АНАЛИЗ ПОЛЬЗОВАТЕЛЬСКОГО ПОВЕДЕНИЯ В СЕТЯХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Муминов Мухамадали Адахамджон ўғли
Резидент ИТ-парка

Аннотация: *В статье рассматривается применение методов глубокого обучения для анализа поведения пользователей в компьютерных сетях. Рост объемов сетевого трафика и использование сложных цифровых сервисов создают новые вызовы в обеспечении безопасности и управлении сетевыми ресурсами. Целью работы является исследование подходов, основанных на нейронных сетях, для идентификации аномальных действий и моделирования типичных паттернов поведения пользователей. Предложена концепция системы анализа сетевых данных в реальном времени, способной выявлять подозрительную активность на основе исторических данных.*

Ключевые слова: *Глубокое обучение, анализ поведения пользователей, нейронные сети, кибербезопасность, сетевой трафик, искусственный интеллект.*

Введение: С увеличением числа пользователей и разнообразия сетевых сервисов анализ поведения пользователей становится важной задачей для обеспечения безопасности и оптимизации работы сетей. Понимание поведенческих закономерностей позволяет своевременно выявлять аномалии, которые могут указывать на потенциальные угрозы или неэффективное использование ресурсов. Традиционные методы основаны на статических правилах и не способны адаптироваться к новым типам активности. Применение глубокого обучения открывает возможность автоматического изучения сложных закономерностей и построения адаптивных моделей, реагирующих на изменения поведения пользователей.

Обзор литературы и существующих подходов

Ряд исследований посвящен применению машинного обучения для анализа пользовательского поведения и обнаружения аномалий. Классические методы, такие как кластеризация и классификация на основе деревьев решений, показали ограниченные результаты при анализе больших объемов данных. Современные подходы используют глубокие нейронные сети (DNN), сверточные (CNN) и рекуррентные (RNN) архитектуры, способные выявлять нелинейные зависимости во временных данных. Особое внимание уделяется применению автоэнкодеров и моделей обучения без учителя для выявления отклонений в поведении пользователей без предварительной разметки данных. Исследования

последних лет показывают, что комбинация нейронных сетей и методов обработки временных рядов обеспечивает высокую точность при анализе сетевых событий.

Методология исследования

Предлагаемая система анализа поведения пользователей основана на применении рекуррентных нейронных сетей (LSTM) и сверточных слоев для выделения признаков из временных данных сетевого трафика. На первом этапе выполняется сбор данных о действиях пользователей: типы соединений, продолжительность сессий, частота обращений и объем переданных данных. Затем данные проходят предварительную обработку, включающую фильтрацию, нормализацию и выделение ключевых признаков. Модель глубокого обучения обучается на исторических данных для распознавания нормальных паттернов поведения. При обнаружении значительных отклонений от обученной модели система помечает события как потенциально аномальные. Результаты анализа визуализируются с помощью панели мониторинга, обеспечивающей поддержку решений специалистами по безопасности.

Ожидаемые результаты и значимость

Ожидается, что разработанная система позволит повысить точность выявления аномального поведения пользователей и сократить время реагирования на инциденты безопасности. Использование глубоких нейронных сетей обеспечит автоматическое выявление закономерностей без необходимости ручной настройки параметров. Система может применяться в корпоративных сетях, центрах обработки данных и облачных инфраструктурах для повышения уровня кибербезопасности. Кроме того, собранные данные могут быть использованы для прогнозирования будущей активности пользователей и оптимизации распределения ресурсов сети.

Заключение

В статье рассмотрены современные подходы к анализу пользовательского поведения в сетях с использованием методов глубокого обучения. Предложена концепция интеллектуальной системы, основанной на рекуррентных нейронных сетях, для выявления аномалий в поведении пользователей. Дальнейшие исследования будут направлены на реализацию прототипа системы, оценку эффективности различных архитектур нейронных сетей и интеграцию с существующими системами мониторинга сетевого трафика.

ЛИТЕРАТУРЫ

1. Kim, J., & Kim, H. (2022). Deep learning-based user behavior analysis for anomaly detection in network systems. *IEEE Access.*

2. Ahmed, M., Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications.*

3. Xu, K., & Wang, J. (2020). Behavioral modeling using LSTM networks for cybersecurity applications. *Computer Communications.*

4. Zhao, Y., & Li, S. (2021). Autoencoder-based approaches for user behavior analysis and intrusion detection. *Neurocomputing.*

5. Sadeghzadeh, M., & Dehghantanha, A. (2023). Deep behavioral analytics for threat detection in large-scale networks. *Future Generation Computer Systems.*