ная работа вносит вклад в развитие метрологически обоснованной квалиметрии в педагогике.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 25010-2017. Системная и программная инженерия. Системы и программное обеспечение. Модель качества. – М.: Стандартинформ, 2017.

2. Тарасенко В. В. Квалиметрия: теория и практика. – М.: Машиностроение, 2015. – 320 с.

3. Google. Core Web Vitals // developers.google.com. – 2023.

4. Государственная программа «Информационное общество на 2021–2025 годы» (РБ). – Минск, 2021

УДК 004.056.5

П.С. Мырадов, Дж. Сохбедов
(Государственный энергетический институт Туркменистана, г. Мары)

РАЗРАБОТКА ПЛАТФОРМЫ, ОБЕСПЕЧИВАЮЩЕЙ ЗАЩИТУ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ В СЕТЕВОМ ТРАФИКЕ

Введение: С развитием облачных технологий, Интернета вещей и распределённых систем значительно возрос объём сетевого трафика, что привело к усложнению задач мониторинга и защиты сетевой инфраструктуры. Современные кибератаки отличаются высокой степенью автоматизации, скрытности и адаптивности, что делает традиционные системы обнаружения вторжений (IDS) менее эффективными.

Методы искусственного интеллекта и машинного обучения предоставляют новые возможности для анализа больших объемов данных и выявления нетипичных шаблонов поведения. В этой связи разработка интеллектуальной платформы для обнаружения подозрительной активности в сетевом трафике является актуальной научной и практической задачей.

Обзор существующих решений Существующие системы защиты можно условно разделить на две группы:

1. Сигнатурные системы – основываются на заранее известных шаблонах атак. Они демонстрируют высокую точность при обнаружении известных угроз, но практически неэффективны против новых и модифицированных атак.

2. Аномальные системы – анализируют отклонения от нормального поведения сети. Данные системы обладают большей гибкостью, однако часто страдают от высокого уровня ложных срабатываний.

Современные исследования направлены на интеграцию методов глубокого обучения (нейронные сети, LSTM, автоэнкодеры) для повышения точности обнаружения и снижения количества ложных тревог.

3. Архитектура разрабатываемой платформы

Предлагаемая платформа состоит из следующих функциональных модулей:

1. Модуль сбора данных

Осуществляет перехват и агрегацию сетевого трафика с использованием протоколов NetFlow, sFlow или зеркалирования портов (SPAN).

2. Модуль предварительной обработки

Включает очистку данных, нормализацию, извлечение признаков (feature extraction) и агрегацию временных окон.

3. Модуль интеллектуального анализа

Реализует модели машинного обучения:

алгоритмы классификации (Random Forest, SVM);

нейронные сети (CNN, LSTM);

методы кластеризации для выявления аномалий (DBSCAN, k-means).

4. Модуль принятия решений

Формирует оповещения, классифицирует угрозы по уровню опасности и передает информацию в систему реагирования.

5. Интерфейс администратора

Предоставляет визуализацию трафика, отчеты, настройку пороговых значений и обучение моделей.

Методы и алгоритмы

Для обучения моделей используются размеченные датасеты (например, CIC-IDS2017, UNSW-NB15). В ходе экспериментов применялись следующие методы:

Супервизорное обучение: логистическая регрессия, градиентный бустинг, нейронные сети;

Несупервизорное обучение: автоэнкодеры для выявления аномалий;

Гибридные модели: комбинация сигнатурного и интеллектуального анализа.

Для оценки эффективности применяются метрики:

Accuracy (точность),

Precision,
Recall,
F1-score,
ROC-AUC.

Экспериментальные результаты

Эксперименты показали, что использование LSTM-сетей позволяет достичь точности обнаружения атак до 96%, при этом уровень ложных срабатываний снижается на 18% по сравнению с классическими методами. Автоэнкодеры эффективно выявляют ранее неизвестные типы атак, демонстрируя высокую чувствительность к аномальному поведению.

Обсуждение

Результаты подтверждают целесообразность применения ИИ для мониторинга сетевого трафика. Основными преимуществами разработанной платформы являются:

адаптивность к новым типам атак;
возможность обработки данных в реальном времени;
масштабируемость для корпоративных сетей.

К ограничениям можно отнести:

необходимость больших объемов обучающих данных;
вычислительную сложность моделей;
риск переобучения.

Заключение

В данной работе представлена концепция и реализация интеллектуальной платформы для обнаружения подозрительной активности в сетевом трафике. Применение методов искусственного интеллекта значительно повышает эффективность защиты по сравнению с традиционными подходами. В дальнейшем планируется внедрение механизмов самообучения, интеграция с SIEM-системами и расширение базы сценариев атак.

ЛИТЕРАТУРА

1. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 2010.

2. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 2016.

3. Sharafaldin I., Lashkari A., Ghorbani A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSP, 2018.