УДК 004.056

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ В СОВРЕМЕННЫХ СРЕДСТВАХ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ

Калугина А.С. (Университет ИТМО),
Научный руководитель – доктор технических наук, профессор практики Лившиц И.И.
(Университет ИТМО)

Введение. Традиционные продукты кибербезопасности не обеспечивают полного представления о деятельности пользователей внутри организации [1]. В корпоративной безопасности одним из ключевых аспектов является обнаружение скомпрометированных учетных записей пользователей, а также внутренних нарушителей в частности, когда в компании имеется множество сценариев и различные сетевые сегменты. Если действия скомпрометированного пользователя сильно отличаются от повседневных обязанностей пользователя, то необходимо собирать поведенческий профиль пользователя и исследовать любые отклонения от этого базового профиля, которые можно пометить как потенциальную аномалию [2].

Основная часть. В докладе рассматриваются различные алгоритмы от машинного обучения до глубокого обучения. Каждый из методов используется в зависимости от необходимости анализа и набора данных. Также рассмотрены параметры пользователей, по которым формируются шаблоны поведения пользователей и выявлены параметры, для которых необходимо формировать шаблоны поведения [3].

Выводы. В работе представлен результат анализа перспектив применения алгоритмов машинного обучения в современных средствах поведенческой аналитики. Выявлены недостатки и проблемы, возникающие при формировании шаблона поведения пользователей в зависимости от используемого алгоритма, различные подходы, используемые в аналитике поведения пользователей и объектов, включая обнаружение пользователей и ролей, сопоставление активности пользователей и объектов, методы профилирования пользователей и другие.

Список использованных источников:

1. Salman Khaliq; Zain Ul Abideen Tariq; Ammar Masood, Prof. Role of User and Entity Behavior Analytics in Detecting Insider Attacks [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/abstract/document/9292394, свободный. Яз. англ. (дата обращения 01.02.2024).
2. Raguvir. S, Prof. Shekar Babu. Detecting Anomalies in Users – An UEBA Approach [Электронный ресурс]. – URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ieomsociety.org/ieom2020/papers/632.pdf, свободный. Яз. англ. (дата обращения 01.02.2024).
3. Pratik Dhaygudea, Nilesh Dhulshettea, Omkar Ganjalea. A Review Paper on Different Deep Learning Methodologies for User and Entity Behavior Analytics (UEBA) [Электронный ресурс]. – URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ijrpr.com/uploads/V4ISSUE5/IJRPR13230.pdf, свободный. Яз. англ. (дата обращения: 01.02.2024)

Калугина А.С. (автор) Подпись

Лившиц И.И. (научный руководитель) Подпись