, системи розпізнавання облич, кібербезпеку та багато іншого. Використання ШІ дозволяє ефективно виявляти, аналізувати та прогнозувати потенційні загрози, забезпечуючи надійний рівень безпеки. Нище розглянуто нові можливості для підвищення рівня безпеки операційних систем [1].

Штучний Інтелект може виявляти аномальну поведінку в системі, що може свідчити про кіберзагрозу. Алгоритми ШІ аналізують дані про використання системи, такі як трафік, активність користувачів, системні процеси, та шукають відхилення від нормальної поведінки. Це може бути ознакою шкідливого програмного забезпечення, спроби несанкціонованого доступу або іншої кібератаки. Наприклад, Алгоритм ШІ може виявити незвичайний трафік з невідомого IP-адреси, що може свідчити про спробу злому [2].

Штучний Інтелект може аналізувати дані про кібератаки в минулому, щоб прогнозувати й запобігати майбутнім атакам. Алгоритми ШІ навчаються на великих масивах даних про кібератаки, щоб ідентифікувати патерни та вчитися на помилках минулого. Це дозволяє їм прогнозувати й запобігати атакам до того, як вони завдають шкоди. Наприклад, Алгоритм ШІ може виявити новий тип шкідливого програмного забезпечення, порівнявши його з відомими зразками, й запобігти його поширенню.

Штучний Інтелект може автоматизувати процес реагування на кібератаки, що може значно скоротити час, необхідний для нейтралізації загрози. Алгоритми ШІ можуть автоматично блокувати шкідливе програмне забезпечення, ізолювати заражені системи, повідомляти про кіберінциденти та вживати інших заходів для мінімізації збитків. Наприклад, Алгоритм ШІ може автоматично заблокувати доступ до шкідливого веб-сайту, щоб захистити користувачів від зараження.

Штучний Інтелект може бути використаний для персоналізації захисту мобільних пристроїв з урахуванням індивідуальних ризиків кожного користувача. Наприклад, ШІ-алгоритм може аналізувати дані про те, як користувач використовує свій мобільний пристрій, щоб визначити, які типи кібератак для нього найбільш ризиковані. Ця інформація може бути використана для налаштування параметрів захисту пристрою відповідно до індивідуальних потреб користувача. Один із прикладів використання ШІ для персоналізації захисту - це система Adaptive Defense от Palo Alto Networks. Adaptive Defense використовує машинне навчання для аналізу трафіку даних на мобільному пристрої. Система може адаптувати параметри захисту пристрою відповідно до типу трафіку, який використовується.

Висновки

Таким чином, штучний інтелект в сфері безпеки має великі перспективи та можливості. Він допомагає покращувати якість та ефективність систем безпеки, забезпечуючи надійний захист від різних загроз. Проте, використання ШІ також вимагає постійного вдосконалення та розвитку, щоб забезпечити безпеку самого ШІ та запобігти його можливому зламу. Використання ШІ в сфері безпеки ОС веде до посилення кіберстійкості та надійності систем, зниження ризиків кібератак та їхніх наслідків, економії часу та ресурсів на реагування в інцидентах, персоналізації захисту та кращого досвіду користувачів. ШІ відкриває нові горизонти в сфері кібербезпеки, роблячи ОС більш стійкими до кіберзагроз та забезпечуючи надійний захист користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Майбутнє ШІ в галузі безпеки. *Worldvision – інтернет магазин систем безпеки*. URL: https://worldvision.com.ua/rol-iskusstvennogo-intellekta-v-sovremennykh-sistemakh-bezopasnosti/ (дата звернення: 29.04.2024).
2. Шість викликів та перспективи сфери безпеки - як впоратися з ними. *Mediacom*. URL: https://mediacom.com.ua/shi-u-sferi-bezpeki-vikliki-ta-perspektivi/ (дата звернення: 29.04.2024).

***ЩЕПІНСЬКА* Оксана Олександрівна** - студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: oksiksu2005@gmail.com

***ГАРНАГА* Володимир Анатолійович** – доцент кафедри Захисту Інформації, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: garnaga.volodymyr@vntu.edu.ua

***SCHEPINSKA* Oksana Oleksandrivna** - student of group 1BS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: oksiksu2005@gmail.com

***HARNAHA* Volodymyr Anatoliyovych** - associate professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: garnaga.volodymyr@vntu.edu.ua