

**Классификация сетевого трафика с использованием моделей глубокого обучения**

**Аль-имари Б. (ИТМО), Иванов С.Е. (ИТМО)**

**Научный руководитель – к. ф.-м. н., доцент Иванов С.Е. (ИТМО)**

**Введение.** Быстрое расширение сетевых коммуникаций в сочетании с растущим числом подключенных интеллектуальных устройств и приложений IoT привело к росту неоднородного сетевого трафика. Традиционные методы классификации сетевого трафика, включая методы на основе портов и полезной нагрузки, с трудом справляются с современными зашифрованными и динамическими сетевыми средами. В этом исследовании изучается применение моделей глубокого обучения (DL) для расширенной классификации сетевого трафика, решая такие ключевые проблемы, как идентификация зашифрованного трафика, обработка в реальном времени и масштабируемость.

**Основная часть.**

В исследовании представлен гибридный подход глубокого обучения, который объединяет сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN) для использования как пространственных, так и временных характеристик трафика. Этот подход повышает точность классификации, особенно в сценариях с зашифрованным и динамически изменяющимся трафиком. Кроме того, изучаются методы дополнения данных для уменьшения дефицита маркированных наборов данных, а также предлагаются легкие архитектуры моделей для повышения эффективности развертывания в реальном времени.

Экспериментальные результаты показывают, что предлагаемая гибридная модель CNN-RNN достигает превосходной производительности по сравнению с традиционными методами, предлагая более высокую точность определения шаблонов трафика, меньшую задержку классификации и улучшенную адаптивность к зашифрованным потокам данных. Предлагаемая модель достигает расчетной точности классификации 95% при сохранении низкой задержки, что делает ее пригодной для приложений управления сетями в реальном времени.

Растущая зависимость от цифровых сетей требует надежных методов классификации трафика для управления качеством обслуживания (QoS) и повышения безопасности сети. Традиционные методы классификации, такие как методы на основе портов и полезной нагрузки, сталкиваются с ограничениями из-за шифрования и меняющихся моделей трафика. Машинное обучение, в частности глубокое обучение, предлагает многообещающее решение за счет автоматического извлечения признаков из необработанных данных трафика.

В этом исследовании предлагается гибридная модель глубокого обучения, объединяющая CNN и RNN. CNN фиксируют пространственные зависимости в сетевом трафике, в то время как RNN анализируют временные корреляции. Предлагаемая модель обучается на маркированном наборе данных и оценивается на основе метрик точности, достоверности, отклика и задержки.

**Выводы.**

Предлагаемая модель демонстрирует точность классификации 95%, что значительно превосходит традиционные методы, такие как SVM и Random Forest. Модель эффективно обрабатывает зашифрованный трафик и демонстрирует задержку классификации 10 мс, что делает ее подходящей для приложений мониторинга сети в реальном времени.

Это исследование подчеркивает потенциал моделей глубокого обучения для улучшения классификации сетевого трафика. Гибридный подход CNN-RNN обеспечивает масштабируемое, эффективное и точное решение для управления сетью в реальном времени, решая ключевые проблемы в современных сетевых средах.

#### **Список использованных источников:**

1. Lotfollahi M. et al. Deep packet: A novel approach for encrypted traffic classification using deep learning //Soft Computing. – 2020. – Т. 24. – №. 3. – С. 1999-2012.
2. Lim H. K. et al. Packet-based network traffic classification using deep learning //2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC). – IEEE, 2019. – С. 046-051.
3. Abbasi M., Shahraki A., Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey //Computer Communications. – 2021. – Т. 170. – С. 19-41.
4. Bendiab G. et al. IoT malware network traffic classification using visual representation and deep learning //2020 6th IEEE Conference on Network Softwarization (NetSoft). – IEEE, 2020. – С. 444-449.
5. Mohammed A. Ş. R., Mohammed S. A., Shirmohammadi S. Machine learning and deep learning based traffic classification and prediction in software defined networking //2019 IEEE International Symposium on Measurements & Networking (M&N). – IEEE, 2019. – С. 1-6.
6. Kalwar J. H., Bhatti S. Deep Learning Approaches for Network Traffic Classification in the Internet of Things (IoT): A Survey //arXiv preprint arXiv:2402.00920. – 2024.