УДК 004.056.5:004.8

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ

Хазиев Г.Р.[1], Золотухин А.А.[1] , Курдай Н.В.[1]
Научный руководитель – кандидат военных наук, доцент Федирко А.А.[1]
[1]Военно-космическая академия имени А.Ф.Можайского

Введение

Современные информационные системы функционируют в условиях постоянного роста объёма сетевого трафика и увеличения числа кибератак различной природы. Традиционные сигнатурные методы обнаружения вторжений демонстрируют высокую эффективность при выявлении известных угроз, однако оказываются недостаточно результативными при анализе ранее неизвестных атак и сложных многоэтапных сценариев. В условиях динамически изменяющейся сетевой среды актуальной задачей становится разработка интеллектуальных систем, способных выявлять отклонения от нормального поведения трафика без предварительного знания конкретных сигнатур атак. Одним из перспективных направлений является применение нейросетевых моделей для построения систем обнаружения аномалий, основанных на анализе статистических и поведенческих характеристик сетевого взаимодействия. Использование методов машинного обучения позволяет формировать адаптивные модели нормального состояния сети и выявлять аномальные события, потенциально свидетельствующие о нарушении информационной безопасности.

Основная часть

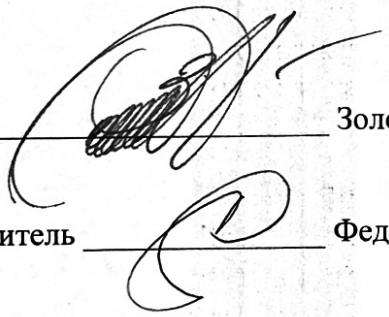
Предлагаемый подход основан на построении интеллектуальной системы анализа сетевого трафика, включающей этапы сбора, предобработки, обучения и выявления аномалий. На этапе сбора данных формируется поток признаков, характеризующих сетевые соединения: длительность сессии, объём переданных данных, число пакетов, направления обмена, используемые протоколы и временные интервалы между пакетами. Полученные данные агрегируются и преобразуются в структурированное представление, пригодное для последующей обработки нейросетевыми алгоритмами. В качестве модели обнаружения аномалий рассматривается использование автоэнкодеров и рекуррентных нейронных сетей. Автоэнкодер обучается на нормальном трафике и формирует компактное латентное представление сетевых характеристик. При поступлении аномального трафика ошибка реконструкции существенно возрастает, что позволяет интерпретировать данное событие как потенциальную угрозу. Рекуррентные архитектуры, в свою очередь, позволяют учитывать временную динамику сетевых процессов и выявлять последовательностные аномалии, характерные для распределённых атак и сканирования. С целью повышения устойчивости системы применяется механизм адаптивной калибровки порога аномальности, учитывающий текущую нагрузку сети и сезонные изменения трафика. Дополнительно реализуется модуль кластеризации обнаруженных аномалий, позволяющий группировать события по степени сходства и формировать приоритеты реагирования. Интеллектуальная система интегрируется в инфраструктуру мониторинга и обеспечивает формирование структурированных уведомлений, содержащих характеристики выявленного отклонения, уровень риска и рекомендации по дальнейшему анализу. Такой подход позволяет снизить нагрузку на аналитиков и повысить скорость реагирования на инциденты информационной безопасности.

Выводы

Разработанный подход к обнаружению аномалий в сетевом трафике на основе нейросетевых моделей обеспечивает возможность выявления ранее неизвестных угроз без использования сигнатурных баз. Применение автоэнкодеров и рекуррентных архитектур позволяет учитывать как статистические характеристики трафика, так и его временную динамику. Интеграция интеллектуального модуля в систему мониторинга способствует повышению адаптивности и эффективности защиты информационных систем. Дальнейшие исследования могут быть направлены на расширение набора используемых признаков, оценку устойчивости модели к атакам типа adversarial, а также на проведение сравнительного анализа эффективности различных архитектур нейронных сетей в задачах сетевой безопасности.

Литература

1. Bishop C. M. Pattern Recognition and Machine Learning [Электронный ресурс]. – URL:https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf – (дата обращения 14.03.2025).
2. Goodfellow I., Bengio Y., Courville A. Deep Learning [Электронный ресурс]. – URL: https://www.deeplearningbook.org/ – (дата обращения 28.04.2025).
3. IEEE Communications Surveys & Tutorials [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9040692 – (дата обращения 12.05.2025).
4. DD Cup 1999 Data Set [Электронный ресурс]. – URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html – (дата обращения 21.03.2025).
5. Canadian Institute for Cybersecurity. CIC-IDS2017 Dataset [Электронный ресурс]. – URL: https://www.unb.ca/cic/datasets/ids-2017.html – (дата обращения 05.05.2025).



Автор _____ Золотухин А.А.

Научный руководитель _____ Федирко А.А.

Выводы

Разработанный подход к обнаружению аномалий в сетевом трафике на основе нейросетевых моделей обеспечивает возможность выявления ранее неизвестных угроз без использования сигнатурных баз. Применение автоэнкодеров и рекуррентных архитектур позволяет учитывать как статистические характеристики трафика, так и его временную динамику. Интеграция интеллектуального модуля в систему мониторинга способствует повышению адаптивности и эффективности защиты информационных систем. Дальнейшие исследования могут быть направлены на расширение набора используемых признаков, оценку устойчивости модели к атакам типа adversarial, а также на проведение сравнительного анализа эффективности различных архитектур нейронных сетей в задачах сетевой безопасности.

Литература

1. Bishop C. M. Pattern Recognition and Machine Learning [Электронный ресурс]. – URL:https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf – (дата обращения 14.03.2025).
2. Goodfellow I., Bengio Y., Courville A. Deep Learning [Электронный ресурс]. – URL: https://www.deeplearningbook.org/ – (дата обращения 28.04.2025).
3. IEEE Communications Surveys & Tutorials [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9040692 – (дата обращения 12.05.2025).
4. DD Cup 1999 Data Set [Электронный ресурс]. – URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html – (дата обращения 21.03.2025).
5. Canadian Institute for Cybersecurity. CIC-IDS2017 Dataset [Электронный ресурс]. – URL: https://www.unb.ca/cic/datasets/ids-2017.html – (дата обращения 05.05.2025).