УДК 004.9

Левицька Т. О. канд. техн. наук, доцент
ДВНЗ «Приазовський державний технічний університет»

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІЧНИХ СИСТЕМ У КРИПТОВАЛЮТНОМУ ТРЕЙДИНГУ

Сучасний розвиток цифрових фінансових ринків і стрімке поширення технологій децентралізованих фінансів (DeFi) сприяли появі складних алгоритмічних систем аналізу та прогнозування ринкових даних. У подібних системах дедалі частіше використовуються моделі глибинного навчання, зокрема архітектури Long Short-Term Memory та Gated Recurrent Unit, що дозволяють ефективно працювати з часовими рядами та реалізовувати ринково-нейтральні торгові стратегії. Разом із високою точністю прогнозування виникає проблема забезпечення належного рівня інформаційної безпеки. Недостатній захист API-ключів, можливість модифікації вхідних даних або витік параметрів моделі можуть призвести до значних фінансових втрат і порушення вимог міжнародних регуляторних стандартів, таких як MiFID II [1] та NIST AI Risk Management Framework [2]. У зв'язку з цим актуальним є формування захищеної інфраструктури для систем криптовалютного алгоритмічного трейдингу, що використовують методи машинного навчання.

Об'єктом дослідження є експериментальний прототип торгової системи, який отримує ринкову інформацію з криптовалютної біржі Binance та децентралізованої платформи деривативів dYdX. Методологія роботи ґрунтується на аналізі технічних характеристик блокчейн-протоколів, дослідженні поширених вразливостей екосистеми DeFi [3,4] та застосуванні сучасних підходів до керування секретними даними в хмарних обчислювальних середовищах. Додатково використовуються криптографічні методи автентифікації запитів до зовнішніх сервісів.

У ході дослідження було визначено чотири ключові рівні загроз, які потребують реалізації відповідних механізмів захисту. Перший рівень пов'язаний із зовнішніми джерелами даних. У середовищі DeFi можливі атаки, що базуються на маніпуляції ціновими оракулами [5] або використанні механізмів флеш-кредитування[6], які здатні тимчасово викривляти ринкові котирування. Для зменшення впливу таких атак запропоновано механізм попередньої обробки даних, який передбачає фільтрацію аномальних значень та перевірку котирувань за даними декількох біржових джерел. Другий рівень загроз стосується інфраструктури системи. У запропонованій архітектурі всі програмні

компоненти розміщуються в ізольованому сегменті хмарної мережі. При цьому жоден із модулів не зберігає конфіденційні параметри локально. Доступ до API-ключів і конфігураційних даних реалізовано через спеціалізовані сервіси керування секретами, наприклад Key Vault або KMS, із використанням механізму керованих ідентифікацій. Третій рівень пов'язаний із виконанням торгових операцій. Для запобігання атакам повторного відтворення запитів застосовується криптографічний підпис на основі алгоритму HMAC-SHA256. Додатково встановлюється обмежене часове вікно дії запиту (30 секунд), що унеможливлює використання перехоплених повідомлень[7]. Експериментальні перевірки показали ефективність такого підходу для блокування несанкціонованих транзакцій. Четвертий рівень безпеки стосується безпосередньо моделей машинного навчання та торгової стратегії. Для зниження ризиків впроваджено механізм аварійного зупинення торгівлі («kill-switch»), який працює на основі аналізу зміни статистичних характеристик даних та фінансових показників системи[8-10]. У випадку виявлення значних відхилень у розподілі ознак або перевищення встановлених обмежень ризику система автоматично припиняє торгові операції та деактивує ключі доступу.

Під час апробації системи були отримані наступні науково-практичні результати:

- Ефективність захисту: Впровадження механізму HMAC-SHA256 разом із nonce-валідацією дозволило заблокувати 98,7% спроб атак повторного відтворення (replay attacks) під час стрес-тестування.
- Швидкодія: Додаткова затримка (latency), впроваджена криптографічним підписом та зверненням до KMS, склала лише 12-15 мс, що є прийнятним для середньочастотних стратегій і не впливає на проковзування (slippage).
- Точність Kill-switch: Система детектування аномалій (feature drift) показала detection rate на рівні 94,5% при спробах маніпулювання вхідними ознаками моделі через спотворення цінових оракулів.

Запропонована архітектура дозволяє підвищити стійкість алгоритмічного торгового контуру до широкого спектра кіберзагроз. Проведене тестування підтвердило ефективність запропонованої архітектури при роботі з реальними торговими API. Поєднання хмарних механізмів безпеки, криптографічних методів захисту та моніторингу стану моделей машинного навчання забезпечує зниження операційних ризиків і сприяє відповідності сучасним вимогам регуляторного середовища щодо надійності алгоритмічних фінансових систем.

Список використаних джерел

1. European Securities and Markets Authority. MiFID II Review Report on Algorithmic Trading. ESMA70-156-4572, 2021. URL: https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf (дата звернення: 10.12.2025).

2. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, Gaithersburg, 2023. DOI: 10.6028/NIST.AI.100-1.

3. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized Finance (DeFi) Attacks. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2444–2461). IEEE. https://doi.org/10.1109/SP46215.2023.10179435

4. Werner S., Perez D., Gudgeon L., Klages-Mundt A., Harz D., Knottenbelt W. SoK: Decentralized Finance (DeFi). AFT '22: 4th ACM Conference on Advances in Financial Technologies. 2022. P. 30–46. DOI: 10.1145/3558535.3559780

5. Daian P., Goldfeder S., Kell T. та ін. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. 2020 IEEE Symposium on Security and Privacy. IEEE, 2020. DOI: 10.1109/SP40000.2020.00097.

6. Cao S., Huang L., Wang Z. Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem. 2021 IEEE International Conference on Blockchain. IEEE, 2021. DOI: 10.1109/Blockchain53845.2021.00060.

7. FICC Markets Standards Board. Emerging themes and challenges in algorithmic trading and machine learning. Spotlight Review, 2020. URL: https://fmsb.com/wp-content/uploads/2020/04/FMSB-Spotlight-Review-Emerging-themes-and-challenges-in-algorithmic-trading-and-machine-learning.pdf (дата звернення: 10.12.2025).

8. Yerlikaya F. A., Bahtiyar Ş. Data poisoning attacks against machine learning algorithms. Expert Systems with Applications, 2022, vol. 208, 118101. DOI: 10.1016/j.eswa.2022.118101.

9. Pialla, G., Ismail Fawaz, H., Devanne, M., Weber, J., Idoumghar, L., Muller, P.-A., Bergmeir, C., Schmidt, D. F., Webb, G. I., & Forestier, G. (2025). ime series adversarial attacks: An investigation of smooth perturbations and defense approaches. International Journal of Data Science and Analytics, 19, 129–139. https://doi.org/10.1007/s41060-023-00438-0

10. Rigaki, M., & Garcia, S. (2023). A survey of privacy attacks in machine learning. ACM Computing Surveys, 56(4), Article 101, 1–34. https://doi.org/10.1145/3624010