УДК 004.056.5

ЗЛОНАМЕРЕННОЕ ПОВЕДЕНИЕ И ФОРМИРОВАНИЕ ПРОФИЛЯ ЗЛОУМЫШЛЕННИКА В LMS СИСТЕМЕ

Еритенко Н.А. (ИТМО), **Менщиков А.А.** (ИТМО)
Научный руководитель – кандидат технических наук, доцент Заколдаев Д.А. (ИТМО)

Введение. Злонамеренное поведение в информационной системе может проявляться через недобросовестные действия с функционалом системы, такие как недействительные просмотры и клики, DoS, фишинг, получение несанкционированного доступа к информации и др. Хорошо изученным классом информационных систем в данном контексте в современной научной литературе являются социальные сети [1] [2]. Класс систем управления обучением или LMS (Learning Management System) имеет свою специфику в контексте рассмотрения вопроса о злонамеренном поведении и, как следствие, особенности формирования профиля злоумышленника.

Основная часть. Самым очевидным объектом исследования вопроса злонамеренного поведения могут послужить социальные сети. Целый ряд работ посвящен исследованию злонамеренного поведения в социальной сети, имеющий собственную специфику и особенности. Так, в работе R.Ikwu [2], исследуется Twitter как площадка для распространения вредоносного кода в социальных сетях, осуществленного скоординированной деятельностью вступивших в сговор групп злоумышленников, скрывающихся за несколькими цифровыми личностями.

На большинстве платформ нелегко установить разницу между злонамеренными пользователями, представляющими опасность для сообщества, и неактивными пользователями, которые редко взаимодействуют с другими. Поскольку злоумышленники хорошо осведомлены об этом, они могут внедрять множество ботов / поддельных профилей, которые невозможно сразу обнаружить и удалить.

Важной вехой в изучении злонамеренного поведения посредством цифровых технологий являются скомпрометированные пользователи. Компрометация учетной записи представляет серьезную угрозу для всех пользователей и для пользователей социальных сетей, в частности.

Социальное поведение пользователей может иметь различную классификацию. Нарушитель и злоумышленник могут быть не только внешним по отношению к рассматриваемой системе, но и внутренним. Выбранная классификация, «природа» злоумышленника и другие параметры накладывают свою специфику на формирование профиля.

LMS-системы значительно отличаются от широко изученных социальных сетей, но, тем не менее, имеют множество общих черт. Детальное изучение имеющихся различностей и общностей является необходимым шагом для алгоритмизации формирования профиля злоумышленника в LMS-подобных системах.

Выводы. В большинстве случаев в качестве инструмента классификации полученного профиля используют алгоритмы искусственного интеллекта, реже - математические алгоритмы.

Общим недостатком можно выделить создание специфической модели под конкретную задачу и набор данных. Обобщенные алгоритмы и феймворки, на примере UEBA [3], обладают узостью рассматриваемых данных и в полной мере не охватывают пространство возможных параметров, по которым можно было бы определить злоумышленника. Кроме того, рассмотренные системы основаны на изученных и обученных данных и датасетах в определенной конфигурации информационной системы, что исключает предиктивность в

случае изменения протокола или введения новых функциональных элементов информационной системы.

Рассмотренные аспекты LMS-подобных систем показывают необходимость специфического подхода к формированию профиля злоумышленника и обеспечения информационной безопасности целевой информационной системы.

Список использованных источников:

1. Al-Qurishi et al. Leveraging Analysis of User Behavior to Identify Malicious Activities in Large-Scale Social Networks // IEEE Transactions on Industrial Informatics. – Vol. 14. – No. 2. – pp. 799-813. – 2018.
2. Ruth et al. Digital fingerprinting for identifying malicious collusive groups on Twitter // Journal of Cybersecurity. – Volume 9. – Issue 1. – 2023.
3. Khaliq S et al. Role of User and Entity Behavior Analytics in Detecting Insider Attacks // 2020 International Conference on Cyber Warfare and Security (ICCWS). – pp. 1-6.