DOI 10.34185/1562-9945-3-158-2025-04
УДК 004.62:004.04

Р.С. Ситник, Вік.В. Гнатушенко

МЕТОД ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ТА ЦІЛІСНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ

Анотація. В умовах стрімкої цифровізації та зростання кількості кіберзагроз особливої актуальності набуває проблема захисту персональних даних у сучасних інформаційних системах. Технологія блокчейн, завдяки своїм властивостям незмінності та розподіленості, створює нові можливості для захисту даних, проте вимагає розробки спеціалізованих методів забезпечення їх достовірності та цілісності. Досліджено специфічні виклики, пов'язані з верифікацією джерел даних та контролем за їх модифікацією в умовах розподіленої системи на базі технології блокчейн. У роботі запропоновано новий метод забезпечення цілісності та достовірності персональних даних, що базується на математичній моделі оцінки достовірності даних з використанням комплексної функції валідації та концепції "довірених джерел", що дозволило підвищити рівень захищеності даних та автоматизувати процес їх верифікації . Розроблено архітектуру системи з ієрархічною структурою вузлів верифікації та механізмами управління життєвим циклом даних. Результати дослідження підтверджують ефективність запропонованого методу для забезпечення балансу між захистом персональних даних та зручністю їх використання в реальних умовах.
Ключові слова: потоки даних, інформаційні системи, блокчейн, промисловість, ланцюги постачань, Blockchain.

Постановка проблеми. В умовах стрімкої цифровізації суспільства та зростаючої кількості кіберзагроз особливої актуальності набуває питання захисту персональних даних громадян. Технологія блокчейн, завдяки своїм фундаментальним властивостям незмінності та розподіленості, представляє собою перспективний інструмент для забезпечення безпеки персональних даних. Однак, впровадження цієї технології для обробки персональних даних створює низку специфічних викликів, пов'язаних із забезпеченням їх достовірності та цілісності [1].

Особливої уваги потребує проблема верифікації джерел даних та контролю за їх модифікацією в рамках блокчейн-системи. Традиційні методи захисту інформації виявляються недостатньо ефективними через специфіку розподіленої архітектури блокчейну та особливості обробки персональних даних. Додатковим фактором ризику є необхідність забезпечення відповідності вимогам законодавства щодо захисту персональних данихта можливості внесення змін до даних за запитом суб'єкта [2].

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Існуючі рішення часто фокусуються на загальних аспектах безпеки блокчейн-систем, не враховуючи специфіку роботи з персональними даними. Це створює потребу в розробці спеціалізованих методів, які б забезпечували необхідний рівень достовірності та цілісності персональних даних при їх обробці в блокчейн-системі, одночасно відповідаючи нормативним вимогам та забезпечуючи необхідну гнучкість у керуванні даними [3].

Аналіз останніх досліджень і публікацій. В попередньому дослідженні було розглянуто методологічні засади впровадження технології блокчейн в інформаційні системи в рамках концепції "Індустрії 4.0" та запропоновано підходи до керування потоками даних у таких системах [4]. Проте питання забезпечення безпеки персональних даних у контексті блокчейн-систем потребує окремого глибокого дослідження. Внесок у розвиток цього напрямку зробили роботи, присвячені загальним принципам безпеки блокчейн-систем та особливостям їх застосування для захисту конфіденційної інформації. Особлива увага приділяється механізмам криптографічного захисту та методам верифікації даних у розподілених системах [5].

Важливим напрямком досліджень є розробка методів забезпечення відповідності блокчейн-систем вимогам законодавства про захист персональних даних. Дослідники зосереджують увагу на створенні механізмів, що дозволяють реалізувати право на забуття та можливість модифікації даних без порушення цілісності блокчейну [6]. Окремий напрямок складають роботи, присвячені розробці смарт-контрактів для управління доступом до персональних даних та автоматизації процесів їх обробки [7].

Актуальними залишаються питання інтеграції блокчейн-систем з існуючими інформаційними системами обробки персональних даних та забезпечення їх сумісної роботи. Дослідники також приділяють увагу проблемам масштабованості рішень та оптимізації продуктивності при збереженні необхідного рівня безпеки [8].

Метою дослідження є забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системі завдяки розробці нового методу на основі математичної моделі оцінки достовірності даних, що враховує комплексну функцію валідації для верифікації цифрового підпису, перевірки цілісності ланцюжка версій та валідації метаданих. Запропонований метод базується на концепції "довірених джерел" та ієрархічній структурі вузлів верифікації з алгоритмом консенсусу Proof-of-Authority, що дозволяє забезпечити високий рівень захисту при збереженні можливості контрольованої модифікації даних.

Основна частина. В сучасних умовах технологія блокчейн набуває все більшого поширення для захисту персональних даних завдяки своїм фундаментальним властивостям незмінності та розподіленості. Основними викликами при роботі з персональними даними в блокчейн-системах є забезпечення надійної верифікації джерел даних, контроль за їх модифікацією та створення ефективних механізмів валідації в умовах розподіленої архітектури. Традиційні методи захисту інформації не повністю відповідають цим вимогам через специфіку розподіленої архітектури блокчейну та особливості обробки персональних даних, що зумовлює необхідність розробки спеціалізованих рішень.

Запропонований метод базується на математичній моделі оцінки достовірності персональних даних у розподіленій блокчейн-системі, де кожен елемент даних D представляється як кортеж:

$$D = (V, S, T, H, M),$$

де V - версія даних;

S - цифровий підпис джерела;

T - часова мітка;

H - хеш попередньої версії;

M - метадані верифікації.

Достовірність даних оцінюється через комплексну функцію валідації:

$$F(D) = \alpha_1 V(S) + \alpha_2 T(H) + \alpha_3 C(M),$$

де D - набір даних, що перевіряється;

$V(S) \in [0,1]$ - функція верифікації цифрового підпису;

$T(H) \in [0,1]$- функція перевірки цілісності ланцюжка версій;

$C(M) \in [0,1]$ - функція валідації метаданих;

α_1, α_2, α_3 - вагові коефіцієнти, що визначають пріоритетність різних аспектів перевірки.

Інтегральний показник достовірності розраховується як:

$$R = F(D) \times \Pi(1 - P_i)$$

де P_i - ймовірність компрометації і-го рівня верифікації.

Кінцевий показник R знаходиться в діапазоні [0,1], де:

R = 1 означає максимальну достовірність даних;

R = 0 означає повну недостовірність даних.

В основі методу лежить концепція "довірених джерел" - спеціально авторизованих вузлів мережі, які мають право вносити та модифікувати персональні дані. Кожен такий вузол характеризується власним рівнем довіри, який динамічно оновлюється на основі історії операцій.

Архітектура системи передбачає створення ієрархічної структури вузлів верифікації, де кожен рівень відповідає за певний аспект перевірки даних. На першому рівні здійснюється базова валідація форматів даних та перевірка відповідності встановленим схемам. Другий рівень забезпечує криптографічну верифікацію цифрових підписів та перевірку повноважень джерела даних. Третій рівень реалізує складні механізми перехресної перевірки даних та їх узгодження з існуючими записами.

Важливим елементом методу є система управління життєвим циклом даних, яка забезпечує можливість контрольованої модифікації інформації при збереженні історії змін. Це досягається через впровадження спеціальних смарт-контрактів, які реалізують логіку обробки запитів на модифікацію даних та забезпечують автоматизоване виконання необхідних перевірок.

Метод також включає механізми забезпечення відповідності вимогам законодавства щодо захисту персональних даних. Це досягається через впровадження системи керування згодами на обробку даних та механізмів реалізації права на забуття. Важливою особливістю є можливість селективного видалення даних без порушення цілісності

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

блокчейну, що реалізується через механізми soft-deletion та шифрування даних з подальшим знищенням ключів.

Наукова новизна запропонованого методу полягає у розробці підходу до забезпечення достовірності та цілісності персональних даних через впровадження динамічної системи верифікації з використанням математичного апарату теорії ймовірностей та криптографічних механізмів. На відміну від існуючих рішень, метод забезпечує можливість контрольованої модифікації даних без порушення принципу незмінності блокчейну, що досягається через новий механізм версіонування та валідації змін.

Реалізація методу. Практична реалізація запропонованого методу здійснюється через розгортання спеціалізованої блокчейн-системи, що використовує модифікований алгоритм консенсусу Proof-of-Authority (PoA) з додатковими механізмами верифікації для роботи з персональними даними.

Архітектура системи складається з наступних ключових компонентів:

1. Мережевий рівень:
- Модифікований протокол консенсусу PoA з підтримкою багаторівневої верифікації
- Система динамічного розподілу навантаження між вузлами
- Механізми синхронізації стану з підтримкою часткової реплікації
2. Рівень смарт-контрактів:
- Контракти управління доступом з підтримкою рольової моделі
- Контракти версіонування даних та управління життєвим циклом
- Контракти аудиту та моніторингу операцій
3. Рівень додатків:
- API для інтеграції з зовнішніми системами
- Інтерфейси адміністрування та моніторингу
- Модулі генерації звітності та аналітики

Технічна реалізація системи включає впровадження наступних інноваційних механізмів:

Ключовим елементом реалізації є система смарт-контрактів, які забезпечують автоматизацію процесів верифікації та управління даними. Контракти реалізують складну логіку перевірок та валідації, включаючи механізми крос-валідації даних між різними джерелами. Особлива увага приділяється оптимізації продуктивності та забезпеченню масштабованості рішення.

Система включає спеціалізовані компоненти для роботи з різними типами персональних даних, враховуючи їх специфіку та вимоги до захисту. Ключовими технічними інноваціями є:

1. Механізм версіонування даних з використанням системи контролю версій на основі деревовидної структури даних. Така структура дозволяє зберігати повну історію змін та забезпечує можливість відстеження всіх модифікацій персональних даних. На відміну від простого ланцюжка блоків, деревовидна структура дозволяє підтримувати паралельні гілки змін та їх подальше об'єднання, що важливо при роботі з персональ-

ними даними в розподіленому середовищі. Кожна версія даних зберігається як окремий вузол дерева з наступною структурою:

```
Version = {
id: UUID,
data: EncryptedData,
parentVersion: Hash,
timestamp: Integer,
signature: Signature,
metadata: {
validatorSet: [NodeID],
trustScore: Float,
validationProof: Hash
    }
}
```

2. Алгоритм псевдокоду розподіленого консенсусу з підтримкою валідації персональних даних:

```
ValidationConsensus(data) {
validators = SelectValidators(data.type)
validationResults = []
forvalidatorinvalidators {
result = validator.Validate(data)
validationResults.append(result)
    }
consensusReached = CalculateConsensus(validationResults)
returnconsensusReached
}
```

3. Система керування доступом на основі розширеної рольової моделі, яка враховує не тільки ролі користувачів, але й додаткові атрибути та контекст операцій. Така модель дозволяє реалізувати гнучкі політики доступу, що враховують різні параметри: роль користувача, тип даних, час доступу, місце доступу, історію операцій тощо. Правила доступу описуються наступною структурою:

```
PolicyRule = {
userRole: String, // Роль користувача (адміністратор, оператор, аудитор)
dataType: String, // Тип персональних даних
operation: String, // Тип операції (читання, запис, модифікація)
timeRestrictions: { // Часові обмеження доступу
allowedHours: [Int], // Дозволені години доступу
allowedDays: [String]  // Дозволені дні тижня
    },
locationRestrictions: { // Географічні обмеження
allowedIPs: [String],  // Дозволені IP-адреси
allowedRegions: [String] // Дозволені регіони
    },
```


ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Механізми диференційованого доступу та контролю за використанням даних через систему смарт-контрактів, що забезпечує автоматичну валідацію прав доступу, аудит всіх операцій з даними, контроль за дотриманням політик безпеки та. автоматичне виконання процедур відкликання доступу

Висновки. Запропонований у роботі метод забезпечення достовірності та цілісності персональних даних у блокчейн-системі представляє собою комплексне рішення, що враховує як технічні аспекти захисту інформації, так і нормативні вимоги до обробки персональних даних. Важливою перевагою є можливість забезпечення балансу між захистом даних та зручністю їх використання, що досягається через впровадження гнучких механізмів, таких як система керування доступом на основі розширеної рольової моделі, смарт-контрактів для автоматизації процесів верифікації даних та механізми диференційованого доступу з контролем за використанням даних.

Подальший розвиток методу передбачає вдосконалення механізмів автоматизації процесів верифікації, практичної реалізації та впровадження та розширення можливостей інтеграції з різними інформаційними системами: включаючи корпоративні бази даних, системи електронного документообігу та державні реєстри, у яких можна впровадити використання технології блокчейн. Планується також розробка додаткових інструментів аналізу та моніторингу для підвищення ефективності виявлення потенційних загроз та забезпечення превентивного захисту даних.

ЛІТЕРАТУРА

1. G. Zyskind, O. Nathan. 2015. Decentralizing privacy: Using blockchain to protect personal data. IEEE security and privacy workshops (pp. 180-184). IEEE. DOI: 10.1109/SPW.2015.27.

2. U.Tatar, Y.Gokce, B. Nussbaum. 2020. Law versus technology: Blockchain, GDPR, and tough trade-offs. Computer Law & Security Review, 38. DOI: 10.1016/j.clsr.2020.105454.

3. A.B. Haque, A. N. Islam, S. Hyrynsalmi, B. Naqvi, K.Smolander. 2021. GDPR compliant blockchains–a systematic literature review. Ieee Access, 9. DOI: 10.1109/ACCESS.2021.3069877

4. R. Sytnyk, Vik. Hnatushenko. "DATA FLOW MANAGEMENT IN INFORMATION SYSTEMS USING BLOCKCHAIN TECHNOLOGY." Scientific Bulletin of National Mining University 3 (2024). DOI: 10.33271/nvngu/2024-3/142.

5. R. Zhang, R. Xue, L. Liu. 2019. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), pp.1-34. DOI: 10.1145/3316481.

6. Truong, N.B., Sun, K., Lee, G.M. and Guo, Y., 2019. GDPR-compliant personal data management: A blockchain-basedsolution. IEEE Transactions on Information Forensics and Security, 15, pp.1746-1761. DOI: 10.1109/TIFS.2019.2948287.

7. Kushwaha, S.S., Joshi, S., Singh, D., Kaur, M. and Lee, H.N., 2022. Systematic review of security vulnerabilities in Ethereum blockchain smart contract. IEEE Access, 10, pp.6605-6621. DOI: DOI:10.1109/ACCESS.2021.3140091.

8. Mourtzis, D., Angelopoulos, J. and Panopoulos, N., 2023. Blockchain integration in the era of industrial metaverse. Applied Sciences, 13(3), p.1353. DOI: 10.3390/app13031353.

REFERENCE

1. G. Zyskind, O. Nathan. 2015. Decentralizing privacy: Using blockchain to protect personal data. IEEE security and privacy workshops (pp. 180-184). IEEE. DOI: 10.1109/SPW.2015.27.

2. U.Tatar, Y.Gokce, B. Nussbaum. 2020. Law versus technology: Blockchain, GDPR, and tough trade-offs. Computer Law & Security Review, 38. DOI: 10.1016/j.clsr.2020.105454.

3. A.B. Haque, A. N. Islam, S. Hyrynsalmi, B. Naqvi, K.Smolander. 2021. GDPR compliant blockchains–a systematic literature review. Ieee Access, 9. DOI: 10.1109/ACCESS.2021.3069877

4. R. Sytnyk, Vik. Hnatushenko. "DATA FLOW MANAGEMENT IN INFORMATION SYSTEMS USING BLOCKCHAIN TECHNOLOGY." Scientific Bulletin of National Mining University 3 (2024). DOI: 10.33271/nvngu/2024-3/142.

5. R. Zhang, R. Xue, L. Liu. 2019. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), pp.1-34. DOI: 10.1145/3316481.

6. Truong, N.B., Sun, K., Lee, G.M. and Guo, Y., 2019. GDPR-compliant personal data management: A blockchain-basedsolution. IEEE Transactions on Information Forensics and Security, 15, pp.1746-1761. DOI: 10.1109/TIFS.2019.2948287.

7. Kushwaha, S.S., Joshi, S., Singh, D., Kaur, M. and Lee, H.N., 2022. Systematic review of security vulnerabilities in Ethereum blockchain smart contract. IEEE Access, 10, pp.6605-6621. DOI: DOI:10.1109/ACCESS.2021.3140091.

8. Mourtzis, D., Angelopoulos, J. and Panopoulos, N., 2023. Blockchain integration in the era of industrial metaverse. Applied Sciences, 13(3), p.1353. DOI: 10.3390/app13031353.

Received 31.03.2025.
Accepted 01.04.2025.

Method for ensuring the reliability and integrity of personal data processed in a blockchain system

Recent research and publications. Blockchain technology has shown significant potential for securing personal data through its fundamental properties of immutability and distribution. However, existing solutions often focus on general blockchain security aspects without considering the specifics of personal data processing and compliance requirements.

The aim of the study. Development of a specialized method for ensuring the reliability and integrity of personal data in blockchain systems while maintaining compliance with data protection regulations and enabling controlled data modification.

Main material of the study. The paper presents amethod based on a mathematical model for data reliability assessment using a complex validation function and the concept of "trusted sources". Conclusions. The designed method provides a comprehensive solution that balances technical security aspects with regulatory requirements for personal data processing.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Гнатушенко Вікторія Володимирівна – доктор технічних наук, професор, завідувач кафедри інформаційних технологій і систем Українського державного університету науки і технології.

Ситник Роман Сергійович – аспірант кафедри інформаційних технологій і систем Українського державного університету науки і технології.

Hnatushenko Viktoriia – Doctor of engineering's sciences, Professor, Head of Department of Information Technologies and Systems, Ukrainian State University of Science and Technology.

Sytnyk Roman – Postgraduate Student, Department of Information Technologies and Systems, Ukrainian State University of Science and Technology.