

УДК 004.8

РАЗРАБОТКА АЛГОРИТМА ПРОГНОЗИРОВАНИЯ ВЕКТОРОВ АТАК ЗЛОУМЫШЛЕННИКОВ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ С ПРИМЕНЕНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ ПРОГНОЗНЫХ МОДЕЛЕЙ.

Горбунов К.Д. (ИТМО)

Научный руководитель – кандидат физико-математических наук, доцент Иванов С.Е. (ИТМО)

Введение. Рост и развитие цифровизации и информационных технологий непременно сопровождаются увеличением количества атак злоумышленников на информационные системы. Атаки становятся все более сложными и изощренными, регулярно появляются новые техники, которыми руководствуются злоумышленники. Более того, атака не происходит в моменте, обычно это определенная последовательность действий, приводящая к успешной эксплуатации какой-либо уязвимости. Таким образом, актуальным аспектом информационной безопасности является разработка алгоритма прогнозирования векторов атак злоумышленников на информационные системы. Использование интеллектуальных прогнозных моделей, таких как алгоритмы Apriori и FP-Growth, может позволить выявлять закономерности в массиве данных и прогнозировать возможные сценарии действий злоумышленников [1]. Данный подход особенно актуален в контексте работы с большими объемами данных, где превосходят по своей эффективности традиционные методы анализа [2].

Основная часть. Целью исследования является разработка алгоритма прогнозирования векторов атак злоумышленников на информационные системы с применением интеллектуальных прогнозных моделей.

Для успешного достижения цели работы были определены следующие задачи:

- 1) Определение бизнес-ограничений для работы алгоритма;
- 2) Определение ограничений ИТ-ресурсов;
- 3) Обзор литературы по прогнозным моделям Apriori и FP-Growth [3];
- 4) Составление датасета на основе открытых источников данных об угрозах информационной безопасности;
- 5) Анализ эффективности работы алгоритмов на выбранном датасете, доработка параметров моделей для достижения наилучших результатов;
- 6) Валидация полученных результатов.

Выводы. Разработан алгоритм прогнозирования векторов атак злоумышленников на информационные системы с применением интеллектуальных прогнозных моделей. Определены оптимальные параметры прогнозных моделей, позволяющие достичь наибольшей точности прогнозов.

Список использованных источников:

1. Пальмов С.В., Франузова Е.Н. Алгоритм поиска ассоциативных правил FP-GROWTH // Национальная ассоциация ученых. – М.. Изд-во: ООО «Евразийское Научное Содружество», 2016. – № 10-1 (26). – С. 27-32.
2. Газиев Г.З., Курдюкова Г.Н., Курдюков В.В. Кластеризация Big Data для их анализа и обработки // Сб. конференции «Направления и механизмы развития науки нового времени: от теории до внедрения результатов». – 2017. – С. 150-162.
3. Бова В.В., Кулиев Э.В., Щеглов С.Н. Оценка эффективности метода поиска ассоциативных правил для задач обработки больших данных // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2020. – № 2. – С. 66–78. – УДК 004.853. DOI: 10.18522/2311-3103-2020-2-66-78.