Сенчило Т.С., магістрантка
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

СИСТЕМА ЗАХИСТУ ВІД АТАК НА BLOCKCHAIN-МЕРЕЖІ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ СМАРТ-КОНТРАКТІВ

В умовах стрімкого розвитку децентралізованих фінансів (DeFi) та впровадження blockchain-технологій у критично важливі сфери діяльності, забезпечення безпеки смарт-контрактів стає першочерговим завданням. Згідно з даними аналітичних агентств, у 2023 році втрати від атак на смарт-контракти перевищили 2 мільярди доларів, що підкреслює актуальність розробки ефективних систем захисту.

Існуючі методи забезпечення безпеки blockchain-систем переважно базуються на статичному аналізі коду та моніторингу транзакцій. Проте такий підхід не враховує комплексний характер сучасних атак, які використовують складні сценарії взаємодії між смарт-контрактами та особливості роботи blockchain-протоколів. Показовим прикладом є атака на протокол Beanstalk у квітні 2022 року, де зловмисники використали складну послідовність flash-loan операцій та маніпуляцій з governance-механізмом для викрадення активів на суму понад 180 мільйонів доларів. Цей інцидент продемонстрував обмеженість традиційних методів захисту перед складними векторами атак, що використовують легітимні механізми протоколу у зловмисних цілях. [1]

Метою дослідження є розробка системи виявлення та запобігання атак на blockchain-мережі, що базується на поведінковому аналізі смарт-контрактів з використанням методів машинного навчання.

В рамках дослідження розроблено: математичну модель поведінкового аналізу смарт-контрактів, що враховує динамічні патерни взаємодії та контекст виконання транзакцій; архітектуру системи моніторингу реального часу з використанням розподілених сенсорів; алгоритм машинного навчання для класифікації аномальної поведінки; методику автоматизованого реагування на виявлені загрози.

Запропонована система включає три основні компоненти:

- модуль збору та попередньої обробки даних, що забезпечує моніторинг мережевої активності та виконання смарт-контрактів [2];
- аналітичний модуль на базі ансамблю моделей машинного навчання для виявлення аномалій;
- підсистему реагування, що реалізує механізми превентивного захисту.

Попередні симуляції та теоретичний аналіз розробленої системи дозволяють прогнозувати високу ефективність у виявленні найпоширеніших векторів атак на смарт-контракти. Очікується, що система буде здатна ідентифікувати:

- reentrancy-атаки з теоретичною ефективністю виявлення до 95%;
- маніпуляції з цінами в liquidity pools через фронтраннінг та інші техніки;
- комплексні атаки з використанням flash-loans та крос-протокольних взаємодій.

Для підтвердження ефективності запропонованого рішення планується проведення серії експериментів на тестовій мережі Ethereum з імітацією різних сценаріїв атак. Попередні результати на обмеженому наборі тестових даних демонструють перспективність підходу, однак потребують подальшої валідації в умовах, наближених до реальних [3].

Потенційна практична цінність розробленої системи полягає у можливості її інтеграції з існуючими DeFi-протоколами як додаткового шару безпеки, що дозволить значно зменшити ризики фінансових втрат від нових типів атак. Очікується, що впровадження подібних систем моніторингу може скоротити загальні збитки галузі від хакерських атак на 30-40% щорічно.

Таким чином, запропонована система повинна забезпечувати комплексний захист blockchain-мереж через поведінковий аналіз смарт-контрактів, що дозволяє виявляти та запобігати складним атакам ще до їх реалізації. Подальші дослідження спрямовані на розширення можливостей системи для роботи з різними blockchain-платформами та вдосконалення механізмів автоматизованого реагування.

Список використаних джерел:

1. CertiK. Beanstalk Farms Loses $182M in Flash Loan Attack. URL: https://www.certik.com/resources/blog/k6eZOpnK5Kdde7RfHBZgw-beanstalk-farms-exploit (дата звернення: 20.02.2025).
2. Kanga D., Azzouazi M., Ghoumrari M., Daif A. Management and Monitoring of Blockchain Systems / Dominique Kanga, Mohamed Azzouazi, Mohammed Ghoumrari, Abderrahmane Daif // Procedia Computer Science. – 2020. – T. 177. – P. 605-612. URL: https://www.researchgate.net/publication/346870622_Management_and_Monitoring_of_Blockchain_Systems (дата звернення: 19.02.2025).
3. Перелік токенів Ethereum. [URL].- Режим доступу: https://etherscan.io/tokens (дата звернення: 19.02.2025).