operations of multiplying numbers of length $p_0 = p_1 = (p+1)/3$ and $p_2 = p_0 - 1$ bits.

$$\left\langle A^2 \right\rangle_{M_p} = \left\langle R_2 \cdot 2^{p_0+p_1} + R_1 \cdot 2^{p_0} + R_0 \right\rangle_{M_p}, \text{ where}$$

$$M_0 = (A_0 + (A_1 + A_2))^2, \quad R_0 = \frac{M_0 + M_1}{2} - M_2,$$
$$M_1 = (A_0 - (A_1 + A_2))^2,$$
$$M_2 = (A_1 - A_2)^2, \quad R_1 = \frac{M_0 - M_1}{2} - M_3,$$
$$M_3 = 2 \cdot (A_0 - A_2) \cdot A_2, \quad R_2 = \frac{M_0 - M_1}{2} - M_4.$$
$$M_3 = (2 \cdot A_0 - A_1) \cdot A_1.$$

For verification:

$$R_0 = (A_0)^2 + 4 \cdot A_1 \cdot A_2,$$
$$R_1 = 2 \cdot (A_2)^2 + 2 \cdot A_0 \cdot A_1,$$
$$R_2 = (A_1)^2 + 2 \cdot A_0 \cdot A_2.$$

Similarly to Lemma 1, multiplication and division by 2, multiplication by 2^{p_0} and $2^{p_0+p_1}$ can be disregarded in the total number of multiplication operations.

The algorithm for squaring a Mersenne number modulo by dividing the number into two sections (Lemma 1) is 33% more efficient than the Karatsuba method. The algorithm for squaring a Mersenne number modulo by dividing the number into three sections (Lemma 2) allows us to calculate the squaring operation by using three smaller-length squaring operations out of the five required multiplication operations. Squaring smaller-length numbers based on the fast Fourier transform is one of the reserves for optimizing the implementation of the multiword multiplication operation.

1. Zadiraka, V.K., Tereshchenko, A.M. An Efficient Algorithm for Squaring Multi–Word Numbers. *Cybern Syst Anal*, 61, 521-526 (2025).
2. Schönhage A., Strassen V. Schnelle Multiplikation großer Zahlen. *Computing*. – 1971. – № 7. – P. 281–292.
3. Karatsuba, A. A.; Ofman, Y. P. (1962). Multiplication of Many-Digital Numbers by Automatic Computers. Proceedings of the USSR Academy of Sciences (in Russian). 145: 293–294.

Система виявлення інформаційно-фінансових атак на криптовалютних ринках із застосуванням показника поглинання імпульсу

УДК 004.056.5:004.42:336.74

Ігор Цапро[1], Оксана Золотухіна[2]

Державний університет інформаційно-комунікаційних технологій,
[1]tsapro.ihor.work@gmail.com, [2]o.zolotukhina@duikt.edu.ua

Постановка проблеми. Стрімкий розвиток цифрових фінансових платформ, криптовалютних бірж та децентралізованих фінансових сервісів супроводжується збільшенням кількості кіберфінансових загроз, серед яких особливу небезпеку становлять координовані інформаційно-фінансові атаки: алгоритмічні маніпуляції ліквідністю, spoofing, wash trading та приховане накопичення позицій великими учасниками ринку [1]. Особливість таких атак

полягає у тому, що їх початкові ознаки часто не супроводжуються очевидною зміною ринкової ціни, а проявляються через аномальні торгові обсяги, зміну структури ліквідності та нетипову поведінку учасників ринку.

Метою дослідження є розробка програмної системи для виявлення потенційних інформаційно-фінансових атак на криптовалютних ринках шляхом статистичного аналізу часових рядів та використання показника поглинання імпульсу ринкових обсягів (Momentum Absorption Score, MAS) [2].

Актуальність дослідження обумовлена потребою створення програмних засобів раннього виявлення прихованих ринкових аномалій, які можуть передувати маніпулятивним або координованим фінансовим атакам.

Наукова новизна роботи полягає у поєднанні статистичного методу виявлення поглинання ринкових обсягів із принципами інженерії програмного забезпечення для побудови програмної системи моніторингу інформаційно-фінансових атак. На відміну від традиційних індикаторів технічного аналізу [3], показник MAS дозволяє виявляти ринкові стани, за яких значні обсяги торгів не супроводжуються суттєвою зміною ціни, що може сигналізувати про приховану ринкову боротьбу або підготовку до подальшого інформаційно-фінансового впливу.

Результати дослідження. В основу запропонованого рішення покладено аналіз часових рядів даних формату OHLCV, які включають ціну відкриття, максимальну та мінімальну ціну, ціну закриття та торговий обсяг. Формула показника сумарних ринкових обсягів має наступний вигляд (1):

$$MAS_{V,t} = (Z_{HL_t} < P_{25}(HL_t)) \wedge (Z_{V_t} > P_{75}(V_t)), \quad (1)$$

де Z_{HL_t} – це стандартна оцінка (z-score) різниці між максимальною та мінімальною цінами за час *t*, Z_{V_t} – це стандартна оцінка сумарних ринкових обсягів за час *t*, P_{25} – процентиль 25, P_{75} – процентиль 75.

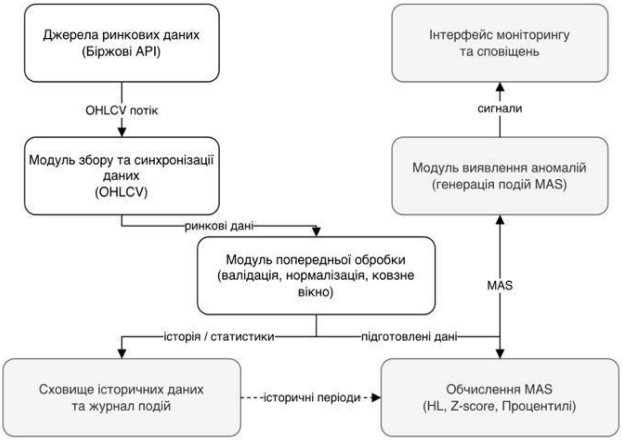

Рис.1. Схема програмної реалізації системи

Програмна система реалізована (Рис. 1) за модульною архітектурою та складається з компонентів збору ринкових даних, потокової обробки часових рядів, обчислення статистичних характеристик, генерації MAS-подій та журналювання результатів. Отримання даних здійснюється через біржові API у режимі реального часу. Для забезпечення обчислювальної ефективності застосовано механізми кешування проміжних розрахунків та планування виконання обчислювальних модулів. Архітектура системи забезпечує масштабованість, відмовостійкість та можливість інтеграції у середовища оперативного моніторингу фінансових ризиків.

Висновки. Розроблено програмну систему виявлення потенційних інформаційно-фінансових атак на криптовалютних ринках на основі показника поглинання імпульсу. Події MAS регулярно виникають у фазах низької волатильності перед значними імпульсними рухами ринку. Запропонований підхід дозволяє виявляти приховані ринкові аномалії, які не фіксуються класичними індикаторами технічного аналізу, що підвищує ефективність моніторингу потенційно маніпулятивної активності. Запропоноване рішення поєднує статистичний аналіз часових рядів та принципи інженерії програмного забезпечення, забезпечуючи можливість раннього виявлення прихованих інформаційно-фінансових загроз у режимі реального часу. Перспективами подальших досліджень є інтеграція алгоритмів машинного навчання для автоматичного відсіювання хибнопозитивних сигналів та підвищення точності детекції аномальної активності.

1. Cong, Lin William and Li, Xi and Tang, Ke and Yang, Yang, Crypto Wash Trading. *SSRN*. – 2023. DOI: http://dx.doi.org/10.2139/ssrn.3530220.
2. Цапро І. В. Застосування машинного навчання в задачі відсіювання неефективних торгових сигналів згенерованих показниками механістичного підходу. *Зв'язок*. – 2025. № 5 (177). – С. 79-86. DOI: 10.31673/2412-9070.2025.051067.
3. Han, Yufeng and Liu, Yang and Zhou, Guofu and Zhu, Yingzi, Technical Analysis in the Stock Market: A Review. *SSRN*. – 2021. DOI: http://dx.doi.org/10.2139/ssrn.3850494

Інтегрований контур захищеності вебсистем із криптографічною фіксацією та графово-нейромережевим оцінюванням подій

УДК 004.4:004.415.2 (043.2)
Ірина Замрій[1], Іван Шахматов[2], Діана Шахматова

Державний університет інформаційно-комунікаційних технологій, Київ, Україна, [1]i.zamrii@duikt.edu.ua, [2]i.shahmatov@duikt.edu.ua

Забезпечення захищеності сучасних вебсистем потребує формування єдиного контуру [1] обробки критичних подій. Метою дослідження є формалізація такого підходу для подій вебформ, транзакційних операцій та інших функціональних компонентів вебсистеми, щоб результат роботи механізмів захисту був не лише обчисленим, а й відтворюваним та доказово підтвердженим [3].