https://doi.org/10.31891/2219-9365-2025-81-35
УДК 004.75

РЕГІДА Павло
Хмельницький національний університет
https://orcid.org/0000-0002-6591-7069
email: pavlo.rehida@gmail.com

# ПОВЕДІНКОВА МОДЕЛЬ ДОВІРИ В ГРІД ОБЧИСЛЮВАЛЬНІЙ СИСТЕМІ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

*Цю роботу присвячено дослідженню можливостей застосування нечіткої логіки для побудови та вдосконалення моделі довіри до обчислювальних елементів у грід-обчислювальних системах. Такі системи набули значного поширення завдяки своїй гнучкості, простоті масштабування та здатністю ефективно залучати нові вузли, що дозволяє збільшувати загальну доступну обчислювальну потужність для вирішення складних задач. Використання грід-систем успішно підтверджується численними науковими, академічними та профільними проектами, які об'єднують велику кількість користувачів, що добровільно надають власні ресурси для виконання інтенсивних, з точки зору обчислювальної складності, завдань. Проте, незважаючи на очевидні переваги, залишається актуальною і складною проблема забезпечення високого рівня захисту, надійності та достовірності результатів обчислень. Основна складність полягає у відсутності прямого контролю над програмними та апаратними компонентами обчислювальних елементів, що приєднуються до системи. Внаслідок цього виникає необхідність у додаткових повторних перевірках отриманих результатів, що неминуче призводить до підвищення навантаження на систему та зниження її загальної продуктивності. Відсутність додаткових перевірок може призвести до спотворення підсумкового результату, враховуючи специфіку виконання завдань у такому середовищі. Оскільки обчислення розподіляються на окремі частини між великою кількістю обчислювальних елементів, а отримані часткові результати об'єднуються в єдине рішення, навіть одна помилка або зловмисна дія окремого елемента здатна критично вплинути на точність загального результату. Враховуючи зазначене, метою цієї статті є представлення модифікованої моделі довіри на основі нечіткої логіки, яка дозволить правильно розподілити ролі між елементами у системі. Така модифікація дозволить скоротити кількість необхідних повторних перевірок і підвищити ефективність функціонування грід-системи загалом.*

*Ключові слова: розподілені системи, модель довіри, нечітка логіка.*

REHIDA Pavlo
Khmelnytskyi National University

# BEHAVIOUR-BASED TRUST MODEL IN A GRID COMPUTING SYSTEM BASED ON FUZZY LOGIC

*This paper is dedicated to exploring the application fuzzy logic for the development and improvement of a trust model for computational elements in grid computing systems. Such systems have gained significant popularity due to their flexibility, scalability and ability to efficiency incorporate new nodes, thereby increasing overall computational power available for solving complex problems. The effectiveness of grid systems has been successfully demonstrated through numerous scientific, academic and domain-specific projects that involve a large number of users voluntarily contributing their own resources to perform computationally intensive tasks. However, despite these clear advantages, the challenge of ensuring a high level of security, reliability and accuracy of computational results remains both relevant and complex. The main difficulty lies in the lack of direct control over the software and hardware components of the computing elements that join the system. As a result, there is a need for repeated verification of obtained results, which certainly increases system load and reduces overall performance. Without such verification, there is a risk of result alteration due to the specific nature of task execution in this environment. Since computation are divided into smaller parts and distributed among a large number of nodes, with partial results later aggregated into single output, even one error or malicious action can critically affect the accuracy of the final result. Given this, the goal of the article is to present a modified trust model based on fuzzy logic, which enables the appropriate distribution of roles among elements in the system. This modification is expected to reduce the number of required result verifications and improve the overall efficiency of grid system functioning.*

*Keywords: distributed systems, trust model, fuzzy logic*

## ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Грід-обчислювальні системи є перспективним та актуальним напрямком в організації розподілених обчислень, що дозволяє залучити значні обчислювальні ресурси завдяки здатності такої топології до масштабування [1]. Зворотним боком цього підходу є низка особливостей, пов'язаних із залученням зовнішніх обчислювальних елементів. На відміну від кластерних [2] чи хмарних систем [3], грід використовує ресурси, які не перебувають під прямим контролем системи [4], що означає обмежений доступ як до апаратного, так і до програмного забезпечення цих елементів. Кожен вузол є автономним і самостійно визначає обсяг роботи участі у виконанні завдань [5], а отже, система не може гарантувати достовірність результатів обчислень. У зв'язку з чим виникає ключова проблема – відсутність довіри до результатів, отриманих від сторонніх обчислювальних елементів.

Для її вирішення широко використовують моделі довіри [6], які дозволяють формувати індивідуальний рівень довіри до кожного вузла [7], що враховується під час розв'язання або критичних

ситуацій у процесі обчислень. Такий підхід знижує потребу у частих додаткових перевірках, які необхідні для забезпечення правильності обчислень. Це своєю чергою, дозволяє зменшити навантаження на систему та підвищити її загальну ефективність. Формування рівня довіри може базуватись на різних підходах: репутаційний підхід [8] оцінює надійність вузла за історією виконаних завдань; поведінковий аналіз [9] враховує типові дії вузла попередніх сценаріях; блокчейн-підхід [10] забезпечує прозорість і незмінність взаємодій через децентралізований облік усіх подій, які відбуваються в системі; натомість еволюційні алгоритми [11] використовуються для оптимального налаштування параметрів довіри, адаптуючи їх до змін середовища. Вибір конкретного підходу залежить від архітектури системи, цілей обчислень та вимог до безпеки.

Розподілені системи активно застосовуються в різних наукових і прикладних сферах [12,13], зокрема в аналізі зловмисного програмного забезпечення [14-16], дослідженні мережевих компонентів [17], а також у задачах, що потребують значних обчислювальних ресурсів [18-19], таких як навчання моделей штучного інтелекту [20]. Тому пошук нових методів організації обчислень і підвищення їх захищеності залишається актуальним напрямком дослідження.

## АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

З розвитком цифрових технологій за зростанням складності сучасних систем моделі довіри стали одними з ключових механізмів, які забезпечують рівень безпеки та ефективну взаємодію між різними суб'єктами. У своїй основі модель довіри визначає ступінь надійності певного об'єкта, чи то користувача, пристрою чи програмного забезпечення. Сфера застосування моделей довіри є надзвичайно широкою та охоплює численні галузі. Наприклад, у сфері кібербезпеки такі моделі використовуються для автентифікації та авторизації користувачів, у сфері електронної комерції вони допомагають оцінювати надійність продавців та покупців, а в соціальних мережах сприяють ідентифікації фейкових новин та профілів. Для формування моделей довіри розробники вдаються до багатьох підходів. Основні з них можна визначити наступним чином:

*Репутаційний підхід.* Репутаційні моделі довіри базуються на історії взаємодії вузлів у системі. Кожен учасник отримує певний рейтинг або бал довіри, що регулярно оновлюється залежно від коректності чи некоректності виконання завдань, підтверджених іншими елементами. Репутаційний підхід активно використовується в системах з великою кількістю учасників та непостійною структурою, оскільки дозволяє швидко оцінювати надійність вузлів. Відповідно, система може приймати рішення про делегування завдань тільки тим елементам, які демонструють високий рівень довіри.

*Блокчейн-підхід*. У моделях довіри, що базуються на технології блокчейн, інформація про взаємодію між вузлами зберігається в децентралізованому реєстрі, що забезпечує незмінність та доступність даних для всіх учасників. Це гарантує прозорість та можливість проведення незалежного аудиту й верифікації будь-яких виконаних подій. Завдяки децентралізованому характеру, блокчейн-підхід особливо ефективний у відкритих або гібридних середовищах, де відсутня централізована довірена сторона. Крім того, можливе автоматичне прийняття рішень на основі довіри за допомогою смарт-контрактів, що значно спрощує управління процесами.

*Генетичний підхід.* Генетичні алгоритми застосовуються для оптимізації параметрів моделі довіри в умовах складних та динамічних середовищ. Вони імітують процес природнього відбору генеруючи і поступово вдосконалюючи набори стратегій оцінювання довіри шляхом мутацій, кросоверів і використання функцій пристосованості. Генетичні моделі дозволяють створювати адаптивні системи, здатні реагувати на зміни поведінки елементів чи структурні зміни у мережі. Цей підхід особливо корисний у випадках, коли аналітичне налаштування параметрів є складним або навіть неможливим.

*Поведінковий підхід.* Поведінкові моделі довіри базуються на аналізі дій вузла під час виконання завдань: часу відгуку, кількості помилок, відмов у виконанні або відхилень від очікуваної поведінки. Рівень довіри визначається не на основі історичних оцінок від інших елементів, а за поточними і прогнозованими шаблонами поведінки. Такий підхід дає змогу виявляти нестабільні або потенційно зловмисні елементи системи, навіть якщо попередній досвід взаємодії із ними відсутній. Часто поведінковий аналіз інтегрується з методами машинного навчання, що додатково підвищує точність і швидкість прогнозування надійності вузлів.

Впровадження моделей довіри є важливим та необхідним етапом побудови безпечних і надійних інформаційних систем. Використання таких моделей дозволяє знизити ризики шахрайства, несанкціонованого доступу та інших кіберзагроз, сприяючи формуванню стійких і надійних взаємодій між різними учасниками цифрового середовища.

### Ролі в обчислювальних елементів в розподіленій системі

Класична модель довіри оперує бінарними ознаками: це або «довіряю», або «не довіряю». Використовуючи подібну логіку з точку зору організації розподілених систем, можемо визначити, що у класичній моделі грід-систем статус обчислювального елемента означати лише те, чи можна приймати результати виконаних ним обчислень. Однак такий підхід вимагає чіткого визначення ключових факторів, на основі яких робитиметься припущення про довіру або недовіру до конкретного елемента. Ці фактори, у свою

чергу, мають базуватись на інформації, доступній для аналізу. В роботі [21] детально представлено особливості функціонування подібних систем. Під час реалізації програмних застосунків як для обчислювальних елементів, так і для центрального сервера можуть використовуватись основні бібліотеки мов програмування і додаткові, що здатні зчитувати інформацію про апаратне та програмне забезпечення елементів. Отримана інформація є важливою для формування поведінкової характеристики обчислювального елемента. Оцінка поведінки формується після кожного виконаного завдання, що дозволяє постійно оновлювати дані про елемент. Для оцінювання поведінки використовуються два набори даних (1) (2):

$$BI_S = \{os, cpu_a, cpu_m, cpu_s, ram, home\_d, mac\} \quad (1)$$

де, $BI_S$ – це множина, яка формує набір інформації про програмне та апаратне забезпечення; $os$ – версія операційної системи; $cpu_a$ – архітектура процесора; $cpu_m$ – модель процесора; $cpu_s$ – базова швидкість ядра процесора; $ram$ – кількість оперативної пам'яті; $home\_d$ – шлях домашнього каталогу; $mac$ – MAC-адреса.

$$BI_H = \{task_c, task_p, task_s, task_r, task_{prod}\} \quad (2)$$

де, $BI_H$ – множина, яка містить показники, що характеризують поведінку обчислювального елемента під час виконання завдання, $task_c$ – обчислювальна складність виконаної задачі, $taks_p$ – фактичний час, витрачений на її виконання, $task_s$ – час, необхідний для передачі задачі до обчислювального елементу, $task_r$ – час, витрачений на передачу результату після виконання, $task_{prod}$ – коефіцієнт продуктивності виконаного завдання.

Враховуючи, що рівень довіри зазвичай визначається в межах від 0 до 1, а також зважаючи на особливості його застосування в розподілених обчислювальних системах, пропонується розділити цей діапазон між різними ролями обчислювальних елементів. Оскільки система потребує повторних перевірок під час виконання обчислень, а правильність залежить від коректного виконання кожної частини задачі, доцільно виокремити такі ролі: довірений обчислювальний елемент – центральний сервер ніколи не здійснює додаткових перевірок результатів, які повертаються цими елементами; звичайний обчислювальний елемент – система не довіряє цим елементам повністю, тому частини їхніх завдань надсилаються іншим елементам для перевірки коректності обчислень; новий обчислювальний елемент – елементи, що мають початковий рівень довіри. Система надсилає їм тестові завдання для оцінки обчислювальних можливостей, а також звичайні завдання з метою поступового підвищення рівня довіри до рівня «звичайного» елемента; недовірений обчислювальний елемент – вузол, що припустився значної кількості помилок під час виконання завдань (що було виявлено шляхом голосування). Система розцінює його як скомпрометований і вимагає численних перевірок перед поверненням до статусу звичайного обчислювального елемента. Такий підхід до класифікації дозволяє виділити певну частину обчислювальних елементів, що працюватимуть без додаткових перевірок, тим самим вивільняючи ресурси для інших задач. Окрему роль відведено елементам, які щойно приєдналися до системи або довго не брали участі в обчисленнях – така ситуація є типовою для волонтерських систем. Також пропонується реалізувати можливість динамічного коригування меж між ролями, що дозволить адміністратору керувати часткою ресурсів, яку буде спрямовано на повторні обчислення.

**Нечітка логіка для визначення ролі обчислювального елементу**

Для застосування нечіткої логіки в моделі довіри необхідно провести попередню нормалізацію параметрів, які формуються під час виконання завдань обчислювальними елементами. Однак перед нормалізацією доцільно класифікувати ці параметри на окремі групи відповідно до їхньої природи та способу подальшої обробки, оскільки різні параметри мають різне семантичне навантаження і потребують відповідного підходу до нормалізації. Зокрема, виділяємо статичні параметри – які характеризують апаратне та програмне забезпечення обчислювального елемента, та використовуються для визначення чи співпадають поточні характеристики із зафіксованим профілем користувача. До них можна віднести $os$, $cpu_a$, $cpu_m$, $cpu_s$, $ram$, $home\_d$, $mac$. Для них нормалізація відбувається за принципом бінарної відповідності (3). Поведінкові параметри відображають характер виконання завдань, і для забезпечення незалежності від складності завдань усі значення попередньо нормалізуються із урахуванням $task_c$ (4). Після чого застосовується нормалізація методом мінімуму-максимуму.

$$X^i_{static} = \begin{cases} 1, \text{якщо значення збігається з еталонним} \\ 0, \quad \text{якщо значенн відрізняється} \end{cases} \quad (3)$$

$$X^j_{adj} = \frac{X}{task_c}, \quad X^j_{adj_{norm}} = 1 - \frac{X_{adj} - X_{min}}{X_{max} - X_{min}} \quad (4)$$

До поведінкових параметрів належать: час виконання $task_p$, час відправки задачі $task_s$, час відправки результату $task_r$, коефіцієнт продуктивності $task_{prod}$. І далі на основі нормалізованих значень формуються дві групові оцінки: оцінка стабільності конфігурації вузла (5) та оцінка поведінки вузла (6). Сформовані значення використовуються для підрахунку уже рівня довіри обчислювального елемента (7).

$$Trust_{static} = \frac{1}{n}\sum_{i=1}^{n} X_{static}^{i} \tag{5}$$

$$Trust_{behaviour} = \frac{\sum_{j=1}^{m} w_j * X_{adj_{norm}}^{j}}{\sum_{j=1}^{m} w_j} \tag{6}$$

$$TrustLevel = w_{static} * Trust_{static} + w_{behaviour} * Trust_{behaviour} \tag{7}$$

На рисунку 2, зображено основні компоненти центрального сервера та його взаємодію із запропонованими ролями обчислювальних елементів

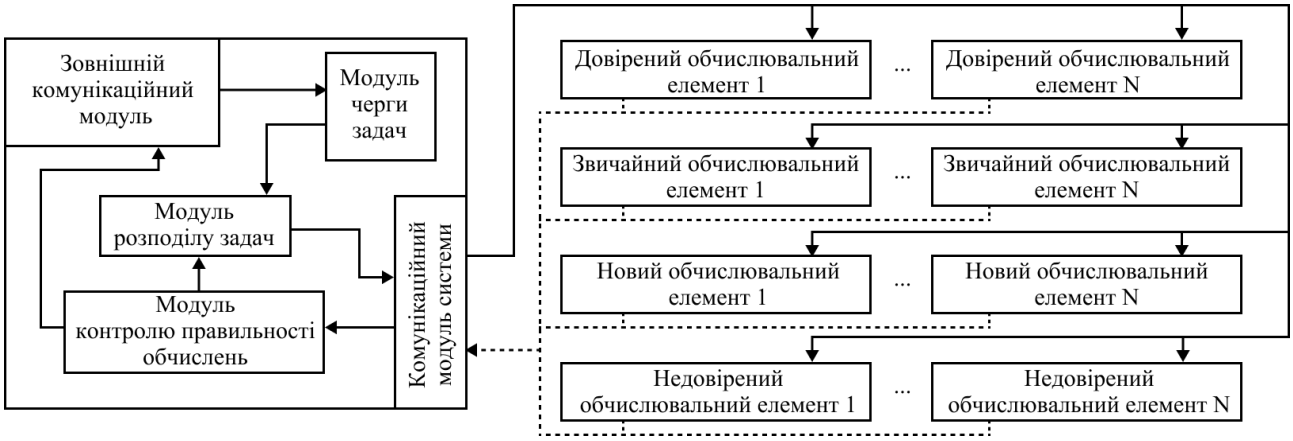


**Рис. 2. Взаємодія елементів в розподіленій системі обчислень**

В цілому, такий підхід дозволяє з одного боку приймати до уваги сталість конфігурації вузла, а з іншого – враховувати продуктивність і надійність виконання обчислювальних задач. У разі компрометації облікового запису користувача показник довіри зміниться, що дозволить виявити підозрілий обчислювальний елемент.

## Експериментальні дослідження

У якості експерименту було проведено дослідження на задачі, детально описаній у роботі [18]. Вона полягала в аналізі поведінки виконання програм на різних обчислювальних елементах, що створювали модифіковані ізольовані середовища для виявлення аномалій виконання, що можуть свідчити про наявність зловмисного програмного забезпечення. Зважаючи на складність виявлення поліморфних вірусів, виникає потреба у додаткових перевірках, які реалізуються за допомогою запропонованої системи. У дослідженні було розроблено визначену кількість вірусних зразків та використано визначену кількість обчислювальних елементів. Результати представлено в таблиці 1.

Таблиця 1

**Результати експериментів із використанням модифікованої моделі довіри**

| Кількість програм на перевірку | Повторні перевірки без моделі | Повторні перевірки з моделлю | Зменшення перевірок | Економія ресурсів |
|---|---|---|---|---|
| 100 | 1200 | 1130 | 70 | 5.83% |
| 100 | 990 | 942 | 48 | 4.85% |
| 80 | 910 | 854 | 56 | 6.15% |
| 120 | 1400 | 1315 | 85 | 6.07% |
| 120 | 860 | 823 | 37 | 4.30% |

Результати використання модифікованої моделі довіри продемонстрували скорочення кількості необхідних повторних перевірок на рівні 4-6%, без зниження надійності виконання обчислень у межах розподіленої грід-обчислювальної системи.

## ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі було запропоновано модифіковану модель довіри для розподілених грід-обчислювальних систем, що базується на використанні нечіткої логіки з урахуванням як апаратно-програмних характеристик, так і поведінкових показників обчислювальних елементів. Для забезпечення правильного використання цих показників у загальну систему оцінки довіри, всі значення було попередньо нормалізовано, зокрема – з урахуванням складності виконуваних завдань. В роботі пропонується виокремлення двох груп ознак: параметри конфігурації та поведінкові характеристики виконання обчислень. Застосування зваженого агрегування дозволило виявляти елементи системи, які могли бути скомпрометовані. В результаті проведених експериментів було зафіксовано скорочення кількості повторних перевірок обчислень на 4-6%. Таким чином, запропонована модель дозволяє зменшити надлишкове навантаження на обчислювальні ресурси. У майбутніх дослідженнях можливе доповнення моделі часовими шаблонами активності обчислювальних елементів, а також розширення критеріїв нечіткої класифікації шляхом використання методів машинного навчання для автоматичного вагових коефіцієнтів.

**Література**

1. Waheed A. A comprehensive review of computing paradigms, enabling computation offloading and task execution in vehicular networks / A. Waheed, M. A. Shah, S. M. Mohsin, A. Khan, C. Maple, S. Aslam, S. Shamshirband // IEEE Access. – 2022. – Т. 10. – С. 3580–3600.
2. Cluster computing [Електронний ресурс] // IBM. – Режим доступу: https://www.ibm.com/think/topics/cluster-computing (дата звернення: 22.03.2025). – Назва з екрану.
3. Golightly L. Adoption of cloud computing as innovation in the organization / L. Golightly, V. Chang, Q. A. Xu, X. Gao, B. S. Liu // International Journal of Engineering Business Management. – 2022. – Т. 14. – С. 1–17.
4. Curiel M. J., Scheduling strategies for mobile devices in BOINC / M. J. Curiel, A. Payares // Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação. – 2021. – Т. 1, вип. 13. – С. 1–25
5. Agrawala A. SETI@home: A Detailed Analysis and Study / A. Agrawala, R. S. Kulkarnib // International Astronautical Congress (IAC): матеріали 70th International Conference, [Washington D.C.]. – 21-25 October 2019 / International Astronautical Federation (IAF). – Washington D.C., 2019. – С. 1-6.
6. Cho J. H. A survey on trust modeling / J. H. Cho, K. Chan, S. Adali // ACM Computing Surveys (CSUR). – 2015. – Т. 48, вип. 2. – С. 1–40.
7. He Y. A survey on zero trust architecture: Challenges and future trends / Y. He, D. Huang, L. Chen, Y. Ni, X. Ma // Wireless Communications and Mobile Computing. – 2022. – вип. 1. – С. 647627.
8. Verma R. RepuTE: A soft voting ensemble learning framework for reputation-based attack detection in fog-IoT milieu / R. Verma, S. Chandra // Engineering Applications of Artificial Intelligence. – 2023. – Т. 118. – С. 105670.
9. Zhu Y. Research on 5G core network trust model based on NF interaction behavior / Y. Zhu, C. Liu, Y. Zhang, W. You // KSII Transactions on Internet and Information Systems (TIIS). – 2022. – Т. 16, вип. 10. – С. 3333–3354.
10. Li W. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions / W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, R. Buyya // Journal of Cloud Computing. – 2021. – Т. 10, вип. 1. – С. 35.
11. Bakhtiari N. B. A trust management system for fog computing using improved genetic algorithm / N. B. Bakhtiari, M. Rafighi, R. Ahsan // The Journal of Supercomputing. – 2024. – Т. 80, вип. 14. – С. 20923–20955.
12. Ming J. Deep Einstein@Home Search for Continuous Gravitational Waves from the Central Compact Objects in the Supernova Remnants Vela Jr. and G347.3-0.5 Using LIGO Public Data / J. Ming, M. A. Papa, H. B. Eggenstein, B. Beheshtipour, B. Machenschalk, R. Prix, B. Allen, M. Bensch // The Astrophysical Journal. – 2024. – Т. 977, вип. 2. – С. 154.
13. Korpela E. J. The next phases of SETI@home / E. J. Korpela, A. P. Siemion, D. Werthimer, M. Lebofsky, J. Cobb, S. Croft, D. Anderson // Instruments, Methods, and Missions for Astrobiology XVII : матеріали International Conference, [San Diego, California, United States] – 11 September 2015 / SPIE Optical Engineering + Applications – San Diego, 2015. – С. 44-48.
14. Savenko B. Malware Detection By Distributed Systems with Partial Centralization / B. Savenko, A. Kashtalian, S. Lysenko, O. Savenko // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) : матеріали IEEE 12th International Conference, [Dortmund, Germany] – 07-09 September.– Том. 1. – / IEEE – Dortmund, 2023. – С. 265-270
15. Kashtalian A. Multi-computer malware detection systems with metamorphic functionality / A. Kashtalian, S. Lysenko, O. Savenko, A. Nicheporuk, T. Sochor, V. Avsiyevych // Radioelectronic and Computer Systems. – 2024. – Т. 2024 – вип. 1. – С. 152–175.
16. Denysiuk D. Method for Detecting Steganographic Changes in Images Using Machine Learning /

D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko, A. Kashtalian // Dependable Systems, Services and Technologies (DESSERT) : матеріали 13th International Conference, [Athens, Greece] – 13-15 October. 2023 / IEEE – Athens, 2023. – С. 1-6.

17. Nicheporuk A. An android malware detection method based on CNN mixed-data model / A. Nicheporuk, O. Savenko, A. Nicheporuk, Y. Nicheporuk // Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : матеріали 16th International Conference, [Kharkiv, Ukraine] – Том. 2732. – October 06-10. 2020. / CEUR – Kharkiv, 2020 – С. 198–213.

18. Rehida P. State-based sandbox tool for distributed malware detection with avoid techniques. / P. Rehida, G.Markowsky, A. Sachenko, O. Savenko // Dependable Systems, Services and Technologies (DESSERT) : матеріали 13th International Conference, [Athens, Greece] – 13-15 October. 2023 / IEEE – Athens, 2023. – С. 1-6.

19. Rehida P. A distributed malware detection model based on sandbox technology / P. Rehida, T. Sochor, V. Martynyuk, O. Tarasova, V. Orlenko // Intelligent Information Technologies & Systems of Information Security 2023 : матеріали 4th International Workshop, [Khmelnytskyi, Ukraine] – 22-24 March. 2023 / CEUR – Khmelnytskyi, 2023. С. 475-485.

20. Lysenko S. IoT multi-vector cyberattack detection based on machine learning algorithms: traffic features analysis, experiments, and efficiency / S. Lysenko, K. Bobrovnikova, V. Kharchenko, O. Savenko // Algorithms. – 2022. – Т. 15, вип. 7. – С. 239-263.

21. Rehida P. A trust model that ensures the correctness of computing in grid computing system. / Rehida P., Savenko O., Sachenko A., Drozd A., Vizhevski P. // Intelligent Information Technologies & Systems of Information Security 2024 : матеріали 5th International Workshop, [Khmelnytskyi, Ukraine] – 28 March, 2024 / CEUR - Khmelnytskyi, 2024. С 388-401.

## References

1. Waheed A. A comprehensive review of computing paradigms, enabling computation offloading and task execution in vehicular networks / A. Waheed, M. A. Shah, S. M. Mohsin, A. Khan, C. Maple, S. Aslam, S. Shamshirband // IEEE Access. – 2022. – Vol. 10. – P. 3580–3600.м

2. Cluster computing [Electronic resource] // IBM. – Available at: https://www.ibm.com/think/topics/cluster-computing (accessed: 05.03.2025). – Screen name.

3. Golightly L. Adoption of cloud computing as innovation in the organization / L. Golightly, V. Chang, Q. A. Xu, X. Gao, B. S. Liu // International Journal of Engineering Business Management. – 2022. – Vol. 14. – P. 1–17.

4. Curiel M. J., Scheduling strategies for mobile devices in BOINC / M. J. Curiel, A. Payares // Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação. – 2021. – Vol. 1, №. 13. – P. 1–25

5. Agrawala A. SETI@home: A Detailed Analysis and Study / A. Agrawala, R. S. Kulkarnib // International Astronautical Congress (IAC): proceedings 70th International Conference, [Washington D.C.]. – 21-25 October 2019 / International Astronautical Federation (IAF). – Washington D.C., 2019. – P. 1-6.

6. Cho J. H. A survey on trust modeling / J. H. Cho, K. Chan, S. Adali // ACM Computing Surveys (CSUR). – 2015. – Vol. 48, №. 2. – P. 1–40.

7. He Y. A survey on zero trust architecture: Challenges and future trends / Y. He, D. Huang, L. Chen, Y. Ni, X. Ma // Wireless Communications and Mobile Computing. – 2022. – №. 1. – P. 647627.

8. Verma R. RepuTE: A soft voting ensemble learning framework for reputation-based attack detection in fog-IoT milieu / R. Verma, S. Chandra // Engineering Applications of Artificial Intelligence. – 2023. – Vol. 118. – P. 105670.

9. Zhu Y. Research on 5G core network trust model based on NF interaction behavior / Y. Zhu, C. Liu, Y. Zhang, W. You // KSII Transactions on Internet and Information Systems (TIIS). – 2022. – Vol. 16, №. 10. – P. 3333–3354.

10. Li W. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions / W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, R. Buyya // Journal of Cloud Computing. – 2021. – Vol. 10, №. 1. – P. 35.

11. Bakhtiari N. B. A trust management system for fog computing using improved genetic algorithm / N. B. Bakhtiari, M. Rafighi, R. Ahsan // The Journal of Supercomputing. – 2024. – Vol. 80, №. 14. – P. 20923–20955.

12. Ming J. Deep Einstein@Home Search for Continuous Gravitational Waves from the Central Compact Objects in the Supernova Remnants Vela Jr. and G347.3-0.5 Using LIGO Public Data / J. Ming, M. A. Papa, H. B. Eggenstein, B. Beheshtipour, B. Machenschalk, R. Prix, B. Allen, M. Bensch // The Astrophysical Journal. – 2024. – Vol. 977, № 2. – P. 154.

13. Korpela E. J. The next phases of SETI@home / E. J. Korpela, A. P. Siemion, D. Werthimer, M. Lebofsky, J. Cobb, S. Croft, D. Anderson // Instruments, Methods, and Missions for Astrobiology XVII : proceedings of International Conference, [San Diego, California, United States] – 11 September 2015 / SPIE Optical Engineering + Applications – San Diego, 2015. – P. 44-48.

14. Savenko B. Malware Detection By Distributed Systems with Partial Centralization / B. Savenko, A. Kashtalian, S. Lysenko, O. Savenko // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) : proceedings of IEEE 12th International Conference, [Dortmund, Germany] – 07-09 September.– Vol. 1. – / IEEE – Dortmund, 2023. – P. 265-270

15. Kashtalian A. Multi-computer malware detection systems with metamorphic functionality / A. Kashtalian, S. Lysenko, O. Savenko, A. Nicheporuk, T. Sochor, V. Avsiyevych // Radioelectronic and Computer Systems. – 2024. – Vol. 2024 – №. 1. – P. 152–175.

16. Denysiuk D. Method for Detecting Steganographic Changes in Images Using Machine Learning / D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko, A. Kashtalian // Dependable Systems, Services and Technologies (DESSERT) : proceedings of 13th International Conference, [Athens, Greece] – 13-15 October. 2023 / IEEE – Athens, 2023. – P. 1-6.

17. Nicheporuk A. An android malware detection method based on CNN mixed-data model / A. Nicheporuk, O. Savenko, A. Nicheporuk, Y. Nicheporuk // Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer : proceedings of 16th International Conference, [Kharkiv, Ukraine] – Vol. 2732. – October 06-10. 2020. / CEUR – Kharkiv, 2020 – P. 198–213.

18. Rehida P. State-based sandbox tool for distributed malware detection with avoid techniques. / P. Rehida, G.Markowsky, A. Sachenko, O. Savenko // Dependable Systems, Services and Technologies (DESSERT) : proceedings of 13th International Conference, [Athens, Greece] – 13-15 October. 2023 / IEEE – Athens, 2023. – P. 1-6.

19. Rehida P. A distributed malware detection model based on sandbox technology / P. Rehida, T. Sochor, V. Martynyuk, O. Tarasova, V. Orlenko // Intelligent Information Technologies & Systems of Information Security 2023 : proceedings of 4th International Workshop, [Khmelnytskyi, Ukraine] – 22-24 March. 2023 / CEUR – Khmelnytskyi, 2023. P. 475-485.

20. Lysenko S. IoT multi-vector cyberattack detection based on machine learning algorithms: traffic features analysis, experiments, and efficiency / S. Lysenko, K. Bobrovnikova, V. Kharchenko, O. Savenko // Algorithms. – 2022. – Vol. 15, №. 7. – P. 239-263.

21. Rehida P. A trust model that ensures the correctness of computing in grid computing system. / Rehida P., Savenko O., Sachenko A., Drozd A., Vizhevski P. // Intelligent Information Technologies & Systems of Information Security 2024 : матеріали 5th International Workshop, [Khmelnytskyi, Ukraine] – 28 March, 2024 / CEUR - Khmelnytskyi, 2024. С 388-401.