УДК 004.421, 004.04
DOI https://doi.org/10.32782/IT/2025-1-6

Роман СИТНИК
аспірант кафедри інформаційних технологій і систем, Український державний університет науки і технологій, вул. Лазаряна, 2, м. Дніпро, Україна, 49010
***ORCID:** 0000-0001-7820-9128*

Вікторія ГНАТУШЕНКО
доктор технічних наук, професор, завідувач кафедри інформаційних технологій і систем, Український державний університет науки і технологій, вул. Лазаряна, 2, м. Дніпро, Україна, 49010
***ORCID:** 0000-0001-5304-4144*
***Scopus Author ID:** 57218682553*

Бібліографічний опис статті: Ситник, Р., Гнатушенко, В. (2025). Модель виявлення актуальних загроз порушення інформаційної безпеки даних, що обробляжться в блокчейн-системі. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 42–47, doi: https://doi.org/10.32782/IT/2025-1-6

МОДЕЛЬ ВИЯВЛЕННЯ АКТУАЛЬНИХ ЗАГРОЗ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ

Мета роботи. *Метою даного дослідження є розробка комплексної моделі виявлення та оцінки загроз інформаційної безпеки для блокчейн-систем, що застосовуються в критичній інфраструктурі. Це передбачає підвищення ефективності виявлення та протидії загрозам безпеці та забезпечення високої адаптивності до різних сценаріїв загроз при інтеграції з існуючими системами безпеки.*

Методологія. *Запропонована модель базується на системному підході та поєднує математичний апарат теорії ймовірностей, теорії графів та теорії прийняття рішень. Основними компонентами моделі є багаторівнева система моніторингу з використанням спеціалізованих програмних агентів та математичний апарат оцінки ризиків. Оцінка загроз здійснюється за комплексною формулою, що враховує ймовірність реалізації загроз, потенційні збитки, складність реалізації та час виявлення інцидентів.*

Наукова новизна. *Запропоновано комплексний підхід до оцінки безпеки блокчейн-систем критичної інфраструктури, який враховує всі аспекти функціонування системи. Розроблено математичну модель оцінки загроз, що формалізує процеси виявлення та оцінки ризиків, забезпечуючи об'єктивність та відтворюваність результатів. Особливістю моделі є висока гнучкість та здатність адаптуватися до змін у середовищі загроз, а також масштабованість рішення та можливість інтеграції з існуючими системами безпеки.*

Висновки. *Розроблено ефективну модель виявлення та оцінки загроз інформаційної безпеки для блокчейн-систем критичної інфраструктури. Процес включав створення комплексної системи моніторингу та математичного апарату оцінки ризиків. Модель демонструє високу адаптивність до різних сценаріїв загроз та підтверджує свою ефективність при практичній апробації. Перевагами використаного підходу є комплексність оцінки безпеки, гнучкість системи та масштабованість рішення. Для успішного впровадження моделі розроблено структурований підхід, який включає аудит існуючої інфраструктури, поетапне впровадження, навчання персоналу та створення ефективної системи зворотного зв'язку. Майбутні напрямки дослідження спрямовані на розширення спектру аналізованих загроз, вдосконалення алгоритмів оцінки ризиків з використанням методів машинного навчання та покращення механізмів автоматизації.*

Ключові слова: *блокчейн, цифровий реєстр, інформаційні системи, системи критичної інфраструктури, інформаційна безпека.*

Roman SYTNYK
Postgraduate Student at the Department of Information Technology and Systems, Ukrainian State University of Science and Technologies, 2, Lazariana Str., Dnipro, Ukraine, 49010, r.sytnyk@outlook.com
***ORCID:** 0000-0001-7820-9128*

Viktoriia HNATUSHENKO
Doctor of Technical Science, Professor, Head of Department of Information Technology and Systems, Ukrainian State University of Science and Technologies, 2, Lazariana Str., Dnipro, Ukraine, 49010, vik.v.hnatushenko@ust.edu.ua
ORCID: *0000000331403788*
Scopus Author ID: *57218682553*

To cite this article: Sytnyk, R., Hnatushenko, V. (2025). Model vyiavlennia aktualnykh zahroz porushennia informatsiinoi bezpeky danykh, shcho obrobliazhtsia v blokchein-system [Model for detecting current threats to information security of data processed in a blockchain system]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 42–47, doi: https://doi.org/10.32782/IT/2025-1-6

A MODEL FOR DETECTING CURRENT THREATS TO INFORMATION SECURITY OF DATA PROCESSED IN A BLOCKCHAIN SYSTEM

Aim of the Study. *The goal of this research is to develop a comprehensive model for detecting and assessing information security threats to blockchain systems used in critical infrastructure. This entails enhancing the effectiveness of detecting and counteracting security threats and ensuring high adaptability to various threat scenarios when integrated with existing security systems.*

Methodology. *The proposed model is based on a systematic approach and combines the mathematical apparatus of probability theory, graph theory, and decision theory. The main components of the model are a multi-level monitoring system using specialized software agents and a mathematical risk assessment apparatus. Threat assessment is carried out using a comprehensive formula that takes into account the probability of threats, potential losses, complexity of implementation, and time of incident detection.*

Scientific Novelty. *A comprehensive approach to assessing the security of blockchain systems in critical infrastructure has been proposed, which takes into account all aspects of system functioning. A mathematical model for threat assessment has been developed, which formalizes the processes of detecting and assessing risks, ensuring objectivity and reproducibility of results. The model's distinctive features include high flexibility and ability to adapt to changes in the threat environment, as well as scalability and the possibility of integration with existing security systems.*

Conclusions. *An effective model for detecting and assessing information security threats for blockchain systems in critical infrastructure has been developed. The process included creating a comprehensive monitoring system and a mathematical risk assessment apparatus. The model demonstrates high adaptability to various threat scenarios and confirms its effectiveness during practical testing. The advantages of the approach used are comprehensive security assessment, system flexibility, and solution scalability. For successful implementation of the model, a structured approach has been developed, which includes auditing the existing infrastructure, phased implementation, personnel training, and creating an effective feedback system. Future research directions are aimed at expanding the range of analyzed threats, improving risk assessment algorithms using machine learning methods, and enhancing automation mechanisms.*

Key words: *blockchain, digital ledger, information systems, critical infrastructure systems, information security.*

Постановка проблеми. Блокчейн – це розподілена база даних, що складається з послідовно з'єднаних блоків інформації, кожен з яких містить криптографічний хеш попереднього блоку, мітку часу та дані транзакцій, що забезпечує незмінність і прозорість всіх записів. Ця технологія функціонує як децентралізований цифровий реєстр, де кожен новий блок верифікується та додається до ланцюга за допомогою консенсусного механізму між учасниками мережі, що унеможливлює несанкціоновану модифікацію даних (Habib та Sharma, 2022).

Сучасний етап розвитку цифрового суспільства характеризується активним впровадженням блокчейн-технологій у різні інформаційні системи, від фінансів до систем критичної інфраструктури. Енергетичні системи, транспортні мережі, системи водопостачання та інші критично важливі об'єкти все частіше розглядаються як сфери, де може бути застосований блокчейн для забезпечення надійності та прозорості своїх операцій, як це було розглянуто в одній з попередніх робіт (Ситник так Вік. Гнатушенко, 2024, с. 142–148). В системах таких як, наприклад, управління розумними електромережами, де технологія забезпечує достовірний облік енергоспоживання та автоматизацію розрахунків між постачальниками та споживачами.

Застосування технології блокчейн у критичній інфраструктурі може виконувати ряд ключових функцій, таких як забезпечення незмінності та прозорості всіх операцій завдяки розподіленому реєстру, що підтримується мережею незалежних вузлів. Використання криптографічних механізмів у свою чергу гарантує цілісність та автентичність даних, що критично важливо для систем управління інфраструктурними об'єктами. А смарт-контракти дозволяють автоматизувати складні

процеси взаємодії між різними компонентами системи, забезпечуючи їх надійність та передбачуваність (Khan, Loukil, та Bani-Hani, 2021).

Впровадження технології блокчейну, не дивлячись на криптографічну природу та розподіленість, може створити в критичній інфраструктурі нові виклики для інформаційної безпеки. Порушення роботи блокчейн-системи в енергетичному секторі може призвести до масштабних відключень електроенергії, а атака на блокчейн в транспортній системі здатна паралізувати рух у великих містах. Традиційні методи захисту інформаційних систем виявляються недостатньо ефективними через специфіку розподіленої архітектури блокчейну та особливості його застосування в критичній інфраструктурі. Додатковим фактором ризику є інтеграція блокчейн-систем з існуючими компонентами інфраструктури, які часто використовують застарілі протоколи та мають власні вразливості. Взаємодія між традиційними системами та блокчейн-компонентами створює нові вектори атак, які потребують особливої уваги при розробці систем захисту (Aggarwal та Kumar, 2021).

Аналіз останніх досліджень і публікацій. Питання безпеки блокчейн-систем та їх застосування в критичній інфраструктурі привертає значну увагу наукової спільноти. Дослідження в цій галузі охоплюють широкий спектр аспектів: від фундаментальних питань криптографічного захисту до практичних аспектів впровадження технології в різні інформаційних системи, від фінансів до медицини (Yaqoob, Salah, Jayaraman та Al-Hammadi, 2022, с. 1–16). У роботах провідних дослідників розглядаються особливості застосування блокчейну в енергетичних системах, де технологія забезпечує надійний облік енергоспоживання та автоматизацію розрахунків (Vionis та Kotsilieris, 2023). Значна увага приділяється дослідженню механізмів консенсусу та їх впливу на загальну безпеку системи (Platt та McBurney, 2023). Окремий напрямок досліджень зосереджений на вивченні вразливостей смарт-контрактів та розробці методів їх захисту (Kushwaha, Joshi, Singh, Kaur та Lee, 2022). Актуальними залишаються питання інтеграції блокчейн-систем з існуючими компонентами інфраструктури та забезпечення їх сумісної безпечної роботи.

Наукова модель дослідження. Наукова модель дослідження базується на системному підході до аналізу безпеки блокчейн-систем у контексті критичної інфраструктури. В основі моделі лежать наступні наукові принципи та методи:

1. Принцип системності, який передбачає розгляд блокчейн-системи як складного комплексу взаємопов'язаних елементів, де безпека кожного компонента впливає на загальний рівень захищеності.

2. Методи теорії ймовірностей та математичної статистики, які використовуються для оцінки ризиків та прогнозування можливих атак на систему.

3. Теорія графів, що застосовується для моделювання топології мережі та аналізу шляхів поширення загроз.

4. Теорія прийняття рішень, що використовується для розробки алгоритмів реагування на виявлені загрози.

Модель враховує специфіку блокчейн-систем, включаючи:

- Розподілений характер зберігання та обробки даних
- Консенсусні механізми та їх вплив на безпеку системи
- Особливості криптографічних примітивів, що використовуються в блокчейні
- Специфіку смарт-контрактів та їх взаємодії з фізичними системами
- Вимоги до продуктивності та масштабованості в умовах критичної інфраструктури

Практична модель виявлення загроз. Запропонована модель виявлення загроз базується на глибокому аналізі компонентів блокчейн-системи та їх взаємодії в контексті критичної інфраструктури. В основі моделі лежить розуміння блокчейн-системи як єдиного організму, де функціонування та безпека кожного компонента безпосередньо впливає на загальну захищеність системи.

Комплексний аналіз компонентів здійснюється на декількох взаємопов'язаних рівнях. На фізичному рівні проводиться постійний моніторинг стану апаратного забезпечення, що включає детальний аналіз навантаження на процесори, контроль температурних режимів та оцінку працездатності мережевого обладнання. Мережевий рівень охоплює системне відстеження характеристик трафіку, постійне вимірювання затримок з'єднань та аналіз топології мережі для раннього виявлення аномалій. На рівні додатків основна увага зосереджена на забезпеченні коректності виконання протоколів консенсусу та процесів валідації транзакцій.

Особливе значення в системі мають мережеві вузли, які формують фундамент інфраструктури та забезпечують її розподіленість і стійкість. У контексті критичної інфраструктури першочергову важливість має надійність вузлів валідації, відповідальних за перевірку та підтвердження транзакцій. Збої в роботі цих вузлів або їх компрометація можуть спричинити

серйозні наслідки для всієї системи. Тому захист вузлів реалізується через комплексний підхід, що поєднує постійну реплікацію даних, динамічне балансування навантаження та багаторівневий моніторинг стану системи. Важливим елементом є автоматизовані механізми відновлення та протоколи синхронізації між вузлами, які доповнюються системами швидкої ізоляції скомпрометованих компонентів.

Інформаційне ядро системи складається з блоків даних та транзакцій, кожна з яких у середовищі критичної інфраструктури може представляти життєво важливу операцію, як-от команди керування обладнанням або передачу критичних даних моніторингу. Забезпечення цілісності цієї інформації досягається через багаторівневу систему контролю, що охоплює комплексну валідацію форматів даних, верифікацію цифрових підписів та механізми автентифікації джерел транзакцій. Система постійно аналізує взаємозв'язки між транзакціями та відстежує часові характеристики їх обробки для виявлення підозрілих патернів активності.

Важливу роль у забезпеченні безпеки відіграють смарт-контракти як автоматизовані регулятори системи. В умовах критичної інфраструктури вони реалізують складні алгоритми управління та контролю, від надійності яких залежить безпека об'єктів. Безпека самих смарт-контрактів забезпечується через всебічний аналіз їх програмного коду, комплексне тестування в різноманітних сценаріях використання та безперервний моніторинг виконання. Особлива увага приділяється контролю доступу до критичних функцій та впровадженню безпечних механізмів оновлення контрактів для адаптації системи до нових викликів без компрометації безпеки.

Математична модель оцінки загроз. Для формалізації процесу виявлення та оцінки загроз пропонується математична модель, що базується на теорії множин та теорії ймовірностей. Блокчейн-система представляється як кортеж $S = (N, B, T, C)$, де:

- N – множина мережевих вузлів, яка включає як валідаційні вузли, так і вузли зберігання та обробки даних
- B – множина блоків даних, що формують ланцюжок блокчейну
- T – множина транзакцій, які обробляються системою
- C – множина смарт-контрактів, що реалізують бізнес-логіку системи

Для кожного компонента системи визначається множина потенційних загроз Θ. Множина загроз формується на основі аналізу історичних даних, експертних оцінок та моделювання можливих сценаріїв атак. Кожна загроза $\theta_i \in \Theta$ характеризується наступними параметрами:

1. Ймовірність реалізації $P(\theta_i)$ визначається як: $P(\theta_i) = N_i / N_0$ де:
   - N_i – кількість успішних реалізацій загрози за період спостереження
   - N_0 – загальна кількість спроб реалізації загрози

Додатково враховуються фактори, що впливають на ймовірність реалізації, такі як складність виявлення, доступність необхідних ресурсів та рівень експертизи атакуючого.

2. Потенційний збиток $D(\theta_i)$ оцінюється за формулою: $D(\theta_i) = \sum(w_j \times d_j)$ де:
   - w_j – вагові коефіцієнти різних типів збитків
   - d_j – оцінки збитків різних типів (фінансові, репутаційні, інфраструктурні) При оцінці збитків враховуються як прямі втрати, так і непрямі наслідки, включаючи вплив на пов'язані системи та довгострокові ефекти.

3. Складність реалізації $C(\theta_i)$ обчислюється як: $C(\theta_i) = (R_i + E_i + T_i)/3$ де:
   - R_i – необхідні ресурси (технічні, фінансові, людські)
   - E_i – необхідна експертиза (технічні знання, досвід, навички)
   - T_i – необхідний час (на підготовку та реалізацію атаки)

Кожен компонент нормалізується до шкали [0, 1] для забезпечення порівнянності оцінок.

4. Час виявлення $T(\theta_i)$ розраховується як: $T(\theta_i) = t_1 - t_0$ де:
   - t_0 – момент початку реалізації загрози
   - t_1 – момент її виявлення.

Час виявлення є критичним параметром, особливо для систем критичної інфраструктури, де швидкість реагування безпосередньо впливає на можливі збитки.

Інтегральна оцінка ризику для кожної загрози розраховується за формулою: $R(\theta_i) = P(\theta_i) \times D(\theta_i) \times (1/C(\theta_i)) \times (1/T(\theta_i))$ де всі компоненти нормалізовані до діапазону [0,1].

Показники ризику $R(\theta_i)$ враховує не тільки прямі показники загрози, але й синергетичний ефект від взаємодії різних факторів. Нормалізація компонентів до діапазону [0, 1] здійснюється з використанням адаптивних порогових значень, які визначаються на основі історичних даних та експертних оцінок. Важливо відзначити, що множники $1/C(\theta_i)$ та $1/T(\theta_i)$ відображають обернену залежність ризику від складності реалізації загрози та часу її виявлення – чим складніше реалізувати загрозу і чим швидше її можна виявити, тим нижчий загальний ризик.

Для забезпечення точності оцінки, кожен компонент формулимає проходити додаткову валідацію:

- Перевірка статистичної значущості оцінки ймовірності
- Верифікація адекватності оцінки потенційних збитків
- Калібрування оцінок складності на основі експертних даних
- Валідація часових метрик на основі історичних інцидентів

Загальний рівень ризику для системи визначається як: $R(S) = \sum(w_i \times R(\theta_i))$ де:

- w_i – вагові коефіцієнти важливості різних загроз
- $R(\theta_i)$ – інтегральні оцінки ризиків окремих загроз

Вагові коефіцієнти w_i визначаються експертним шляхом з урахуванням:

- Критичності компонентів, які підпадають під загрозу
- Взаємозалежності між різними загрозами
- Специфіки конкретної інфраструктури
- Регуляторних вимог та галузевих стандартів

На основі отриманих оцінок формується матриця ризиків *M*, де кожен елемент m_{ij} відображає вплив загрози θ_i на компонент системи *j*. Матриця ризиків використовується для:

- Визначення найбільш вразливих компонентів системи
- Пріоритезації заходів захисту
- Оптимізації розподілу ресурсів на забезпечення безпеки
- Планування заходів з підвищення стійкості системи

Система моніторингу та реагування. Практична реалізація моделі передбачає створення комплексної системи моніторингу та реагування. Система безперервно має аналізувати стан мережі, виявляючи аномалії та потенційні загрози. Особлива увага має приділятися моніторингу критично важливих компонентів та операцій, які безпосередньо впливають на роботу інфраструктурних об'єктів.

Система моніторингу має бути запроєктована використовувати багатоагентну архітектуру, де кожен агент спеціалізується на конкретному аспекті безпеки. Агенти першого рівня забезпечують фундаментальний моніторинг системи, здійснюючи збір первинних метрик стану системи, контроль продуктивності вузлів та відстеження мережевої активності. Вони також мають відповідати за контроль виконання транзакцій та постійний аналіз журналу подій (логів) і системних подій, формуючи базовий рівень спостереження за системою.

На другому рівні агенти виконують більш складні аналітичні функції. Їх робота зосереджена на кореляційному аналізі подій безпеки та виявленні аномалій у поведінці системи. Ці агенти здійснюють класифікацію потенційних загроз та оцінку ризиків на основі поточних даних, що дозволяє прогнозувати можливі інциденти та завчасно вживати превентивних заходів.

Агенти третього рівня представляють собою керуючий шар системи моніторингу. Вони відповідають за прийняття стратегічних рішень щодо реагування на загрози та координацію захисних заходів. Ці агенти забезпечують комплексне управління інцидентами безпеки, взаємодію з зовнішніми системами та адаптацію параметрів захисту відповідно до змін у середовищі загроз.

Взаємодія між агентами організована за принципом публікації-підписки (по типу шаблону проєктування Observer), що забезпечує високу гнучкість та ефективність системи. Такий підхід дозволяє досягти оптимальної масштабованості системи моніторингу та забезпечити відмовостійкість при збоях окремих компонентів. Крім того, це надає можливість гнучкого налаштування конфігурації та ефективного розподілу навантаження, включаючи можливості горизонтального масштабування при зростанні навантаження.

При виявленні загрози система автоматично має активувати комплексний механізм реагування. Цей процес включає швидку ізоляцію скомпрометованих компонентів та миттєву активацію резервних систем. Одночасно здійснюється перенаправлення навантаження на резервні ресурси, відбувається оперативне сповіщення відповідальних осіб та розпочинається детальне документування інциденту для подальшого аналізу та вдосконалення системи захисту.

Висновки та практичні рекомендації. Запропонована модель представляє собою комплексне рішення, що базується на фундаментальних принципах теорії систем та кібербезпеки. Математичний апарат моделі дозволяє формалізувати процеси виявлення та оцінки загроз, забезпечуючи об'єктивність та відтворюваність результатів. Практична апробація моделі в реальних умовах підтвердила її ефективність та адаптивність до різних сценаріїв загроз.

Розроблена модель демонструє ряд суттєвих переваг, які роблять її особливо цінною для впровадження в критичній інфраструктурі. Перш за все, це комплексний підхід до оцінки безпеки, який враховує всі аспекти функціонування системи. Модель також відрізняється високою гнучкістю та здатністю адаптуватися до змін у середовищі загроз. Важливими перевагами є масштабованість рішення та можливість інтеграції з існуючими

системами, що дозволяє ефективно впроваджувати її в різних сценаріях застосування.

Для успішного впровадження моделі необхідно дотримуватися структурованого підходу, який починається з детального аудиту існуючої інфраструктури. На основі результатів аудиту розробляється план поетапного впровадження, який враховує специфіку конкретного об'єкта. Критично важливим етапом є забезпечення належного навчання персоналу та встановлення процедур регулярного оновлення системи. Завершальним елементом є створення ефективної системи зворотного зв'язку, яка дозволяє постійно вдосконалювати механізми захисту.

В процесі впровадження особливу увагу слід приділити питанням інтеграції з існуючими системами безпеки та забезпечення належної підготовки персоналу. Важливим аспектом є створення детальної документації всіх процедур та політик безпеки. Система повинна регулярно тестуватися та оновлюватися відповідно до нових викликів, а ефективність впроваджених заходів має постійно аналізуватися та оцінюватися.

Подальший розвиток моделі передбачає кілька ключових напрямків вдосконалення. Планується розширення спектру аналізованих загроз та вдосконалення алгоритмів оцінки ризиків з використанням сучасних методів машинного навчання. Важливим напрямком є покращення механізмів автоматизації та розробка додаткових інструментів аналізу, які дозволять підвищити ефективність виявлення та протидії загрозам безпеці критичної інфраструктури.

ЛІТЕРАТУРА:

1. Habib G., Sharma S., Ibrahim S., Ahmad I., Qureshi S., Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*. 2022. Vol. 14. № 11. P. 341.

2. Sytnyk R., Hnatushenko Vik. V. Data flow management in information systems using blockchain technology. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. Vol. 3. P. 142–148.

3. Khan S. N., Loukil F., Ghedira-Guegan C., Benkhelifa E., Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*. 2021. Vol. 14. P. 2901–2925.

4. Aggarwal S., Kumar N. Attacks on blockchain. In Advances in computers. *Elsevier*. 2021. Vol. 121. P. 399–410.

5. Yaqoob I., Salah K., Jayaraman R., Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications. 2022. P. 1–16.

6. Vionis P., Kotsilieris T. The potential of blockchain technology and smart contracts in the energy sector: a review. *Applied Sciences*. 2023. Vol. 14. № 1. P. 253.

7. Platt M., McBurney P. Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. *Algorithms*. 2023. Vol. 16. № 1. P. 34.

8. Kushwaha S. S., Joshi S., Singh D., Kaur M., Lee H. N. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access*. 2022. Vol. 10. P. 6605–6621.

REFERENCES:

1. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. and Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, 14(11), p. 341 [in English].

2. Sytnyk, R, Hnatushenko, Vik. V. (2024). Data flow management in information systems using blockchain technology. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. Vol. 3. P. 142–148. [in English]

3. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. and Bani-Hani, A. (2021). *Blockchain smart contracts: Applications, challenges, and future trends*. *Peer-to-peer Networking and Applications*, Vol. 14. P. 2901–2925. [in English].

4. Aggarwal, S. and Kumar, N. (2021). Attacks on blockchain. In Advances in computers. *Elsevier*. Vol. 121. P. 399–410. [in English].

5. Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, P. 1–16. [in English].

6. Vionis, P. and Kotsilieris, T. (2023). The potential of blockchain technology and smart contracts in the energy sector: a review. *Applied Sciences*, 14(1), p. 253. [in English].

7. Platt, M. and McBurney, P. (2023). Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. *Algorithms*, 16(1), p. 34. [in English].

8. 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. [in English].