дискретних логарифмів (Чаум–Педерсен) [2], що підтверджує коректне використання приватного ключа. Будь-який аудитор може самостійно відтворити агрегацію з Bulletin Board і верифікувати кожен доказ без знання приватного ключа (Universal Verifiability).

Усі сервери функціонують за протоколом HTTPS. Реєстрація виборців захищена підтвердженням електронної пошти та CAPTCHA. Передбачено rate limiting для захисту від DoS-атак. Схема 2-з-3 за Шаміром із зберіганням часток у HashiCorp Vault [7] унеможливлює компрометацію ключа при доступі до одного сервера.

Розроблена система реалізує ключові складові End-to-End Verifiability — Individual Verifiability та Universal Verifiability: виборець підтверджує врахування голосу через Tracking Code і Bulletin Board; математика гарантує чесність розшифрування через Chaum–Pedersen Decryption Proof [2, 5]. Застосування мережі Tor та сліпих підписів RFC 9474 [3] забезпечує анонімність виборця навіть за умови компрометації окремих вузлів інфраструктури.

1. National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS PUB 186-5. NIST, 2023. 36 p.
2. Chaum D., Pedersen T. Wallet databases with observers. CRYPTO 1992. Lecture Notes in Computer Science, vol. 740. – Springer, 1993. – P. 89–105.
3. Denis F. et al. RFC 9474: RSA Blind Signatures. – IETF, 2023. URL: https://www.rfc-editor.org/rfc/rfc9474 (дата звернення: 01.05.2026).
4. Shamir A. How to share a secret. Communications of the ACM. – 1979. – Vol. 22, №11. – P. 612–613.
5. Cortier V., Galindo D., Glondu S., Izabachène M. Election verifiability for Helios under weaker trust assumptions. ESORICS 2014. Lecture Notes in Computer Science, vol. 8713. – Springer, 2014. – P. 347–364.
6. Jafar U., Ab Aziz M.J., Shukur Z. Blockchain for Electronic Voting System — Review and Open Research Challenges. Sensors. – 2021. – Vol. 21, №17. – P. 5874.
7. Python Cryptography Library. Fernet (symmetric encryption). — URL: https://cryptography.io/en/stable/fernet/
8. The Tor Project. About Tor. — URL: https://support.torproject.org/about-tor/
9. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme. Eur. Trans. Telecommun. – 1997. – Vol. 8, №5. – P. 481–490.

Модель гібридної системи виявлення вторгнень на основі криптографічних перетворень та методів штучного інтелекту

УДК 621.395.7 (043.2)

Аліна Давлетова[1]

Західноукраїнський національний університет, [1]a7davletova@gmail.com

Забезпечення безпеки у сучасних розподілених інформаційних системах потребує комплексного підходу, що виходить за межі стандартного шифрування. Традиційні засоби захисту часто не здатні ідентифікувати загрози, які не порушують цілісність даних, але створюють часові аномалії або статистичні відхилення в каналі зв'язку. Актуальною є розробка систем виявлення вторгнень (IDS), які поєднують математичний апарат криптографії з інтелектуальним аналізом ознак сеансу.

Метою роботи є розробка та дослідження моделі гібридної IDS, яка поєднує методи асиметричного шифрування, завадостійкого кодування та ансамблевого машинного навчання для комплексної оцінки безпеки сеансів зв'язку в умовах динамічної зміни параметрів передачі даних..

На відміну від відомих підходів, де криптографічні механізми та інтелектуальна детекція використовуються переважно окремо або комбінуються в межах однорідних моделей, наприклад, rule-based та machine learning-based IDS [1–3], запропонована система дозволяє враховувати як структурні ознаки порушення даних, так і часові аномалії. Такий підхід узгоджується з сучасними тенденціями розвитку гібридних IDS [4, 5], проте розширює їх функціональні можливості за рахунок інтеграції криптографічного контролю передачі даних у процес формування вектору ознак, що дозволяє одночасно враховувати повторне відтворення повідомлень та їх підміну. В основі розробки лежить багаторівнева модель (рисунок 1):

Рис.1. Узагальнена схема гібридної системи виявлення вторгнень

1) Криптографічний рівень - забезпечення конфіденційності даних шляхом застосування алгоритму асиметричного шифрування RSA, що дозволяє локалізувати потенційні втручання та аналізувати успішність дешифрування для кожного блоку.
2) Рівень контролю цілісності - реалізація завадостійкого кодування на основі коду Хеммінга над небінарними полями дозволяє не лише відновлювати поодинокі спотворення, а й формувати метрики, що слугують індикаторами активного втручання.
3) Інтелектуальний рівень – включає модуль машинного навчання (ML) на базі алгоритму Random Forest, що аналізує вектор ознак (Features), включаючи часові затримки (Input Delay) та метрики успішності декодування, а також модуль аналізу історії (AI), що здійснює ретроспективну оцінку ризику на основі бази даних попередніх сесій.
4) Рівень прийняття рішень – етап, на якому за допомогою гібридного алгоритму, що комбінує «жорсткі» правила криптографічного ядра (crypto), прогнози моделі машинного навчання Random Forest та результати аналізу історії, формується фінальне рішення.

Для оцінки ефективності запропонованого рішення проведено серії з 3000 експериментів у режимі змішаних сценаріїв, де випадковим чином генерувалися різні типи впливів, зокрема помилки передачі, часові затримки та комбіновані атаки.

Такий підхід дозволив оцінити здатність IDS працювати в умовах невизначеності та часткового перекриття ознак різних типів загроз.

Таблиця 1

Результати експериментального дослідження гібридної IDS

Компонент системи	Базова точність детекції, %	Оптимізована точність детекції, %	Усереднена F-міра	Повнота детекції атак
Crypto	78,73	81,23	0,583	0,84
AI	48,06	56,41	0,508	0,61
ML	78,86	99,47	0,992	1,00
Фінальне рішення	72,86	92,29	0,874	1,00

Результати експериментів підтвердили, що криптографічне ядро системи стабільно виявляє прямі порушення цілісності даних, тоді як накопичення статистики аномалій дозволило адаптувати систему до специфічних завад у каналі зв'язку.

Обраний вектор ознак продемонстрував високу роздільну здатність для класифікації станів системи, а гібридна інтеграція компонентів забезпечила підвищення точності фінального рішення на 19,43% при повному виключенні пропуску вторгнень (Recall = 1,00).

1. Viswanathan C., Kirthika G. Hybrid Machine Learning-Based Intrusion Detection System for Cybersecurity in Autonomous Vehicles. 2025. 1-6. https://doi.org/10.1109/ICCDS64403.2025.11209720..
2. Joshi V.R., Assa-Agyei K., Al-Hadhrami T., Qasem, S.N. Hybrid AI Intrusion Detection: Balancing Accuracy and Efficiency. Sensors. 2025. 25(24), 7564. https://doi.org/10.3390/s25247564
3. Mamatha P., Balaji S., Anuraghav S.S. Development of Hybrid Intrusion Detection System Leveraging Ensemble Stacked Feature Selectors and Learning Classifiers to Mitigate the DoS Attacks. Int J Comput Intell Syst 18, 20 (2025). https://doi.org/10.1007/s44196-025-00750-6
4. Bharti J., Singh S. A Machine Learning Based Hybrid Encryption System to Prevent Cloud Data Breach. Journal of Information Systems Engineering and Management. 2025. 10. https://doi.org/708-717. 10.52783/jisem.v10i50s.10350.
5. Ahmad Z., Khan A.S., Wai Shiang C., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol. 2021. 32(1):e4150. https://doi.org/10.1002/ett.4150