УДК 004.056

УСЛОВИЯ РАЗДЕЛИМОСТИ ГРУППЫ ОБЪЕКТОВ В ЗАДАЧЕ БИНАРНОЙ КЛАССИФИКАЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Введение. Согласно статистическим данным компании Positive Technologies за 2023–2024 годы, количество инцидентов ИБ в среднем возросло на 16 % за год [1]. Подвержены атакам оказались государственные учреждения и объекты КИИ, а точками входа злоумышленников стали элементы сетевой инфраструктуры. Обнаружение аномалий в сетевом трафике является активно развивающейся областью, в которой выделяются три основных направления: сигнатурные методы, статистические методы и методы на основе машинного обучения. Однако сигнатурные методы и решения на основе машинного обучения обладают рядом недостатков. Использование формализованных статистических методов в задачах мониторинга информационной безопасности обеспечивает интерпретируемость и прозрачность промежуточных и конечных результатов работы, что является важной задачей в условиях оперативного реагирования или в процессе расследования инцидентов информационной безопасности.

Основная часть.

Для определения событий информационной безопасности в корпоративной компьютерной сети предлагается использовать формальный метод бинаризации Оцу [2]. Однако есть ряд ограничений классического метода Оцу, которые не позволяет обеспечить достоверность выходных результатов. В текущей работе представлены и аргументированы условия, при которых бинарное разделение группы объектов, представленных векторами состояний устройств в корпоративной компьютерной сети, с помощью бинаризации Оцу является корректным в заданных условиях.

Такое разделение является эмпирическим, поэтому в работе предлагается доказательство эквивалентности порога Оцу и границы решения MAP-классификатора.

Выводы. В данной работе представлены условия разделимости группы объектов в задаче бинаризации событий информационной безопасности, а также доказывается эквивалентность порога Оцу и границы решения MAP-классификатора. Метод бинаризации, учитывающий эти условия обеспечивает достоверность выходных результатов разделения группы, интерпретируемость и прозрачность механизма принятия решения.

Список использованных источников:

1. Перегуда А. И. Математическая модель надёжности информационных систем с системами безопасности //Успехи кибернетики. – 2022. – Т. 3. – №. 1. – С. 39-43 Positive Technologies. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 10.02.2026)

2. Otsu, N. A Threshold Selection Method from Gray-Level Histogram // IEEE Transactions on Systems, Man, and Cybernetics. — 1979. — Vol. SMC-9, No. 1. — P. 62–66.

Бучаев А.Я. Подпись

Попов И.Ю. (научный руководитель) Подпись