dern warfare, the winner is the one who is quicker to perceive new technologies and implement them, adopts and implements new military doctrines and concepts that are in line with the spirit of the times and enable not only the use of new technologies and ideas, but also knows well which ones to use and when. High technologies are now turning into a systemic factor in modern armed struggle. They make it possible to reach that new stage in the development of military art – the transition from command and control of troops in the course of armed struggle to conflict management in general.
Keywords: network-centric warfare, hybrid warfare, Warden rings, Boyd's theory.

Артемов Володимир Юрійович, доктор педагогічних наук, професор, професор спеціальної кафедри Національної академії СБУ.

Volodymyr Artemov, doctor of pedagogical sciences, professor, professor of the special department of the National Academy of SBU.
E-mail: Vuk_karadzic@ukr.net.
Orcid ID: 0000-0002-5290-4496.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

DOI: 10.18372/2410-7840.26.18844
УДК 004.056.5

O HARNESSING BLOCKCHAIN AND EBPF FOR IMMUTABLE AUDIT OF SYSTEM EVENTS: A TECHNOLOGICAL CONVERGENCE APPROACH

Pavlo Hlushchenko, Valerii Dudykevych

The importance of secure and reliable system event auditing has grown significantly in today's complex IT environments, where data integrity and security are paramount. Traditional auditing methods, which rely on centralized systems and are vulnerable to tampering and performance bottlenecks, are no longer sufficient. This article addresses these challenges by proposing a novel framework that combines blockchain and eBPF technologies to create an immutable, transparent, and efficient system for event auditing. The proposed solution leverages eBPF's real-time monitoring capabilities and blockchain's tamper-proof ledger to ensure the integrity and verifiability of audit logs. Through a detailed exploration of the conceptual framework and an analysis of potential challenges and solutions, this approach has proven to be effective in enhancing the reliability and security of system event auditing. The results of this study provide a foundation for future implementations, research and robust solutioning for organizations seeking to improve their auditing processes.
***Keywords**: event auditing, blockchain, eBPF, immutability, monitoring.*

INTRODUCTION

The primary objective of this article is to explore the innovative application of blockchain technology coupled with eBPF (Extended Berkeley Packet Filter) in the domain of system event auditing. Given the growing complexity and security requirements of modern computing environments, traditional auditing methods often fall short in providing the necessary transparency and integrity. This article proposes a novel approach that harnesses the immutable and decentralized nature of blockchain along with the powerful monitoring capabilities of eBPF to enhance the reliability and efficiency of auditing processes.

Auditing system events is critical in ensuring the security and compliance of information systems. It involves tracking and analyzing operations on the system to detect anomalies, unauthorized changes, and potential breaches. As systems grow in complexity, the volume of events increases exponentially, making it increasingly challenging to manage and secure these logs against tampering. Effective auditing helps organizations not only to comply with regulatory requirements but also to maintain the integrity and confidentiality of their data.

This article delves into two pivotal technologies: blockchain and eBPF. Blockchain is renowned for its robustness in managing data in a tamper-resistant manner across a distributed network, making it a valuable tool for enhancing the security and transparency of audit trails. On the other hand, eBPF provides a highly flexible and efficient framework for monitoring system events directly from the kernel space, offering precise visibility and control over system operations. The convergence of these technologies presents a promising avenue for redefining traditional system event auditing frameworks, promising enhanced security features and operational efficiencies.

Previous research has extensively explored the use of eBPF for monitoring and observability, highlighting its capabilities in providing real-time, kernel-level monitoring of system activities [2, 4, 9]. Similarly, numerous studies have investigated the application of blockchain technology for securing system event auditing and logging, demonstrating its effectiveness in creating immutable and tamper-proof records [1, 3, 5]. However, none of these works have combined eBPF and blockchain technologies to secure the system event auditing process. This gap in the literature prompted me to undertake this study, aiming to integrate eBPF's real-time monitoring capabilities with blockchain's immutable ledger to enhance the security and reliability of system event auditing.

This exploration aims to demonstrate the applicability and benefits of integrating blockchain with eBPF for auditing purposes as well as an architecture blueprint for future practical implementation.

MAIN PART

Blockchain technology, first introduced as the underlying mechanism behind Bitcoin, is a decentralized ledger that facilitates the recording of transactions across multiple computers in such a way that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. These blocks are cryptographically linked to the previous block, forming an unbroken chain of data. This structure ensures that once a block is added to the blockchain, the information it contains cannot be altered without modifying all subsequent blocks, which requires consensus from the network participants. This technology provides a verifiable and permanent data record, free from control by any single authority, making it inherently resistant to modification, fraud, and deletion. At its core, a blockchain is a series of interconnected blocks, each containing a timestamp, transaction data, and the cryptographic hash of the previous block.

Blockchain technology boasts several distinctive features that contribute to its robustness and reliability. First, decentralization is a fundamental characteristic, meaning that the control of the blockchain is distributed across a network of nodes rather than being centralized in a single entity. This decentralization enhances security and reduces the risk of data manipulation. Second, immutability ensures that once data is recorded on the blockchain, it cannot be changed or deleted, providing a permanent and tamper-proof record. Third, transparency allows all network participants to view and verify the transactions, fostering trust and accountability. Lastly, blockchain employs cryptographic algorithms to secure the data, ensuring that only authorized parties can access and interact with the information.

System event auditing is a crucial aspect of maintaining the integrity and security of IT infrastructures. It involves the continuous monitoring and recording of system activities to detect and investigate anomalies, ensure compliance, and provide forensic evidence in case of incidents. Traditionally, system event auditing is performed using agents that are installed on individual machines or built-in tools such as Windows Event Collector (WEC). These agents collect logs and send the information to a centralized server, where the data is stored, analyzed, and monitored. While this method is effective in capturing system events, it has several vulnerabilities. Centralized storage can be a single point of failure and is susceptible to tampering, unauthorized access, and data breaches. Additionally, the integrity of the audit logs can be compromised if an attacker gains control over the centralized server or the agents themselves.

Blockchain technology addresses these challenges by providing an immutable and transparent ledger for recording system events [6]. By using blockchain, every system event is permanently recorded in a way that cannot be altered retroactively. This ensures that audit logs are both tamper-proof and verifiable, significantly enhancing the trustworthiness of the auditing process. Furthermore, the decentralized nature of blockchain means that the audit logs are not controlled by a single entity, reducing the risk of manipulation and ensuring that the data remains secure and intact. Blockchain's inherent features of decentralization, immutability, and transparency make it an ideal solution for overcoming the limitations of traditional system event auditing methods.

Blockchain was chosen for system event auditing due to its unparalleled ability to create a secure, immutable, and transparent record of events. The decentralized architecture of blockchain eliminates the risks associated with central points of failure, ensuring that the audit logs are resilient and distributed across multiple nodes. This makes it extremely difficult for malicious actors to alter the records without detection. Additionally, the cryptographic techniques employed by blockchain enhance the security of the data, ensuring that only authorized users can access and verify the information. By leveraging blockchain, we can create an audit system that not only preserves the integrity of the recorded events but also provides a reliable and trustworthy

framework for auditing in dynamic and complex IT environments.

Extended Berkeley Packet Filter (eBPF) is a powerful technology that extends the conventional capabilities of the Berkeley Packet Filter (BPF), enabling the safe execution of bytecode at various hook points within a Linux kernel. Originally designed for network packet filtering, the scope of eBPF has expanded significantly to include a wide range of functions such as performance monitoring, network traffic observation, and security-related tasks. eBPF works by allowing the insertion of user-defined, precompiled code into the kernel without the need to change kernel source code or load kernel modules, thereby promoting safety, efficiency, and scalability. By attaching eBPF programs to various hooks in the operating system we can monitor system events in real-time [2]. This capability makes eBPF an invaluable tool for performance monitoring, security, and networking.

eBPF offers several key features that make it a versatile and robust tool for system monitoring and analysis. Firstly, eBPF programs run in a secure, sandboxed environment within the kernel, minimizing the risk of crashes or security breaches. Secondly, eBPF provides high performance and efficiency, as the bytecode runs directly in the kernel, avoiding the overhead associated with user-space applications. Thirdly, eBPF is highly flexible and extensible, allowing users to write custom programs to monitor a wide range of system events. Finally, eBPF integrates seamlessly with existing kernel features and subsystems, providing deep visibility into system behavior and enabling precise, low-level monitoring (fig. 1).

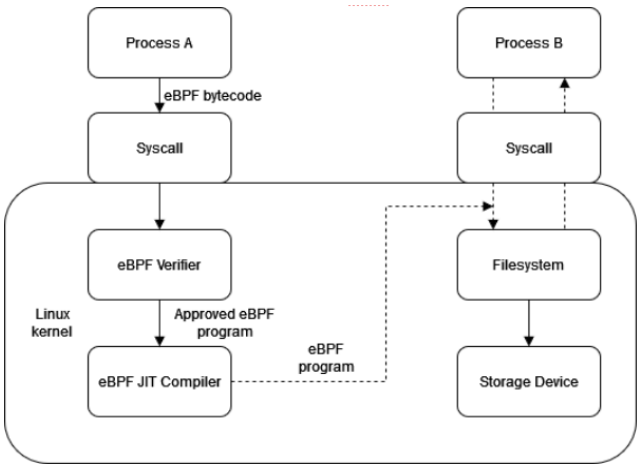

Fig. 1 Conceptual eBPF architecture diagram

eBPF can attach to various points in the kernel as shown in Figure 1, allowing it to monitor a broad spectrum of system events such as system calls, process-level events, network events, configuration changes and file system operations. When an event occurs, the eBPF program is triggered, and it can read or write data to shared data structures, which can be polled by user-space applications (in this case an agent) or put the event directly on the blockchain. This capability is particularly useful for auditing, as it enables real-time data collection directly from the kernel, providing highly granular and accurate monitoring data without significant overhead.

The application of eBPF in system event auditing provides several distinct advantages:

1. High Performance: eBPF programs run in the kernel context, which reduces context-switching overhead and allows for high-performance data capture, essential for monitoring high-velocity system events;

2. Flexibility: administrators can write and deploy custom eBPF programs tailored to specific monitoring needs without rebooting the kernel or compromising system integrity;

3. Security: given its rigorous bytecode verification process, eBPF ensures that only safe code is executed within the kernel, thereby maintaining the security and stability of the system;

4. Extensibility: eBPF's capabilities can be used to track and log virtually any type of system activity, making it an invaluable tool for comprehensive system auditing.

eBPF was chosen for system event auditing because of its unparalleled capabilities in real-time monitoring and analysis. Its ability to run custom programs within the kernel provides a level of detail and immediacy that is difficult to achieve with traditional monitoring tools. eBPF's flexibility allows it to be tailored to specific auditing requirements, enabling precise tracking of relevant system events. Additionally, the performance advantages of eBPF ensure that it can handle the high frequency and volume of system events without introducing significant overhead [4]. By integrating eBPF into the auditing framework, we can achieve a comprehensive and efficient solution for monitoring and recording system activities.

System events encompass a broad range of activities and operations that occur within computer systems, including user actions, system calls, network communications, and file accesses.

These events are generated by the operating system or by applications running on the system and can provide critical insights into the behavior and performance of the system. Auditing these events involves collecting, analyzing, and storing logs of these activities to ensure compliance, enhance securi-

ty, and facilitate forensic analysis in the case of a security incident.

Traditional system event auditing techniques generally involve centralized logging systems that collect and store logs from various system components. Common methods include syslog servers, Windows Event Logs, and proprietary logging solutions provided by security vendors. These methods focus on capturing as much information as possible, often resulting in voluminous logs that can be difficult to manage and analyze. While they provide a basic level of monitoring, they often suffer from issues such as log tampering, performance overhead, and scalability challenges in distributed environments.

Traditional auditing systems face several significant challenges:

1. Scalability: as the number of devices and the volume of logs increase, traditional systems often struggle to manage the data efficiently, leading to potential losses in logging information during high-demand periods;

2. Security: centralized logs present a single point of failure. If compromised, they can provide misleading or incorrect data, or worse, logs can be altered or deleted by attackers to cover their tracks;

3. Performance Impact: extensive logging can consume considerable system resources, affecting the overall performance of the system, especially in high-throughput environments.

These challenges underscore the need for a more robust, secure, and efficient approach to auditing system events. The next chapters will explore how the integration of blockchain and eBPF technologies addresses these issues by providing a decentralized, immutable, and highly efficient auditing framework. This innovative approach not only enhances the security and integrity of the audit process but also improves the performance and scalability of the system event auditing.

Integrating Blockchain and eBPF for Auditing

The integration of blockchain and eBPF represents a strategic convergence of two advanced technologies designed to enhance the security and efficiency of system event auditing.

The conceptual framework involves using eBPF for high-performance, real-time monitoring of system events at the kernel level, while leveraging blockchain to securely store and manage the audit logs generated by these events.

1. Data Capture: eBPF is utilized to capture system events dynamically as they occur. Custom eBPF programs can be tailored to monitor specific types of events, such as network requests, file accesses, and system calls;

2. Data Verification: once captured, data is immediately processed to ensure it adheres to predefined security policies or alert criteria. This preprocessing helps in reducing the volume of data by filtering out irrelevant information;

3. Data Recording: validated events are then formatted into transactions and recorded on a blockchain. This step leverages blockchain's immutability and transparency to ensure that once an event is logged, it cannot be altered or deleted.

The technical architecture underlying this integration involves several key components:

1. eBPF Programs: these are deployed at strategic points within the kernel to capture and preprocess system events based on specified criteria;

2. Blockchain Network: a private, permissioned blockchain is typically recommended for auditing purposes to balance transparency with access control and scalability [7];

3. Smart Contracts: deployed on the blockchain to automate the handling of logged data, including validation, storage, and retrieval processes;

4. User Interface: administrators and auditors access the system through a secure dashboard that provides real-time insights and historical data analysis capabilities.

Step-by-Step Process of the Integration:

1. Deployment of eBPF Programs: dministrators deploy custom eBPF programs designed to monitor specific system events;

2. Event Capture and Preprocessing: as events occur, eBPF programs capture and preprocess the data, filtering and formatting it for blockchain recording;

3. Transaction Creation: preprocessed events are packaged into transactions, each containing a timestamp, event data, and a unique identifier;

4. Consensus Mechanism: before being added to the blockchain, transactions must pass through the network's consensus mechanism to ensure validity and to prevent fraud;

5. Block Creation: once transactions are validated, they are grouped into blocks and linked to the existing blockchain, ensuring a tamper-proof chronological record of all system events.

Query and Audit: the blockchain can be queried through the user interface to retrieve and analyze logged events, ensuring transparency and integrity in the audit process.

This integration not only enhances the reliability and integrity of system event logs but also provides a

scalable solution that reduces the performance overhead associated with traditional auditing techniques. These programs collect event data in real-time and pass it to a logging mechanism that formats the data for blockchain storage. The formatted data is then encapsulated into a transaction and submitted to a blockchain network. The blockchain network, composed of multiple nodes, validates and records the transaction into a new block. Each block contains a cryptographic hash of the previous block, ensuring the integrity and chronological order of the audit trail. This decentralized approach eliminates the risks associated with centralized logging systems and provides a tamper-proof record of system events. The architecture is demonstrated (fig. 2).

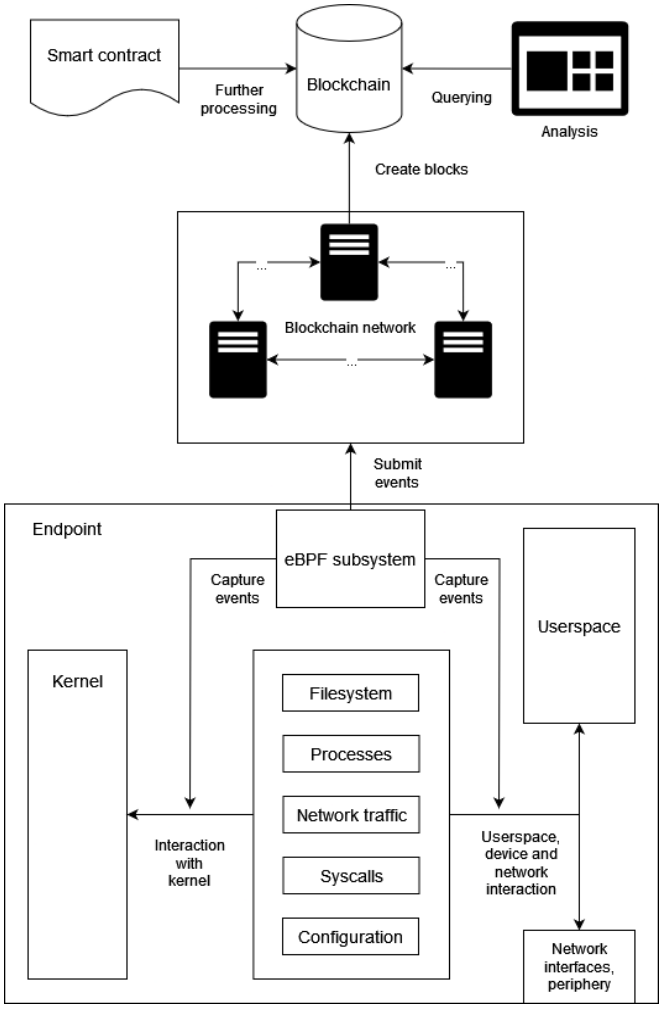

Fig. 2 Diagram of eBPF and blockchain integration

The combined use of blockchain and eBPF offers several significant advantages for system event auditing. Firstly, blockchain ensures immutability, meaning that once an event is recorded, it cannot be altered or deleted, providing a tamper-proof audit trail. This immutability is complemented by the transparency of blockchain, as its decentralized nature allows all participants to verify the recorded events, fostering trust and accountability. Additionally, eBPF's ability to operate within the kernel provides immediate insights into system activities, enabling real-time detection of anomalies and security breaches. The cryptographic techniques used in blockchain further enhance the security of the recorded data, ensuring that only authorized users can access and verify the information. Moreover, the combined approach can scale to handle large volumes of system events, making it suitable for complex and dynamic IT environments. Finally, the decentralized architecture of blockchain eliminates the risks associated with single points of failure, ensuring that the audit system remains robust and reliable even in the face of attacks or system failures.

One of the primary technical challenges in combining blockchain and eBPF for system event auditing is the complexity of initial setup and configuration. Establishing a blockchain network, particularly one that is private and secure, requires significant expertise and resources. Configuring eBPF programs to accurately and efficiently capture relevant system events also demands a deep understanding of both the Linux kernel and the specific auditing requirements. Additionally, integrating these two technologies to work seamlessly together can be technically demanding, requiring custom development and testing.

The performance impact of using eBPF and blockchain for system event auditing is another critical consideration. While eBPF operates with minimal overhead in the kernel, the process of capturing and formatting data, creating transactions, and submitting them to the blockchain can introduce latency. This latency can be exacerbated in high-frequency environments where a large number of system events are generated continuously. Ensuring that the system remains performant while providing real-time auditing capabilities is a significant challenge that requires careful optimization and tuning.

Scalability is a major concern when deploying blockchain for system event auditing, particularly in large and dynamic IT environments. The volume of system events can quickly overwhelm the blockchain network, leading to performance bottlenecks and delays in transaction processing. Traditional blockchain networks, such as those based on Bitcoin or Ethereum, may struggle to handle the high throughput required for real-time auditing. Solutions such as sharding, layer-2 protocols, or hybrid on-chain/off-chain storage mechanisms may be necessary to address these scalability challenges. To overcome these challenges, several potential solutions and areas for

future work can be explored. Optimizing eBPF programs for efficiency and minimizing the amount of data collected without sacrificing detail can help reduce the performance impact. Enhancing the performance of the blockchain network through techniques such as sharding, which partitions the blockchain into smaller, more manageable segments, can improve scalability [8]. Additionally, developing hybrid approaches that leverage both on-chain and off-chain storage can balance the need for immutability with the requirements for high throughput and low latency. Further research into advanced cryptographic methods and consensus algorithms may also yield improvements in both performance and security.

CONCLUSION AND FUTURE DIRECTIONS

This article explored the integration of blockchain and eBPF technologies to create a robust and immutable system for event auditing. Blockchain's immutability and transparency ensure that recorded events cannot be tampered with, while eBPF provides real-time monitoring capabilities within the kernel, capturing detailed system activities with minimal performance overhead. The combination of these technologies addresses the limitations of traditional auditing methods, offering a secure, scalable, and reliable solution for system event auditing.

The primary contribution of this article is the conceptual framework for integrating blockchain and eBPF to enhance system event auditing. By detailing the individual strengths of these technologies and how they can be effectively combined, the article provides valuable insights for researchers and practitioners interested in improving the reliability and security of audit systems. The discussion of challenges and potential solutions also highlights important considerations for future implementations and research in this area.

Future work can build on the foundations laid out in this article by focusing on practical implementations and further optimization of the proposed framework. Areas for future research include developing more efficient eBPF programs, improving the performance and scalability of blockchain networks, and exploring hybrid on-chain/off-chain storage solutions. Additionally, integrating advanced analytics and machine learning techniques for anomaly detection and predictive monitoring could enhance the capabilities of the auditing system. Expanding the framework to support a broader range of system events and applications, as well as investigating the use of public blockchains for wider adoption, can also increase its impact and utility.

REFERENCES

[1] Ahmad A., Saad M., Bassiouni M., Mohaisen A. (2018), "Towards blockchain-driven, secure and transparent audit logs", in Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 443-448.

[2] Deri L., Sabella S., Mainardi S., Degano P., Zunino R. (2019), "Combining System Visibility and Security Using eBPF", in ITASEC.

[3] Kumar, M., Singh, A. K. and Kumar, T. S. (2018), "Secure log storage using blockchain and cloud infrastructure", in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-4.

[4] Lim S. Y., Stelea B., Han X., Pasquier T. (2021), "Secure namespaced kernel audit for containers", in Proceedings of the ACM Symposium on Cloud Computing, pp. 518-532.

[5] Pawar A., Barthare D., Rawat N., Yadav M., Shirole M. (2021), "BlockAudit 2.0: PoA blockchain based solution for secure Audit logs", in 2021 5th International Conference on Information Systems and Computer Networks (ISCON), pp. 1-6.

[6] Regueiro C., Seco I., Gutiérrez-Agüero I., Urquizu B., Mansell J. (2021), "A blockchain-based audit trail mechanism: Design and implementation", Algorithms, Vol. 14, No. 12, pp. 341-342.

[7] Shekhtman L., Waisbard E. (2021), "Engravechain: A blockchain-based tamper-proof distributed log system", Future Internet, Vol. 13, No. 6, 143-144.

[8] Wang R., Ye K., Xu C.-Z. (2019), "Performance benchmarking and optimization for blockchain systems: A survey", in Blockchain–ICBC 2019: Second International Conference, Proceedings 2, pp. 171-185.

[9] Zhuravchak D., Tolkachova A., Piskozub A., Dudykevych V., Korshun, N. (2023), "Monitoring Ransomware with Berkeley Packet Filter", Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3550, pp. 95-106.

ВИКОРИСТАННЯ БЛОКЧЕЙНУ ТА EBPF ДЛЯ НЕЗМІННОГО АУДИТУ СИСТЕМНИХ ПОДІЙ: ПІДХІД ТЕХНОЛОГІЧНОЇ КОНВЕРГЕНЦІЇ

Важливість безпечного та надійного аудиту системних подій значно зросла в сучасних складних IT-середовищах, де цілісність даних та безпека мають першочергове значення. Традиційні методи аудиту, що базуються на централізованих системах і є вразливими до маніпуляцій та проблем з продуктивністю, більше не є достатніми. Ця стаття вирішує ці проблеми, пропонуючи нову структуру, яка поєднує технології блокчейн та eBPF для створення незмінної, прозорої та ефективної системи аудиту подій. Запропоноване рішення використовує можливості реального часу моніторингу eBPF та незмінний реєстр блокчейн

для забезпечення цілісності та перевірюваності журналів аудиту. Завдяки детальному дослідженню концептуальної структури та аналізу потенційних викликів і рішень, цей підхід довів свою ефективність у підвищенні надійності та безпеки аудиту системних подій. Результати цього дослідження надають основу для майбутніх імплементацій, досліджень та рішень для організацій, що прагнуть покращити свої процеси аудиту системних подій.

Ключові слова: аудит подій системи, блокчейн, eBPF, імутабельність, моніторинг.

Глущенко Павло Костянтинович, аспірант кафедри захисту інформації, інститут ІКТА, Національний університет Львівська Політехніка.

Pavlo Hlushchenko, Ph.D. Candidate, Information Security department, Lviv Polytechnic National University.
E-mail: pavlo.k.hlushchenko@lpnu.ua.
Orcid ID: 0000-0002-1262-5484.

Дудикевич Валерій Богданович, доктор технічних наук, професор кафедри захисту інформації, ІКТА, Національний університет Львівська Політехніка.

Valerii Dudykevych, Doctor of technical sciences, professor of Information Security department, Lviv Polytechnic National University.
E-mail: valerii.b.dudykevych@lpnu.ua.
Orcid ID: 0000-0001-8827-9920.

DOI: 10.18372/2410-7840.26.18845
УДК 004.056.5

ЗАХИЩЕНЕ ЗБЕРІГАННЯ ДАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН ETHEREUM

Олег Гарасимчук, Юрій Наконечний, Тарас Луковський, Роман Андріїв, Тарас Наконечний

Постійне збільшення обсягів даних породжує проблеми, пов'язані з вибором ефективних методів та засобів зберігання, а також забезпеченням захисту цих даних від несанкціонованого доступу. У статті детально розглянуто критичну тему збереження та захисту важливої інформації в умовах зростання обсягів даних і численності кібератак. Необхідність надійного збереження і захисту даних наростає, особливо у контексті підвищеної загрози з боку зловмисників. Висвітлюється, як блокчейн-технології, особливо на базі платформи Ethereum, можуть вирішити проблеми надійного збереження і безпеки даних. Ethereum пропонує альтернативу традиційній клієнт-серверній моделі, децентралізуючи зберігання даних за допомогою розподіленої мережі вузлів. Ця технологія значно підвищує безпеку, ускладнюючи несанкціонований доступ до інформації, оскільки для злому приватного ключа потрібні значні обчислювальні ресурси. Смарт-контракти на Ethereum дозволяють створювати застосунки, які виконуються точно відповідно до заздалегідь визначених умов, без можливості втручання третіх осіб. Це особливо важливо для месенджерів, де конфіденційність і доступність даних мають принципове значення. Вартість транзакцій в блокчейні, хоча й висока, компенсується високою надійністю та безпекою зберігання даних. Застосована методологія підтверджує, що використання публічного (децентралізованого) сховища даних є безпечним, оскільки зламати приватний ключ Ethereum практично неможливо.

***Ключові слова**: кібербезпека, зберігання даних, блокчейн, Ethereum.*

ВСТУП

У сучасному світі спостерігається стрімке збільшення обсягів інформації, що містить важливі дані [1-2]. Ця велика кількість інформації потребує систематизації за різними критеріями, а також надійного зберігання та захисту від несанкціонованого доступу. Останнім часом спостерігається зростання кількості атак на інформаційні ресурси [3-5], що підкреслює важливість постійного вдосконалення технологій кібербезпеки та розробки нових методів протидії зловмисним діям. Поруч із цим, розвиток інфраструктури для забезпечення безпеки даних стає ключовим аспектом у забезпеченні інформаційної безпеки [6-10]. Значна частина цієї інформації зберігається на серверах та у хмарах, що належать таким відомим компаніям як Amazon, Google, Apple та Facebook [11-16]. Такому способу зберігання сприяють значні переваги, оскільки згадані компанії володіють штатом кваліфікованих фахівців, які забезпечують надійне обслуговування, а також ці компанії беруть на себе основні витрати, що пов’язані з безвідмовною роботою та хостингом.

Але, незважаючи на всі зручності, є великий мінус – вразливість. Зловмисники можуть отримати небажаний доступ до файлів користувача без його ж відома, атакуючи сторонній сервіс або впливаючи на нього, тобто вони можуть вкрасти, розкрити або змінити важливу інформацію [17-18].

Методи і технології віддалених мережевих атак постійно вдосконалюються, а існуючі алго-