УДК 004.056

МЕТОД АВТОМАТИЧЕСКОГО ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ОБЪЕКТОВ НА ИЗОБРАЖЕНИИ

Бучаев А.Я. (Университет ИТМО),
Научный руководитель – доцент, кандидат технических наук Попов И.Ю.
(Университет ИТМО)

Введение. В настоящее время многие организации проходят этап цифровизации, соответственно их инфраструктура растет, многие услуги переходят в онлайн, а режим работы постепенно переходит от гибридного к удаленному. В такой парадигме растет децентрализованность трафика и степень угроз заражения и будущей активности вредоносного ПО для организации. Корпоративные сети имеют плавный характер изменения интранета, смена состояний устройств внутренней сети имеет является линейным процессом, в течение которого возникают новые угрозы. Существующие методы машинного обучения или правила, фиксирующие нетипичное сетевое взаимодействие, являются субъективными системами и требуют периодического обслуживания и обновления сигнатурной или эвристической базы [1]. Таким образом, существующие риски информационной безопасности не снижаются, а финансовые траты на обеспечение достаточной степени охвата угроз только растут. Целью данной работы является разработка метода отбора информативных признаков при характеристике устройств в корпоративной сетевой инфраструктуре.

Основная часть.

В текущей работе представлен метод отбора информативных признаков, характеризующих устройство в сетевой инфраструктуре, для формирования вектора-описателя [2].

Использование вектора-описателя устройства в сети решает задачу характеристики устройства, а не классификации на вредоносное или легитимное. Исходя из задачи характеристики, были выбраны показатели, основанные на работе устройства в сети. Важно отметить, что некоторые из них носят характер временного ряда, что означает важность упорядоченности полученных значение, в то время как другие показатели не характеризуются временной шкалой и ранжированием. Следующие показатели работы устройства в сети определены общим принципом работы сетевого устройства:

1. информация о длине пакета (временной ряд);
2. задержка между отправками пакетов (временной ряд);
3. количество взаимодействий с уникальными хостами (временной ряд);
4. количество взаимодействий по портам получателя;
5. количество взаимодействий по исходным портам;
6. количество попыток установить сессию;
7. количество установленных сессий;
8. количество успешно завершенных сессий.

Совокупность предложенных информативных признаков сетевых устройств позволяет характеризовать взаимодействие устройства с другими конечными точками в сетевой инфраструктуре. Однако присутствие категориальных признаков затрудняет проведение достоверной оценки линейности переходов. В таком случае необходимо выбрать объективный подход кодирования категориальных признаков, обеспечивающий достоверную оценку расстояния между объектами, обладающими закодированными признаками. Иным способом представление категориальных признаков является конвертация их абсолютную шкалу.

Выводы. В данной работе представлен метод отбора информативных признаков сетевых устройств. Представленный метод характеризуется прозрачностью, универсальность и низкой вычислительной требовательностью. Далее планируется применение и анализ полученных путем отбора признаков векторов-описателей при мониторинге в режиме реального времени.

Список использованных источников:

1. Перегуда А. И. Математическая модель надёжности информационных систем с системами безопасности //Успехи кибернетики. – 2022. – Т. 3. – №. 1. – С. 39-43
2. Мещеряков Р.В., Исхаков С.Ю. Исследование методов формирования индикаторов компрометации от внутренних источников информационных и киберфизических систем//Вопросы кибербезопасности. – 2023. – №. 6(58). – С. 35-49.

Бучаев А.Я. Подпись

Попов И.Ю. (научный руководитель) Подпись