Клименко Д. О., магістрант,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ПОВЕДІНКОВИХ ХАРАКТЕРИСТИК ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНОЇ АКТИВНОСТІ НА ВЕБСАЙТАХ

У сучасному світі захист даних вебсайтів є важливим аспектом їх успішного функціонування. Із розвитком технологій зростає і кількість можливостей для зловмисників, нетипові дії яких, порівняно із звичайними користувачами, можуть привести до порушень роботи системи та витоку інформації. Одним із ефективних підходів для виявлення та попередження таких загроз полягає в аналізі поведінкових характеристик користувачів сайту.

У даній статті було проведено аналіз та порівняльне дослідження характеристик аномальних дій користувачів, від чого вони залежать та як відбувається ідентифікація. Також було визначено способи виявлення такої поведінки, проведено аналіз їх ефективності та можливостей.

Поведінкові характеристики можуть включати різноманітні параметри, такі як час перебування на сайті, кількість переглянутих сторінок, активність на різних розділах вебсайту, частота входів, географічне місцезнаходження користувачів, а також їхні інші взаємодії з інтерфейсом сайту. За допомогою таких характеристик можна розпізнавати як нормальну, так і аномальну активність. Наприклад, низька тривалість сеансу в поєднанні з великою кількістю запитів до різних сторінок може сигналізувати про автоматизовану атаку, тоді як стабільно висока взаємодія з певними розділами може свідчити про шахрайську діяльність.

Аномальна активність може бути результатом зловмисних дій, таких як спроби крадіжки даних, введення шкідливих кодів, спам-атаки, або ж шахрайства через фейкові акаунти. Одним із способів виявлення таких аномалій є застосування алгоритмів машинного навчання, які здатні навчатися на вже існуючих даних, визначаючи нормальний шаблон поведінки користувачів, і згодом виявляти будь-які відхилення від цього шаблону.

Існує кілька підходів до застосування машинного навчання для виявлення аномалій, зокрема, методи класифікації, регресії, а також алгоритми для кластеризації [**Ошибка! Источник ссылки не найден.**].

Класифікаційні алгоритми, наприклад дерево рішень, підтримка векторних машин (SVM) або нейронні мережі можуть ефективно класифікувати активність як нормальну чи нетипову [**Ошибка! Источник ссылки не найден.**]. Інші підходи, такі як кластеризація, дозволяють групувати подібні поведінкові шаблони і виділяти аномальні групи, що відрізняються від більшості користувачів.

При визначенні нетипової користувацької активності на вебсайтах також використовуються методи аналізу часових рядів. Це дозволяє визначити аномалії, що проявляються у часових інтервалах між взаємодіями користувачів з сайтом.

Для аналізу поведінки користувачів вебсайтів важливо також враховувати динамічні аспекти. Поведінка користувача може змінюватися в часі залежно від різних факторів, таких як зміни в контенті сайту або зміни в політиці безпеки. Даний аспект може приводити до хибнопозитивних результатів роботи алгоритмів. Тому системи, які використовують підходи із машинним навчанням, повинні мати можливість адаптуватися до нових умов та оновлюватись відповідно до нових заданих параметрів та даних [**Ошибка! Источник ссылки не найден.**].

Важливим аспектом є також інтеграція з системами безпеки, такими як системи виявлення вторгнень (IDS), для оперативного реагування на загрози. Виявлення аномалій у реальному часі дає змогу вчасно сповістити адміністратора сайту або активувати автоматичні заходи для захисту користувачів і даних.

Отже, використання поведінкових характеристик для виявлення аномалій є потужним інструментом у сфері кібербезпеки. Водночас важливо зазначити, що для досягнення високої ефективності таких систем необхідно використовувати сучасні алгоритми машинного навчання, що мають змогу адаптуватися до нових загроз та тенденцій поведінки користувачів.

Список використаних джерел

1. Anomaly Detection Using AI & Machine Learning. Nile [Електронний ресурс] / A. Carrillo – Режим доступу до ресурсу: https://nilesecure.com/ai-networking/anomaly-detection-ai.
2. AI in anomaly detection. LeewayHertz. [Електронний ресурс] / A. Carrillo – Режим доступу до ресурсу: https://www.leewayhertz.com/ai-in-anomaly-detection.
3. Adopting AI for Anomaly Detection. Eyer. URL: https://eyer.ai/blog/adopting-ai-for-anomaly-detection-a-primer.