УДК 004.942

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ НА ВЕБ-РЕСУРСЕ

Авчин А.А. (ИТМО)

Научный руководитель – кандидат технических наук, доцент ФБИТ Менщиков А.А. (ИТМО)

Введение. Растет число атак с перехватом аккаунта (ATO – от англ. Account Takeover) и потери от них [1]. Межсетевые экраны веб-приложений (WAF) используют подходы, направленные на выявление статистических выбросов (DoS, брутфорс) и поиск запросов с аномальным содержанием (SQLi, XSS и пр.), однако для выявления ATO требуется другой подход, связанный с анализом поведения. Актуальность проблемы связана со слабой исследованностью темы выявления ATO, что обусловлено отсутствием пригодного открытого набора данных [2].

Основная часть. Методы машинного обучения широко исследованы и применяются для анализа поведения пользователей (UBA – от англ. User Behavior Analysis) в информационных системах. Популярным подходом является обучение на нормальном поведении пользователей и последующее обнаружение аномалий в их действиях. Наиболее актуальными моделями являются рекуррентные сети на основе LSTM и GRU [3]. Они предназначены для моделирования последовательностей событий, поэтому отлично подходят для анализа сеанса пользователя. Действия пользователя на сайте также можно рассматривать как поведение в информационной системе, поэтому к нему применим поведенческий анализ.

Для анализа такого поведения необходимо определить данные, на основе которых будет проводиться классификация. Такими данными могут выступать параметры HTTP-запроса (метод, URI, параметры), данные об устройстве пользователя, действия пользователя на сайте, временные параметры его поведения (период активности, скорость действий). Анализ эффективности методов, применяющихся в UBA, необходимо проводить на реальных или приближенных к реальным данных, поэтому для их сбора используются действия реальных пользователей.

Выводы. Для решения задачи обнаружения ATO возможно применять методы машинного обучения, аналогичные используемым в UBA. Для оценки их применимости необходимо провести эксперимент по оценке моделей на эффективность. Для оценки применительности методов UBA к задаче обнаружения ATO определены признаки и исходные данные, основанные на запросах к реальному веб-приложению.

Список использованных источников:

1. Javelin: «ATO Fraud: Why It Remains FIs' Greatest Fraud Risk» [Электронный ресурс]. Режим доступа: https://javelinstrategy.com/research/ato-fraud-why-it-remains-fis-greatest-fraud-risk (дата обращения: 26.11.2024).
2. Jurišić M., Tomičić I., Grd P. User behavior analysis for detecting compromised user accounts: A review paper //Cybernetics and Information Technologies. – 2023. – Т. 23. – №. 3. – С. 102-113.
3. Al-Mhiqani M. N. et al. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations //Applied Sciences. – 2020. – Т. 10. – №. 15. – С. 5208.