

УДК 004.89

РОЛЬ ГЛУБОКОГО ОБУЧЕНИЯ В ВЫЯВЛЕНИИ ФРОДОВЫХ АНОМАЛЬНЫХ ДЕЙСТВИЙ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Петров Р.А., студент гр. 24223, I курс
Новосибирский государственный университет, г. Новосибирск

Фродовые аномалии в электронной коммерции представляют собой серьезную угрозу для бизнеса, клиентов и экономической стабильности. В данной статье рассматривается роль глубокого обучения в выявлении фродовых аномальных действий в электронной коммерции. Мы проанализируем принципы работы глубокого обучения, его применимость к анализу данных электронной коммерции и проведем обзор современных подходов к выявлению фродов с использованием глубокого обучения [1-4].

Введение: Фродовые аномалии в электронной коммерции включают в себя различные виды мошенничества, такие как украденные кредитные карты, фальшивые транзакции и украденные учетные записи. Выявление и предотвращение таких аномалий является приоритетной задачей для электронных коммерческих платформ [5-8].

Принципы работы глубокого обучения: Глубокое обучение представляет собой раздел машинного обучения, основанный на искусственных нейронных сетях с многими слоями (глубокими нейронными сетями). Эти сети способны извлекать сложные зависимости из данных и обучаться на больших объемах информации без необходимости ручного определения характеристик [9-11].

Применение глубокого обучения в электронной коммерции: Глубокое обучение может быть применено к анализу данных электронной коммерции для выявления фродовых аномалий. Например, нейронные сети могут анализировать поведение пользователей, характеристики транзакций и другие параметры для выявления подозрительных активностей.

Современные подходы к выявлению фродов с использованием глубокого обучения: Существует несколько современных подходов к выявлению фродов в электронной коммерции с использованием глубокого обучения, включая использование рекуррентных нейронных сетей для анализа последовательностей действий пользователей, сверточных нейронных сетей для анализа изображений и текста, а также генеративных моделей для создания синтетических данных и обнаружения аномалий.

Преимущества глубокого обучения в выявлении фродов: Преимущества глубокого обучения в выявлении фродов включают высокую точность и

способность к обработке больших объемов данных. Кроме того, глубокое обучение способно автоматически извлекать признаки из данных, что делает его особенно эффективным для выявления сложных и невидимых шаблонов мошенничества.

Список литературы:

1. West J. Intelligent financial fraud detection: A comprehensive review / J. West, M. Bhattacharya // *Computers & Security*. – 2016. – Vol. 57. – P. 47–66. – DOI: 10.1016/j.cose.2015.09.005.
2. Ngai E. W. T. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature / E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, X. Sun // *Decision Support Systems*. – 2011. – Vol. 50, № 3. – P. 559–569. – DOI: 10.1016/j.dss.2010.08.006.
3. Abdallah A. Fraud detection system: A survey / A. Abdallah, M. A. Maarof, A. Zainal // *Journal of Network and Computer Applications*. – 2016. – Vol. 68. – P. 90–113. – DOI: 10.1016/j.jnca.2016.04.007.
4. Hilal W. Financial fraud: A review of anomaly detection techniques and recent advances / W. Hilal, S. A. Gadsden, J. Yawney // *Expert Systems with Applications*. – 2022. – Vol. 193. – Article 116429. – DOI: 10.1016/j.eswa.2021.116429.
5. Bolton R. J. Statistical fraud detection: A review / R. J. Bolton, D. J. Hand // *Statistical Science*. – 2002. – Vol. 17, № 3. – P. 235–255. – DOI: 10.1214/ss/1042727940.
6. Bahnsen A. C. Example-dependent cost-sensitive logistic regression for credit scoring / A. C. Bahnsen, D. Aouada, B. Ottersten // *Proceedings of the 13th International Conference on Machine Learning and Applications*. – Detroit : IEEE, 2014. – P. 263–269. – DOI: 10.1109/ICMLA.2014.48.
7. Dal Pozzolo A. Credit card fraud detection: A realistic modeling and a novel learning strategy / A. Dal Pozzolo, O. Caelen, R. A. Johnson, G. Bontempi // *IEEE Transactions on Neural Networks and Learning Systems*. – 2018. – Vol. 29, № 8. – P. 3784–3797. – DOI: 10.1109/TNNLS.2017.2736643.
8. Lucas Y. Credit card fraud detection using machine learning: A survey / Y. Lucas, P.-E. Portier, L. Laporte, S. Calabretto, L. He-Guelton, F. Oblé, M. Granitzer // *arXiv*. – 2020. – arXiv:2010.06479. – URL: <https://arxiv.org/abs/2010.06479>. (дата обращения: 12.06.2025).
9. LeCun Y. Deep learning / Y. LeCun, Y. Bengio, G. Hinton // *Nature*. – 2015. – Vol. 521. – P. 436–444. – DOI: 10.1038/nature14539.
10. Goodfellow I. Deep Learning / I. Goodfellow, Y. Bengio, A. Courville. – Cambridge : MIT Press, 2016. – 800 p.

11. Pang G. Deep learning for anomaly detection: A review / G. Pang, C. Shen, L. Cao, A. van den Hengel // ACM Computing Surveys. – 2022. – Vol. 54, № 2. – Article 38. – P. 1–38. – DOI: 10.1145/3439950.