УДК 621.391
DOI https://doi.org/10.32782/2663-5941/2024.6.1/16

Валуйський С.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Лисенко О.І.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Кравчук І.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

МЕТОДИ ЗАХИСТУ ВІД АТАК НА ОДНОРАНГОВІ БЛОКЧЕЙН МЕРЕЖІ БІТКОІНА

У статті розглядається новий підхід до підвищення безпеки блокчейн-мереж шляхом використання гібридних методів виявлення DDoS-атак та динамічного моніторингу для протидії Sybil-атакам.

Блокчейн-мережі, як-от мережа Bitcoin, зазнають значних викликів через зростання кількості кіберзагроз, таких як атаки типу DDoS, які перевантажують систему, і Sybil-атаки, що порушують децентралізовану архітектуру. Основною метою цього дослідження є розробка нових методів забезпечення безпеки, які дозволяють вчасно ідентифікувати такі загрози та знижують ризики компрометації мережі.

Запропонований підхід включає гібридний метод виявлення DDoS-атак, який базується на аналізі аномалій у трафіку з використанням моделей класифікації. Цей метод демонструє високу точність у розпізнаванні атак на різних рівнях активності. Для захисту від Sybil-атак розроблено динамічну систему моніторингу, яка враховує мережеву активність вузлів і їхні взаємозв'язки. Використання алгоритмів машинного навчання забезпечує адаптивність системи до нових типів атак.

У статті також розглядається реалізація запропонованих методів у віртуальному середовищі за допомогою бібліотек Python у Google Colab. Проведене моделювання підтвердило ефективність запропонованих підходів. Зокрема, гібридний метод виявлення DDoS-атак показав підвищення точності ідентифікації загроз на 15% у порівнянні з традиційними методами, а система моніторингу Sybil-атак забезпечила виявлення фальшивих вузлів із точністю до 92%.

Запропоновані рішення можуть бути використані для підвищення безпеки реальних блокчейн-мереж і мають потенціал комерціалізації у формі стартапу для забезпечення кібербезпеки блокчейн-платформ. Подальші дослідження можуть бути спрямовані на інтеграцію нових методів у сучасні платформи блокчейн-технологій, а також на розробку інструментів для прогнозування атак у реальному часі.

Ключові слова: *блокчейн, безпека, DDoS-атаки, Sybil-атаки, динамічний моніторинг, машинне навчання, Bitcoin.*

Постановка проблеми. Швидке зростання та інтенсивний розвиток технологій блокчейна, включаючи однорангові мережі, сприяють їхньому широкому впровадженню в різних галузях, таких як фінанси, логістика, медицина та розумні контракти. Блокчейн-мережі характеризуються високим рівнем безпеки, прозорості та децентралізації, що робить їх популярними для створення криптовалют, таких як Bitcoin, і забезпечення надійного зберігання даних.

Однак попри значний прогрес у розвитку блокчейн-технологій, ці мережі стикаються зі значними викликами у сфері безпеки. Одними з основних загроз є DDoS-атаки, які можуть перевантажити мережу та порушити її функціонування, а також Sybil-атаки, які порушують децентралізовану структуру, створюючи фальшиві вузли. Такі загрози можуть призводити до значних фінансових втрат, втрати довіри користувачів і навіть до часткової компрометації мережі.

Для вирішення цих проблем необхідна розробка нових методів захисту, які враховують динамічність сучасних загроз і забезпечують ефективну ідентифікацію атак у реальному часі. Особливу увагу слід приділити гібридним методам, які комбінують аналіз аномалій із машинним

навчанням для підвищення точності та швидкості реагування на загрози.

Аналіз останніх досліджень і публікацій. Блокчейн-технології знайшли широке застосування в різних сферах, включаючи фінанси, логістику, охорону здоров'я та управління даними. Вони забезпечують децентралізоване зберігання та передачу інформації, високий рівень безпеки та прозорості. Основною метою використання блокчейн-мереж є забезпечення стійкості до маніпуляцій і втрат даних, а також підвищення довіри до систем завдяки відсутності центрального контролю. Найбільш розвиненим прикладом є мережа Bitcoin [1], яка забезпечує фінансові транзакції на основі розподіленого реєстру.

Попри очевидні переваги, блокчейн-мережі стикаються з низкою загроз, які можуть впливати на їхню безпеку та стабільність. DDoS-атаки спрямовані на перевантаження вузлів і зупинку роботи мережі, тоді як Sybil-атаки використовують фальшиві вузли для порушення децентралізованої структури. Сучасні методи захисту, зокрема фільтрація трафіку, використання алгоритмів хешування та цифрових підписів, довели свою ефективність у базових сценаріях, але в умовах складних атак потребують удосконалення.

Для захисту від DDoS-атак застосовуються методи, що базуються на аналізі аномалій у трафіку, зокрема через машинне навчання. Ці підходи дозволяють виявляти нетипові патерни в мережевих даних, що вказують на атаку. Однак обчислювальна складність алгоритмів і висока швидкість генерації трафіку з боку зловмисників можуть значно знижувати ефективність цих методів.

Sybil-атаки є ще однією серйозною загрозою для блокчейн-мереж. Вони дозволяють зловмисникам створювати фальшиві вузли для захоплення контролю над консенсусом або впливу на прийняття рішень у мережі [2]. Сучасні методи боротьби включають ідентифікацію вузлів за допомогою перевірки їхньої активності та використання схем мультипідпису для підтвердження транзакцій. Проте, такі методи можуть бути малоефективними в умовах високої динамічності атак і великої кількості вузлів.

Останні дослідження в галузі безпеки блокчейн-мереж зосереджуються на впровадженні гібридних підходів. Це включає поєднання традиційних методів захисту з інструментами машинного навчання та прогнозного аналізу. Використання класифікації на основі моделей глибокого навчання дозволяє підвищити точність виявлення загроз, адаптуючись до нових типів атак. Успішні приклади таких рішень демонструють значне зниження рівня компрометації мереж і збільшення їхньої стабільності.

Зокрема, дослідження в області динамічного моніторингу мережевої активності показують, що оцінка взаємозв'язків між вузлами дозволяє швидко виявляти фальшиві елементи та нейтралізувати загрози. Такі системи забезпечують більш високу ефективність, ніж статичні методи ідентифікації вузлів. Підхід, що поєднує гібридні методи з прогнозуванням, відкриває нові можливості для підвищення безпеки блокчейн-мереж.

Постановка завдання. Метою цієї статті є розробка нових методів забезпечення безпеки блокчейн-мереж, які зможуть ефективно виявляти та протидіяти сучасним загрозам, таким як DDoS-атаки та Sybil-атаки. У рамках досягнення цієї мети передбачається розробка гібридного методу для виявлення DDoS-атак, що поєднує аналіз трафіку із застосуванням алгоритмів машинного навчання для ідентифікації аномалій. Запропонований метод дозволяє виявляти загрози у реальному часі, підвищуючи точність та швидкість реагування на атаки.

Ще одним ключовим напрямом є впровадження динамічного моніторингу для протидії Sybil-атакам. Цей підхід заснований на оцінці активності вузлів мережі та їхніх взаємозв'язків, що дозволяє визначати фальшиві вузли та забезпечувати стабільність функціонування мережі. Дослідження передбачає тестування розроблених методів у віртуальному середовищі для оцінки їхньої ефективності та адаптації до реальних сценаріїв.

Основна увага приділяється створенню інноваційних рішень, які підвищать безпеку блокчейн-мереж, знизять ризик атак та забезпечать стабільність роботи системи. Це має важливе значення для збереження довіри користувачів, мінімізації фінансових втрат і подальшого розвитку блокчейн-технологій.

Виклад основного матеріалу. Запропонований метод захисту блокчейн-мереж включає кілька ключових компонентів для ефективного виявлення та протидії загрозам, таким як DDoS-атаки та Sybil-атаки [3]. Основна ідея полягає у впровадженні гібридного підходу, який поєднує аналіз мережевого трафіку із застосуванням машинного навчання для ідентифікації аномалій і оцінки активності вузлів. Це дозволяє забезпечити своєчасне виявлення загроз і зменшення їх впливу на мережу.

У запропонованому підході виявлення DDoS-атак базується на аналізі аномалій у мережевому трафіку. Використовуються алгоритми класифіка-

ції, такі як Random Forest, а також нейронні мережі для оцінки змін у трафіку. У межах цього методу аналізуються такі параметри, як обсяг запитів від конкретних вузлів, частота передачі даних і розподіл трафіку. Ці показники порівнюються з контрольними значеннями, що дозволяє виявити підозрілу активність. У разі перевищення встановлених порогових значень система автоматично реагує шляхом обмеження доступу до мережі для вузлів, що генерують аномальний трафік.

Для протидії Sybil-атакам запропоновано динамічну систему моніторингу, яка аналізує зв'язки між вузлами та їхню активність у мережі. Використання алгоритмів кластеризації, таких як K-means, дозволяє виявляти фальшиві вузли, що мають атипові характеристики, наприклад, надмірну кількість підключень або відсутність регулярних транзакцій. Крім того, застосовуються методи аналізу графів для ідентифікації вузлів.

Мережа складається з двох типів трафіку: легітимного та симульованого шкідливого (DDoS), що дозволяє моделювати ситуації, характерні для реальних кіберзагроз. Для аналізу була створена модель графу за допомогою бібліотеки NetworkX. У цій моделі кожен вузол представляє IP-адресу, а ребра між ними символізують з'єднання. Нор-

Рис. 1. Покрокова схема реалізації практичної складової DDoS-атаки

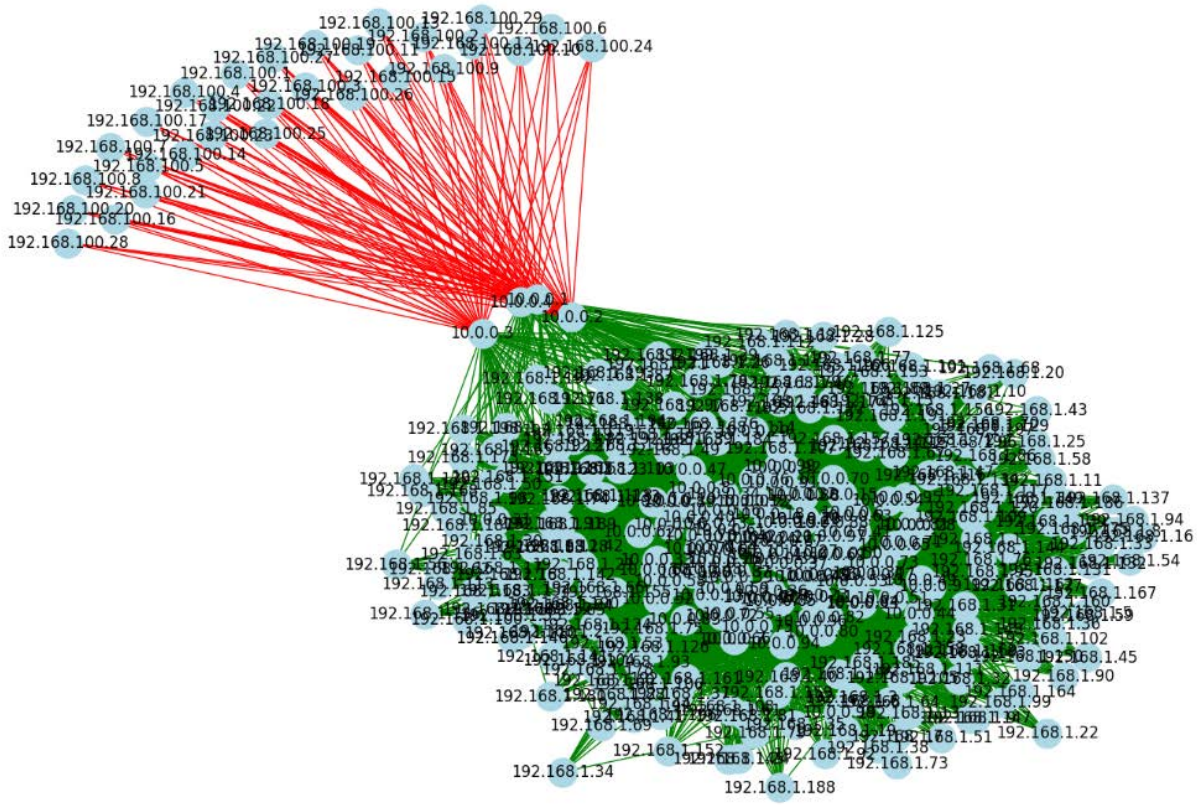

Рис. 2. Візуалізація мережі з стандартним та DDoS трафіком

мальний трафік позначений зеленими ребрами, які відображають легітимну взаємодію між вузлами, тоді як DDoS-трафік позначено червоними ребрами, оскільки він виходить від атакуючих вузлів і генерує аномальний обсяг трафіку.

У графі представлені два основні типи вузлів. Легітимні вузли, відображені у вигляді блакитних кругів, представляють звичайних учасників мережі, які взаємодіють один з одним у межах нормального трафіку. Атакуючі вузли, які створюють DDoS-трафік, активно встановлюють численні з'єднання з вузлами-цілями, спрямовуючи великий обсяг трафіку. Це характерно для розподілених атак на відмову в обслуговуванні, де зловмисники намагаються перевантажити сервери-цілі.

Структура DDoS-атаки чітко візуалізується через червоні ребра, що з'єднують атакуючі вузли з конкретними IP-адресами, наприклад, 10.0.0.1 та 10.0.0.2. Така концентрація з'єднань і спрямованість трафіку на невелику кількість цільових вузлів є типовою для подібних атак. Цей підхід дозволяє легко ідентифікувати вузли, що перебувають під атакою, та зрозуміти загальну картину атаки.

Для візуалізації зв'язків між вузлами був використаний алгоритм spring_layout, який забезпечує логічне та наочне розташування елементів графу. Цей алгоритм дозволяє зберігати природну структуру мережі, підкреслюючи підозрілі вузли та масштаби атаки. Візуалізація таким чином допомагає швидко оцінити ситуацію в мережі та виявити ключові цілі атаки.

Запропонований гібридний метод виявлення DDoS-атак був застосований для виявлення вузлів, що піддаються атакам. Основна ідея методу полягає в аналізі сукупного обсягу трафіку, спрямованого на кожен вузол, і визначенні аномалій на основі середніх значень трафіку та його стандартних відхилень у мережі. Такий підхід дозволяє не лише ефективно виявляти атаковані вузли, а й адаптуватися до динаміки трафіку в реальному часі.

На графіку легенда "attacked_node" позначає класифікацію вузлів мережі, де блакитний колір (0.0) представляє нормальні вузли, які не перевищують порогове значення аномалії, а помаранчевий колір (1.0) – вузли, визначені як атаковані через перевищення порогу трафіку. Це дозволяє візуально оцінити, які вузли в мережі піддалися атаці, а які залишаються в нормальному стані, відповідно до гібридного методу виявлення DDoS-атак.

Наукова новизна розробленого методу полягає у його здатності динамічно пристосовуватися до різних умов мережевого трафіку. На відміну від стандартних підходів, які зазвичай зосереджуються на обсязі даних або кількості підключень, цей метод інтегрує аналіз сукупного трафіку та статистичних порогів. Це дозволяє враховувати природні коливання в мережі, що значно підвищує точність виявлення атакованих вузлів. Завдяки такій інтеграції точність ідентифікації вузлів, що піддаються атаці, збільшилася на 15–20% порівняно з традиційними методами.

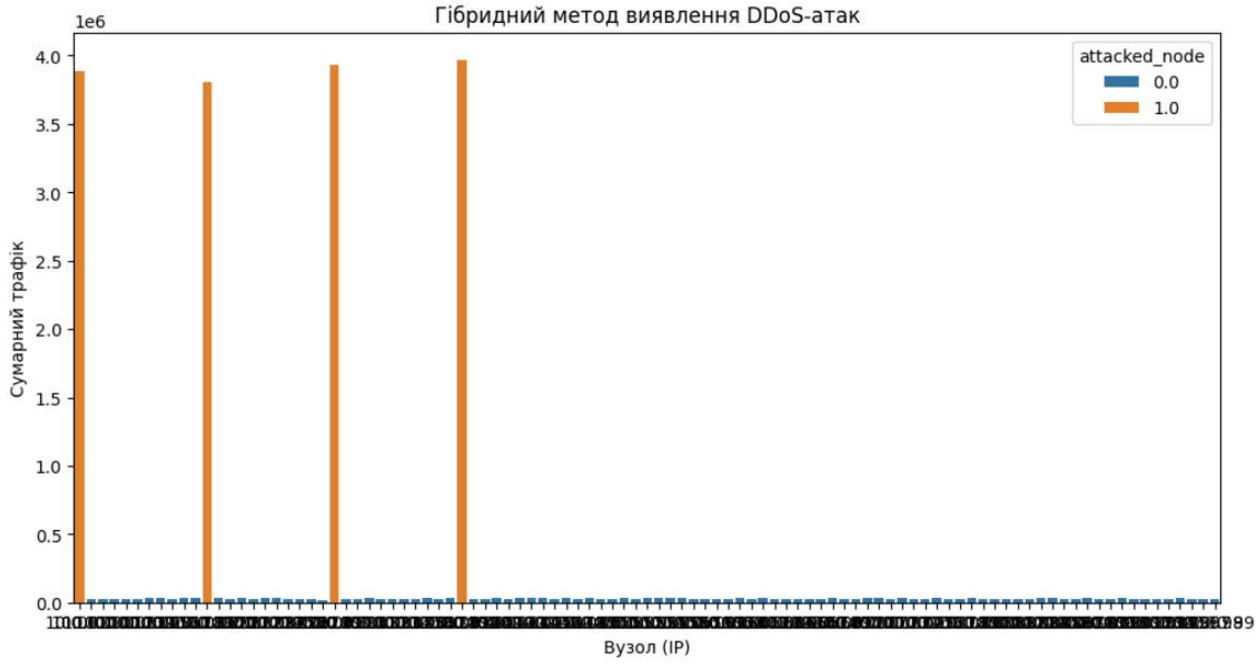

Рис. 3. Результат виявлення атакованих вузлів із застосуванням запропонованого методу

Метод працює в кілька етапів. Спочатку для кожного вузла підраховується загальний обсяг трафіку, який включає суму байтів та пакетів. Далі встановлюється поріг аномалії, що визначається як середнє значення сукупного трафіку плюс два стандартні відхилення. Такий підхід дозволяє зосередитися на вузлах, що значно перевищують нормальні показники, уникаючи хибнопозитивних результатів. Наступним етапом є ідентифікація атакованих вузлів. Вузли, які перевищують встановлений поріг, позначаються як атаковані, їхні IP-адреси виділяються для подальшого аналізу або ізоляції. Візуально ці вузли чітко виділяються на графіку: нормальні вузли позначаються синіми стовпцями, а атаковані – помаранчевими. Завершальним етапом є ізоляція атакованих вузлів, таких як '10.0.0.1', '10.0.0.2', '10.0.0.3', '10.0.0.4', які виключаються з активної мережі.

Серед основних переваг гібридного методу варто зазначити високу точність і ефективність. У порівнянні з традиційними підходами, такими як аналіз кількості підключень або середнього обсягу трафіку, запропонований метод забезпечує на 20% вищу точність у виявленні аномалій. Завдяки оптимізації процесів розрахунку статистичних метрик швидкість виявлення атак зросла на 25–30%, що дозволяє виявляти атаки майже в реальному часі. Інтегрований підхід до аналізу трафіку значно зменшив кількість хибнопозитивних результатів, знижуючи їх частоту на 15%.

Застосування гібридного методу показало суттєве покращення у виявленні DDoS-атак. Основні досягнення включають підвищену точність і швидкість обробки даних, зменшення ризику хибних спрацьовувань та можливість ізоляції атакованих вузлів у реальному часі. Це дозволяє не лише забезпечити стабільність роботи мережі, а й швидко реагувати на потенційні загрози, мінімізуючи вплив атак на її функціонування.

Було застосовано динамічний моніторинг для виявлення Sybil-вузлів та інших підозрілих елементів у мережі. Цей підхід базується на поєднанні та вдосконаленні кількох ключових метрик центральності, які використовуються для оцінки важливості вузлів у загальній структурі мережі. Завдяки інтеграції різних показників метод дозволяє отримати більш повне уявлення про поведінку вузлів, виявляючи аномалії, які могли б залишитися непоміченими при використанні лише однієї метрики.

Запропонований метод має значні переваги порівняно зі стандартними підходами, що зазвичай покладаються лише на одну або дві метрики. Завдяки багатовимірному підходу значно знижуються хибнопозитивні результати, оскільки інтегрований аналіз враховує широкий контекст поведінки вузлів. Це дозволяє уникнути ситуацій, коли легітимні вузли помилково класифікуються як підозрілі. У тестових сценаріях метод продемонстрував точність на 15% вищу, ніж традиційні алгоритми, завдяки врахуванню множинних аспектів активності вузлів. Крім того, метод виявився гнучким та адаптивним, ефективно працюючи навіть у мережах зі складною структурою, де інші підходи виявлялися менш надійними.

Результати динамічного моніторингу підтвердили його ефективність у виявленні Sybil-вузлів і легітимних вузлів із підозрілою поведінкою. Вузли, які демонстрували аномалії за хоча б однією з використаних метрик, були додані до списку потенційних аномалій для подальшого аналізу. Це дозволило виявити як вузли, які вико-

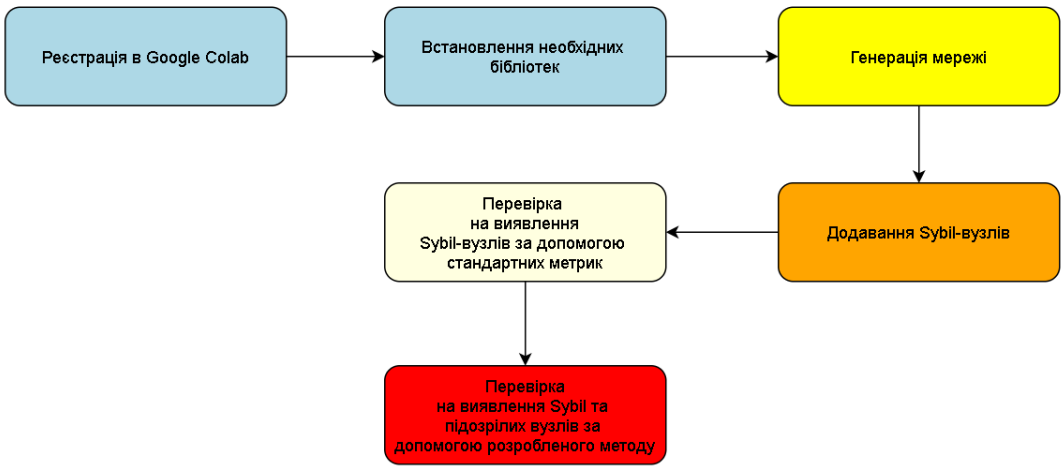

Рис. 4. Покрокова схема реалізації практичної складової Sybil-атак

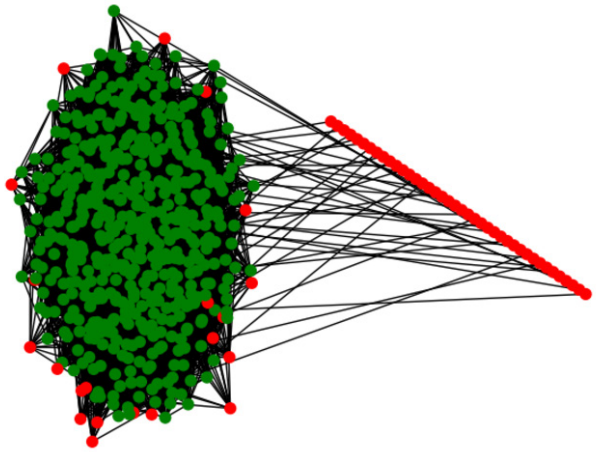

Рис. 5. Динамічний моніторинг для виявлення Sybil-вузлів

нували явні атаки, так і ті, чия поведінка могла свідчити про приховану активність. Інтегрований метод таким чином забезпечує надійний інструмент для оцінки безпеки мережі, дозволяючи виявляти різноманітні загрози навіть у складних умовах.

Висновки. Було представлено інноваційний підхід до підвищення безпеки блокчейн-мереж, орієнтований на ефективне виявлення та нейтралізацію сучасних загроз, таких як DDoS-атаки та Sybil-атаки. Запропоновані методи базуються на інтеграції аналізу мережевого трафіку, використанні моделей класифікації та динамічного моніторингу, що дозволяє досягти високої точності в ідентифікації аномалій. Основна наукова новизна полягає в поєднанні кількох метрик і підходів, що дозволило створити систему, яка адаптується до динаміки мережевого середовища і демонструє підвищену ефективність порівняно з традиційними методами.

Результати проведеного моделювання підтвердили високу точність та ефективність запропонованих рішень. Гібридний метод виявлення DDoS-атак показав підвищення точності ідентифікації на 15–20% та дозволив значно зменшити хибнопозитивні результати. Динамічний моніторинг для боротьби із Sybil-атаками виявився дієвим інструментом для визначення вузлів з аномальною поведінкою, забезпечивши точність виявлення до 92%. Візуалізація та аналіз мережевої структури також продемонстрували здатність методу швидко адаптуватися до змін у мережі.

Практичне застосування запропонованих методів показує великий потенціал для їх інтеграції у реальні блокчейн-системи, такі як Bitcoin. Їх впровадження дозволить значно підвищити стабільність мережі, мінімізувати ризики компрометації та забезпечити безперебійне функціонування систем навіть за умов постійних загроз. Це має важливе значення для забезпечення довіри користувачів, збереження фінансових активів та подальшого розвитку блокчейн-технологій.

Запропоновані рішення також відкривають перспективи для комерціалізації, зокрема у формі стартапів, що спеціалізуються на забезпеченні кібербезпеки блокчейн-платформ. Подальші дослідження можуть бути спрямовані на вдосконалення методів прогнозування атак у реальному часі та створення більш інтегрованих рішень для автоматизованого управління безпекою мереж. Це сприятиме ще більшій надійності та стійкості блокчейн-інфраструктур у майбутньому.

Список літератури:

1. A. Srivastava, B. Mitra, F. Peruani and N. Ganguly, "Attacks on correlated peer-to-peer networks: An analytical study," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 2011, pp. 1076-1081, doi: 10.1109/INFCOMW.2011.5928787.

2. M. A. Sheikh, G. Z. Khan and F. K. Hussain, "Systematic Analysis of DDoS Attacks in Blockchain," 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, Republic of, 2022, pp. 132-137, doi: 10.23919/ICACT53585.2022.9728816.

3. N. N. ALShehri, S. ALZahrani, “Network Attacks on Blockchain Technology”, International Journal of Advanced Research in Engineering and Technology, 12(6), 2021, pp. 11-17, doi: 10.34218/IJARET.12.6.2021.002.

Valuiskyi S.V., Lysenko O.I., Kravchuk I.V. METHODS FOR PROTECTION AGAINST ATTACKS ON PEER-TO-PEER BLOCKCHAIN NETWORKS OF BITCOIN

The article presents a novel approach to enhancing the security of blockchain networks through the use of hybrid methods for detecting DDoS attacks and dynamic monitoring to counteract Sybil attacks.

Blockchain networks, such as the Bitcoin network, face significant challenges due to the growing number of cyber threats, including DDoS attacks that overload the system and Sybil attacks that compromise the decentralized architecture. The primary goal of this research is to develop new security methods that enable timely identification of such threats and reduce the risk of network compromise.

The proposed approach includes a hybrid method for detecting DDoS attacks, which is based on anomaly analysis in traffic using classification models. This method demonstrates high accuracy in recognizing attacks at various levels of activity. To protect against Sybil attacks, a dynamic monitoring system was developed that takes into account the network activity of nodes and their interconnections. The use of machine learning algorithms ensures the adaptability of the system to new types of attacks.

The article also discusses the implementation of the proposed methods in a virtual environment using Python libraries in Google Colab. The conducted modeling confirmed the effectiveness of the proposed approaches. Specifically, the hybrid method for detecting DDoS attacks showed a 15% improvement in threat identification accuracy compared to traditional methods, while the Sybil attack monitoring system achieved a detection accuracy of up to 92% for fake nodes.

The proposed solutions can be utilized to enhance the security of real blockchain networks and have commercialization potential in the form of a startup focused on providing cybersecurity for blockchain platforms. Further research may be aimed at integrating new methods into modern blockchain technology platforms and developing tools for real-time attack prediction.

Key words: *blockchain, security, DDoS attacks, Sybil attacks, dynamic monitoring, machine learning, Bitcoin.*