УДК 004.056.2

МЕТОД АВТОМАТИЧЕСКОГО ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ОБЪЕКТОВ НА ИЗОБРАЖЕНИИ

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

Введение. Одним из направлений обеспечения информационной безопасности является построение математических моделей решения частных задач в рамках заданных условий. Общей задачей при формировании конечного решения является обоснование и выбор информативных признаков, определение способа их представления и разработка/адаптация универсальных математических моделей для получения требуемого результата. Теоретические модели решения частных задач обеспечения ИБ находят практическое применение в реализации программно-аппаратных систем с учётом экономических аспектов, определяемых универсальными технико-экономическими показателями: эффективности, стоимости разработки (производства, приобретения), стоимости владения и т.п. Целью работы является повышение эффективности обнаружения искаженных и нетипичных данных. В работе предлагается обладающий общностью метод обнаружения аномалий в пространстве событий ИБ вне зависимости от способа формирования описателей совокупности событий.

Основная часть.

В текущей работе представлен автоматический метод обнаружения аномальных элементов пространства событий. В качестве входных данных был взят набор изображений, содержащих однородную среду и несколько аномальных объектов, машины, кусты, дорога и тд. В контексте цели исследования ставится задача: найти аномалии в представленном наборе данных, характеризующиеся линейными зависимостями между смежными элементами.

Гипотеза: изменения между соседними участками изображения описываются линейными зависимостями.

Обоснование: в случае появления или наличия аномального объекта происходит нарушения однородности рассматриваемого участка изображения, следовательно, статистические показатели текущего фрагмента имеют аномальные значения относительно смежных фрагментов.

Задача автоматического обнаружения аномалий в пространстве событий информационной безопасности решается в несколько этапов:

1. отбор доступных для наблюдения информативных признаков, характеризующих состояние ИБ ИС с использованием известных и развивающихся подходов [1];
2. формирования вектора-описателя состояния системы/компонента, например [2], с возможным снижением размерности пространства признаков;
3. при необходимости – трансформация вектора-описателя, введение метрического пространства и определение способа расчёта близости наблюдаемых значений, например [3, 4];
4. определение статистических характеристик состояния системы, описанных зафиксированными векторами-описателями;
5. выделение точек аномалий, характеризующихся нарушением статистических закономерностей;
6. анализ точек аномалий; при наличии ретроспективной базы данных шаблонов аномалий – распознавание типа аномалии.

Для проверки гипотезы проведён анализ статистических характеристик шумовой компоненты исходного изображения [5]. В ходе проведения исследования были сформированы вектора, описывающие совокупность статистических характеристик разделенного изображения, включая характеристики отдельных упорядоченных фрагментов. В соответствии с оценкой полученных характеристик выстраивается тепловая карта степени

аномальности фрагментов, которые классифицируется по порогу, вычисляемому автоматически.

Выводы. В данной работе представлен метод обнаружения искаженных и нетипичных элементов в пространствах событий информационной безопасности. Представленный подход характеризуется прозрачностью, универсальность и низкой вычислительной требовательностью. Далее планируется повышение точности определения нетипичных объектов, а также распознавание локальных объектов внутри глобальных аномалий.

Список использованных источников:

1. Семенов В. В. Подход к формированию информативных признаков в задачах мониторинга информационной безопасности киберфизических систем //Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21. – №. 6. – С. 887-894.
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.
3. Ишкуватов С.М., Швед В. Г., Филькова И. А. Метод оценки близости цифровых отпечатков реализаций протоколов // Защита информации. инсайд. – 2022. - №2 (104). – С. 29-33.
4. Ишкуватов С.М., Комаров И.И. Анализ аутентичности трафика на основании данных цифровых отпечатков реализаций сетевых протоколов // Научно-технический вестник информационных технологий, механики и оптики. - 2020. Т. 20. № 5. С. 747–754.
5. K. Wang, X. Yu and S. Gou, "Classification of Heterogeneous Scenes in POL-SAR Image Based on Statistical Analysis," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 2164-2169.

Бучаев А.Я. Подпись

Попов И.Ю. (научный руководитель) Подпись