УДК 004.056.5:004.738

І. С. Зоря
М. В. Римаренко

ІНТЕГРАЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТВОРЕННЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ОБМІНУ КІБЕРРОЗВІДУВАЛЬНОЮ ІНФОРМАЦІЄЮ

Вінницький національний технічний університет

Анотація

У роботі розглянуто підхід до побудови децентралізованої системи обміну кіберрозвідувальною інформацією на основі інтеграції технології блокчейн та методів штучного інтелекту. Показано, що блокчейн доцільно використовувати для забезпечення цілісності, простежуваності та розподіленої довіри, а штучний інтелект – для автоматизованого вилучення, класифікації та оцінювання кіберрозвідувальних даних. Запропоновано концептуальну архітектуру системи та визначено її основні переваги й обмеження.

Ключові слова: блокчейн, штучний інтелект, кіберрозвідувальна інформація (CTI) кібербезпека, смарт-контракти, децентралізована система, індикатори компрометації.

Abstract

This paper considers an approach to building a decentralized cyber threat intelligence sharing system through the integration of blockchain technology and artificial intelligence methods. Blockchain is used to ensure integrity, traceability, and distributed trust, while artificial intelligence is applied to the automated extraction, classification, and evaluation of cyber threat intelligence data. A conceptual architecture of the system is proposed, and its main advantages and limitations are outlined.

Keywords: blockchain, artificial intelligence, cyber threat intelligence (CTI), cybersecurity, smart contracts, decentralized system, indicators of compromise.

Вступ

Сучасні кіберзагрози стають дедалі складнішими, тому ефективний обмін кіберрозвідувальною інформацією є важливою умовою своєчасного виявлення та попередження атак. Традиційні централізовані платформи обміну мають обмеження, пов'язані з довірою, прозорістю та захистом даних, тоді як значна частина CTI надходить у неструктурованій формі й потребує автоматизованого аналізу. У зв'язку з цим перспективним є поєднання блокчейну як засобу забезпечення цілісності та простежуваності даних із методами штучного інтелекту, що дозволяють автоматизувати їх вилучення, класифікацію та оцінювання. Метою роботи є обґрунтування концептуальної моделі децентралізованої системи обміну кіберрозвідувальною інформацією на основі інтеграції цих технологій.

Результати дослідження

Обмін кіберрозвідувальною інформацією є важливим складником проактивного кіберзахисту, однак його практична ефективність залежить від своєчасності, релевантності та надійності даних. Серед основних проблем у цій сфері зазвичай виокремлюють недостатній рівень довіри між учасниками, небажання організацій ділитися чутливою інформацією, ризики витоку даних, а також труднощі автоматизації процесів споживання й повторного використання отриманої розвідувальної інформації [1].

Одним із перспективних способів усунення частини цих обмежень є використання технології блокчейн. Розподілений реєстр дозволяє фіксувати факти надходження, перевірки, оновлення та використання даних таким чином, щоб кожен запис мав часову позначку, криптографічний відбиток і міг бути перевірений усіма уповноваженими учасниками мережі. Завдяки цьому забезпечуються

цілісність та стійкість до несанкціонованої модифікації, що є критично важливим для побудови довіреного середовища обміну CTI [2].

Разом із цим використання блокчейну в системах обміну кіберрозвідувальною інформацією не означає, що всі дані повинні зберігатися безпосередньо в ланцюжку блоків. Більш доцільним є підхід, за якого в реєстр записуються метадані, хеші документів, відомості про джерело, права доступу та результати валідації, водночас великі масиви інформації, такі як: звіти, телеметрія, добірки індикаторів компрометації – зберігаються поза блокчейном. У такій моделі смарт-контракти можуть керувати правилами доступу, реєстрацією учасників, механізмами стимулювання та контролем взаємодії між постачальниками і споживачами інформації [3].

Інтеграція штучного інтелекту є необхідною через те, що значна частина кіберрозвідувальних відомостей надходить у неструктурованій формі. Методи машинного навчання та обробки природної мови дають змогу автоматично вилучати з текстових джерел індикатори компрометації, назви шкідливого програмного забезпечення, домени, IP-адреси, хеші файлів, а також відомості про тактики, техніки й процедури порушників. Це дозволяє перетворювати текстові повідомлення та звіти на структуровані дані, придатні для подальшого пошуку, кореляції та використання в системах моніторингу безпеки [4].

Для забезпечення сумісності така архітектура має спиратися на стандартизоване представлення та передавання даних. Доцільним є використання STIX для формалізованого опису кіберрозвідувальних об’єктів і TAXII для регламентованого обміну. Поєднання цих стандартів із приватним блокчейном дає змогу впорядкувати дані CTI, контролювати доступ до них і підвищити надійність та прозорість обміну. [5].

З урахуванням наведених підходів архітектура децентралізованої системи обміну кіберрозвідувальною інформацією може складатися з кількох взаємопов’язаних рівнів: рівня джерел даних, рівня інтелектуальної обробки, блокчейн-рівня реєстрації подій, рівня смарт-контрактів і прикладного рівня використання отриманої інформації в SIEM, SOAR та аналітичних системах. На першому рівні відбувається збирання відомостей із сенсорів, логів, відкритих джерел, CERT/CSIRT повідомлень та аналітичних звітів.

На другому рівні модулі ШІ виконують очищення, нормалізацію, класифікацію і пріоритизацію даних. Далі блокчейн забезпечує реєстрацію подій обміну, а смарт-контракти – формалізацію політик взаємодії. У підсумку споживачі отримують не лише набір сирих повідомлень, а структуровану, перевірювану й придатну до оперативного використання кіберрозвідувальну інформацію.

Попри значні переваги, запропонований підхід має й низку обмежень. Блокчейн потребує вирішення питань масштабованості, конфіденційності та узгодження правил участі у мережі, а якість рішень на базі ШІ залежить від повноти навчальних вибірок, точності моделей і здатності адаптуватися до нових типів загроз. Водночас сучасні дослідження у сфері CTI свідчать, що поєднання автоматизованого аналізу, машинного навчання та інтелектуального вилучення знань із різнорідних джерел є одним із найперспективніших напрямів розвитку проактивного кіберзахисту [6].

Висновки

У роботі показано, що інтеграція технології блокчейн та штучного інтелекту є доцільною для створення децентралізованої системи обміну кіберрозвідувальною інформацією. Блокчейн забезпечує цілісність, простежуваність, аудит та розподілену довіру між учасниками, а штучний інтелект дозволяє автоматизувати вилучення, класифікацію й оцінювання даних про загрози.

Запропонований підхід доцільно розглядати як основу для побудови сучасних CTI-платформ, орієнтованих на безпечний міжорганізаційний обмін, зменшення залежності від централізованих посередників та прискорення реагування на інциденти. Перспективою подальших досліджень є створення прототипу системи з підтримкою STIX/TAXII, смарт-контрактів і модулів ШІ для аналізу неструктурованих джерел загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wagner T. D., Mahbub K., Palomar E., Abdallah A. E. Cyber threat intelligence sharing: Survey and research directions. Computers & Security. 2019. Vol. 87. Art. 101589.

2. Gong S., Lee C. BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance. Electronics. 2020. Vol. 9, No. 3. Art. 521.

3. Riesco R., Larriva-Novo X., Villagra V. A. Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and smart contracts to foster the cyber threat and risk intelligence exchange of information. Telecommunication Systems. 2020. Vol. 73, No. 2. P. 259–288.

4. Ghazi Y., Anwar Z., Mumtaz R., Saleem S., Tahir A. A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. 2018 International Conference on Frontiers of Information Technology (FIT). 2018.

5. Provatas K.-A., Tzannetos I., Vescoukis V. C. Standards-based Cyber Threat Intelligence Sharing Using Private Blockchains. *Proceedings of the 18th Conference on Computer Science and Intelligence Systems*. 2023. P. 649–656.

6. Sun N., Ding M., Jiang J., Xu W., Mo X., Tai Y., Zhang J. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials. 2023. Vol. 25. P. 1748–1774.

Римаренко Микола Вікторович **–** студент групи КІТС-25м, Факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: craaaashbaaashl@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** **–** ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: ira.zoria@vntu.edu.ua

Rymarenko Mykola V. – student of the KITS-25m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: craaaashbaaashl@gmail.com

Supervisor: ***Zoria Iryna S.*** **–** assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: ira.zoria@vntu.edu.ua