МЕТОДИ ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-РЕСУРСІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Цемма Д.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні WEB-ресурси є невід'ємною складовою цифрової інфраструктури та часто стають об'єктами кібератак. Зростання складності веб-додатків, використання API та мікросервісної архітектури підвищує ризик виникнення вразливостей. У зв'язку з цим актуальним є застосування методів штучного інтелекту (ШІ) та машинного навчання для автоматизації процесів виявлення загроз [1, 2]. **Метою доповіді** є аналіз методів пошуку вразливостей WEB-ресурсів із використанням ШІ та оцінка ефективності їх застосування у сучасних системах кібербезпеки. Основними типами вразливостей веб-додатків залишаються SQL-ін'єкції, XSS, CSRF та інші атаки, що пов'язані з некоректною обробкою даних. В умовах постійного ускладнення атак традиційні методи, засновані на сигнатурному аналізі, стають менш ефективними. Методи машинного навчання дозволяють виявляти аномалії та нові типи атак за рахунок аналізу поведінкових характеристик систем. У сучасних дослідженнях розглядається застосування ШІ для автоматизації тестування на проникнення, що дозволяє значно зменшити участь людини у процесі пошуку вразливостей. Зокрема, використання алгоритмів класифікації та нейронних мереж дозволяє ефективно аналізувати мережевий трафік та поведінку веб-додатків. Крім того, перспективним напрямком є використання інтелектуальних систем для генерації тестових сценаріїв та fuzzing-тестування. Такі системи здатні адаптуватися до структури додатка та знаходити складні логічні помилки, які важко виявити традиційними методами [3].

Дослідження також показують ефективність гібридних підходів, які поєднують класичні методи кібербезпеки з алгоритмами машинного навчання. Це дозволяє підвищити точність виявлення атак, зокрема у випадках zero-day вразливостей та складних багатокрокових атак [3]. Водночас використання ШІ має певні обмеження, зокрема залежність від якості навчальних даних, складність інтерпретації результатів та можливість помилкових спрацювань.

Таким чином, використання методів штучного інтелекту є перспективним напрямком розвитку систем кібербезпеки WEB-ресурсів, що дозволяє автоматизувати процес пошуку вразливостей та підвищити ефективність захисту інформаційних систем.

Список літератури

1. Іваніченко Є., Сабліна М., Кравчук К. Використання машинного навчання в кібербезпеці. Кібербезпека: освіта, наука, техніка. 2021. DOI: https://doi.org/10.28925/2663-4023.2021.12.132142
2. Кавецький, М. С., Сєвєрінов, О. В., Гвоздьов, Р. Ю., Смірнов, А. О. (2024). Використання машинного навчання для класифікації атак типу DOS/DDOS.
3. Савчук К. Гібридні стратегії кібербезпеки для веб-додатків з використанням штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2025. DOI: https://doi.org/10.28925/2663-4023.2025.31.969