0.1. *Самойленко Р.В.* Обнаружение мошеннических действий в финансовых наборах данных с применением методов глубокого обучения

Трансформация технологического ландшафта финансовой и торгово-экономической деятельности привела к появлению интернет-банкинга, многочисленных маркетплейсов и других элементов цифровой экосистемы. Как следствие, стали возможными принципиально новые виды мошенничества, эффективность противодействия которым традиционными средствами крайне низка. Основанные на правилах системы обнаружения аномалий (подозрительных транзакций), работают по заранее определенным алгоритмам и, чтобы оставаться актуальными, требуют частых обновлений при появлении новых видов атак. Такой подход крайне неэффективен, поскольку действует «с опозданием» и не позволяет обнаруживать атаки, признаки которых еще отсутствуют в системе. Цель данной работы – оценка потенциала методов глубокого обучения для обнаружения аномалий в области электронных платежей и выявление моделей машинного обучения, способных самообучаться и эффективно работать даже при появлении ранее неизвестных атак.

Обнаружение аномалий в наборах данных осуществляется с помощью методов неконтролируемого обучения для выявления отклонений в финансовых транзакциях. Нейронные сети, с их способностью моделировать сложные закономерности и взаимосвязи в данных, предлагают надежную основу для выявления мошеннических транзакций. В исследовании рассматривается применение различных нейронных сетей, включая сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), которые специализируются на обработке последовательных данных и выявлении мошеннического поведения [1].

Основным результатом исследования является определение наиболее актуального метода машинного обучения для анализа электронных платежей. В работе были использованы наборы данных финансовых транзакций с ресурса Kaggle и продемонстрировано сочетание различных нейронных сетей, что позволило использовать сильные стороны разных методов для улучшения обнаружения мошенничества. Также в исследовании отражена роль автоэнкодеров, которые могут использоваться для изучения обычных схем транзакций и выявлять отклонения, в то время как рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN) могут моделировать последовательный характер транзакций с течением времени и осуществлять обработку последовательностей данных.

Таким образом, показано, что для выявления мошенничества в финансовых транзакциях наиболее результативным является объединение нескольких моделей нейросетей, таких как CNN, RNN и автоэнкодеров, с помощью которых можно создать ансамблевую модель, которая фиксирует различные аспекты транзакций, повышая общую точность обнаружения. Объединение разных нейронных сетей может обеспечить более полное представление данных, расширяя возможности обнаружения сложных схем мошенничества.

Список литературы

[1] Khemani B., Patil S., Kotecha K., Tanwar S. A review of graph neural networks: concepts, architectures, techniques, challenges, datasets, applications, and future directions // Journal of Big Data. 2024. Vol. 11. N. 1. P. 18-21.