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].

Формальну основу контуру захищеності вебсистем подамо у вигляді

$$K = (S, O, L, F, D, P, J), \tag{1}$$

де S - критичні події, O - пов'язані об'єкти й суб'єкти, L - зв'язки між ними, F - формування ознак, D - прийняття рішення, P - політики реагування, J - незмінний журнал.

Інтегрований механізм обробки подій можна подати як відображення:

$$M : S \to C \times A \times Q \times V, \tag{2}$$

де $C = \{NORM, ALERT, CRIT\}$ - множина класів стану події, $A = \{PASS, CHECK, ISOLATE, BLOCK\}$ - множина можливих дій реагування, Q - множина доказових записів, $V = \{0,1\}$ - множина результатів верифікації.

Для окремої критичної події s_i результат роботи механізму має вигляд $M(s_i) = (c_i, a_i, q_i, v_i)$, де c_i - визначений клас події, a_i - дія реагування, q_i - доказовий запис, $v_i \in \{0,1\}$ - результат перевірки коректності запису та його включення до журналу.

Послідовність роботи механізму подається як композицію функціональних перетворень:

$$M = J_q \circ Q_f \circ A_p \circ C_r \circ R_s \circ K_h, \tag{3}$$

де K_h виконує криптографічну фіксацію події, R_s формує оцінку ризику, C_r визначає клас події, A_p вибирає дію реагування відповідно до політики, Q_f формує доказовий запис, J_q додає цей запис до незмінного журналу.

Криптографічна фіксація події задається як $K_h(s_i) = (n_i, h_i, g_i)$, де n_i - нормалізоване подання події s_i, $h_i = H(n_i)$ - хеш нормалізованого подання, $g_i = Sign_{sk}(h_i)$ - цифровий підпис хешу, сформований із використанням закритого ключа sk. Оцінка ризику події визначається як $R_s(s_i) = r_i, r_i \in [0,1]$, де r_i - нормалізований рівень ризику події. Його значення залежить від типу події:

$$r_i = \begin{cases} b_i, & t_i = \text{FORM}, \\ z_i, & t_i = \text{PAY}, \\ r_i^0 \text{ для інших типів подій}, \end{cases} \tag{4}$$

де t_i - тип події, b_i - ризик подання вебформи за результатом графово-нейромережевого аналізу, z_i - ризик транзакції, r_i^0 - базова оцінка ризику [2].

Після прийняття рішення формується доказовий запис:

$$q_i = (h_i, g_i, m_i, w_i, l_i, r_i, c_i, a_i, d_i), \tag{5}$$

де h_i - хеш події, g_i - цифровий підпис, m_i - ідентифікатор версії моделі, w_i - контрольна сума параметрів моделі, l_i - контрольна сума політики реагування, r_i - оцінка ризику, c_i - клас події, a_i - дія реагування, d_i - час формування рішення. Такий запис фіксує не лише факт події, а й підстави прийнятого рішення. Завершальним етапом є включення доказового запису до незмінного журналу:

$$J_q(q_i) = (B_j, v_i), \tag{6}$$

де B_j - блок незмінного журналу, до якого включено запис q_i, $v_i \in \{0,1\}$ - результат перевірки коректності цього включення. Якщо змінюється зміст запису або порушується зв'язок між блоками журналу, результат верифікації набуває значення 0, що свідчить про порушення цілісності.

Запропонована формалізація описує єдиний контур забезпечення захищеності вебсистем, у якому критична подія проходить криптографічну фіксацію, ризикове оцінювання, класифікацію, вибір дії реагування та доказове журналювання. Використання композиції функціональних відображень дає змогу поєднати механізми верифікованого журналювання, контролю доступу та графово-нейромережевого аналізу подій, забезпечуючи простежуваність рішень, аудитну перевірність і контроль цілісності історії подій у вебсистемі.

1. Балацька В. Блокчейн-орієнтований підхід до забезпечення простежуваності та перевірюваності виконання політик КСЗІ. Кібербезпека: освіта, наука, техніка. 2026. Т. 4, № 32. С. 674–685. DOI: 10.28925/2663-4023.2026.32.1136.
2. Zamrii I., Shakhmatov I. Multi-View Graph Model with Representation Alignment and Adaptive Fusion for Better Spam Detection. Proceedings of the Workshop on Cryptology and Data Security (WCDS 2025), co-located with SMICS 2025, Lviv, Ukraine, October 16-18, 2025, CEUR Workshop Proceedings, 2026, Vol. 4191. P. 99-106.
3. Sha J., Wu J., Wang M., Pu Y., Lu S., Bilal M. QoE-aware edge server placement in mobile edge computing using an enhanced genetic algorithm. International Journal of Intelligent Networks. 2025. Vol. 6. P. 65–78.