УДК 004.056.2

Разработка алгоритма обнаружения атак в компьютерных сетях на основе микросегментации с использованием предобработки трафика

Пастухова А.А. (ИТМО), **Колесников Н.Д.** (ИТМО)
Научный руководитель – ассистент Есипов Д.А. (ИТМО)

Введение. Микросегментация применяется в крупных сетях все чаще, ввиду ее удобства отдельных рабочих зон, разделения ресурсов и изолирования последствий атак, однако это не отменяет ряд сопутствующих проблем, например, горизонтальное распространение угроз и снижение производительности средств защиты данных. Помимо явной необходимости отслеживания входящего трафика стоит вопрос в выделении аномальной активности и верификации угроз безопасности. Таким образом, повышение точности обнаружения аномальной активности во внутреннем сегменте сети при использовании микросегментации, что является действительно актуальной задачей.

Основная часть. В рамках данной работы предполагается работа со смешанными сетями, включающими в себя IP-based и SDN компьютерные сети. Последнее очевидно усложнено собственной архитектурой – несколько уровней маршрутизации данных и дополнительные контроллеры, что вызывает дополнительные сложности в реализации алгоритма. Несмотря на их различия, в результате перехода от классических сетей к сегментированным происходит ситуация, когда на протяжении длительного срока данные сети по факту соседствуют.

Важно отметить, что разработка алгоритма обнаружения атак в IP-сетях и SDN-сетях происходит после предобработки трафика [1]. С этой целью уже готовые наборы данных из открытых источников приводятся к оптимальному состоянию с помощью выборки определенных признаков [2] и устранения дисбаланса классов за счет искусственного дополнения методом SMOTE [3]. Затем проверяется трафик между крупными сегментами сети и внутри каждой отдельной части. Результаты выводятся в отдельный файл в конкретном формате для дальнейшего анализа.

Валидация аномальной активности с использованием методов машинного обучения происходит только после того, как алгоритм зафиксирует подозрительные действия в ходе анализа сегментов.

Выводы. После анализ трафика между устройствами в микросегменированных сетях происходит выделение отклонений от стандартного представления передачи данных, среди которых и фиксируются атаки информационной безопасности. В дальнейшем планируется выполнить программную реализацию алгоритма и повысить его эффективность, используя различные наборы входных данных.

Список использованных источников:

1. Hela Mliki, Abir Hadj Kaceam, Lamia Chaari. A Comprehensive Survey on Intrusion Detection based Machine Learning for IoT Networks // EAI. – 2021. – Ч. 6. – С. 10-13.
2. Furqan Rustam, Anca Delia Jurcut. Malicious traffic detection in multi-environment networks using novel S-DATE and PSO-D-SEM approaches // Computers & Security 136. – 2024. – Ч. 6.4. – С. 11-12.
3. Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad. Network intrusion detection system: A systematic study of machine learning and deep learning approaches // Wiley. – 2020. – Ч. 4.3.5. – С. 12-17.