DOI 10.31891/2307-5732-2024-339-4-74
УДК 004.056.5

ЛУЖЕЦЬКИЙ ВОЛОДИМИР
Вінницький національний технічний університет
https://orcid.org/0000-0001-7466-7738
e-mail: lva.kzi2002@gmail.com
САВИЦЬКА ЛЮДМИЛА
Вінницький національний технічний університет
https://orcid.org/0000-0003-1130-2621
e-mail: savytska.liudmyla@vntu.edu.ua

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ У ПІРИНГОВИХ МЕРЕЖАХ

У статті досліджено проблеми захисту даних у пірингових мережах. Такі мережі стають все більш популярними для комунікації завдяки їхній гнучкості, ефективності та стійкості до збоїв. Однак вони залишаються вразливими до різних видів атак, зокрема DoS/DDoS-атак, фальсифікації даних і перехоплення інформації. Основна увага приділена забезпеченню конфіденційності, доступності та цілісності даних під час їх передачі та зберігання, а також автентифікації вузлів для протидії несанкціонованому доступу та підміні ідентичностей.

Проаналізовані у статті підходи до захисту даних в пірингових мережах базуються на сучасних криптографічних методах, таких як симетричне, асиметричне шифрування, а також наскрізне шифрування. Використання геш-функцій дозволяє забезпечити контроль цілісності даних та виявлення їхньої модифікації. Цифрові підписи забезпечують автентифікацію джерела даних та підтверджують їх незмінність. Також розглянуто механізми анонімізації та псевдонімізації для захисту метаданих і збереження конфіденційності учасників комунікації. Доступність забезпечується кешуванням, автоматичним оновленням після збоїв, реплікацією даних та децентралізованим управлінням ресурсами.

Особливу увагу приділено методам виявлення аномалій у мережевій активності, що базуються на аналізі поведінки вузлів та застосуванні алгоритмів машинного навчання й нечіткої логіки. Механізми протидії атакам включають чорні списки для блокування підозрілих вузлів, динамічну зміну маршрутів передачі даних для захисту від атак типу «людина посередині» та методи самоізоляції для мінімізації ризиків поширення загроз. Пропонується запровадити модель нульової довіри для підвищення захищеності пірингових мереж.

Ключові слова: пірингова мережа, шифрування, автентифікація, геш-функція, захист даних, кіберзагроза, кібератака, чорний список, цифровий підпис, блокчейн, модель нульової довіри.

LUZHETSKYY VOLODYMYR, SAVYTSKA LIUDMYLA
Vinnytsia National Technical University

DATA PROTECTION MECHANISMS IN PEER-TO-PEER NETWORKS

The article examines the problems of data protection in peer-to-peer networks. Such networks are becoming increasingly popular for communication due to their flexibility, efficiency, and resilience to failures. However, they remain vulnerable to various types of attacks, in particular DoS/DDoS attacks, data falsification, and information interception. The main attention is paid to ensuring the confidentiality, availability, and integrity of data during their transmission and storage, as well as the authentication of nodes to counteract unauthorized access and identity substitution. The analysed approaches in the article are based on modern cryptographic methods, such as symmetric and asymmetric encryption, as well as end-to-end encryption. The use of hash functions allows for data integrity control and detection of their modification. Digital signatures provide authentication of the data source and confirm their immutability. Anonymization and pseudonymization mechanisms are also considered to protect metadata and maintain the confidentiality of communication participants. Availability is ensured by caching, automatic updates after failures, data replication, and decentralized resource management.

Particular attention is paid to methods for detecting anomalies in network activity based on the analysis of node behavior and the use of machine learning algorithms and fuzzy logic. The proposed mechanisms for countering attacks include blacklists for blocking suspicious nodes, dynamic change of data transmission routes to protect against man-in-the-middle attacks, and self-isolation methods to minimize the risks of spreading threats. It is proposed to introduce a zero-trust model to increase the security of peer-to-peer networks.

Keywords: peer-to-peer network, encryption, authentication, hash function, data protection, cyber threat, cyber attack, blacklist, digital signature, blockchain, zero trust model.

Вступ

У сучасному цифровому середовищі пірингові мережі набувають все більшого поширення завдяки їх децентралізованій архітектурі, високій стійкості до відмов окремих вузлів та здатності до масштабування. Такі мережі застосовуються в широкому спектрі сучасних технологій: від файлообмінних систем та мереж для розповсюдження мультимедійного контенту до блокчейну та розподілених обчислювальних платформ [1]. Відсутність центрального керівного органу в цих системах сприяє підвищенню автономності, ефективності використання ресурсів та гнучкості у відповіді на змінні умови функціонування.

Разом із тим, децентралізована природа пірингових мереж зумовлює низку складних питань у сфері безпеки інформації [2–5]. Зокрема, існують такі ключові напрямки небезпек:

- загрози конфіденційності, адже існує підвищений ризик несанкціонованого доступу до чутливих даних, що передаються між вузлами, через перехоплення трафіку або використання вразливостей у протоколах обміну.

- загрози цілісності пов’язані із тим, що дані, які розповсюджуються децентралізовано, можуть зазнавати модифікацій або підміни зловмисниками, що призводить до втрати їх достовірності та точності.

- загрози доступності пов’язані із використання методів зловмисного навантаження мережі

(DoS/DDoS-атаки), несанкціонованого резервування ресурсів чи інших способів порушення нормального функціонування системи, що ставлять під загрозу забезпечення стабільної роботи мережі.

- недоліки автентифікації вузлів пов'язані із відсутністю централізованого механізму ідентифікації, що ускладнює встановлення довіри між учасниками мережі, створюючи можливості для підробки ідентичностей та неправомірного використання ресурсів.

З огляду на вищезазначене, забезпечення належного рівня захисту даних у піринговых мережах набуває виняткової актуальності. Зростаюча популярність технологій, побудованих на децентралізованих засадах, у поєднанні з постійним удосконаленням методів атак, підкреслює необхідність системного підходу до розробки механізмів безпеки. Відтак, комплексний аналіз та інтеграція заходів захисту, спрямованих на збереження конфіденційності, підтримку цілісності та забезпечення доступності в децентралізованих системах, стають нагальною потребою сучасної інформаційної інфраструктури. У контексті цього дослідження розглядаються теоретичні засади, практичні методи та перспективні напрями розвитку захисних рішень для піринговых мереж з метою формування більш надійних та безпечних децентралізованих платформ.

Аналіз досліджень та публікацій

Аналіз останніх досліджень у сфері безпеки піринговых мереж свідчать про значний прогрес у розробці підходів до забезпечення безпеки децентралізованих систем. Науковці та фахівці індустрії пропонують широку гаму рішень, орієнтованих на підвищення конфіденційності, цілісності та доступності даних, одночасно долаючи недоліки традиційних підходів до автентифікації та контролю доступу. Зокрема, у фокусі дослідницьких зусиль перебувають такі напрями:

– Криптографічні методи. Інтенсивні дослідження присвячено впровадженню інноваційних криптографічних протоколів, спрямованих на підвищення захищеності комунікацій у піринговых мережах [6, 7]. Ці роботи пропонують використання комбінацій симетричних та асиметричних шифрів, оптимізацію криптографічних алгоритмів та застосування сучасних методів керування ключами, що мають забезпечити належну рівновагу між продуктивністю системи та її безпекою. Крім того, розглядаються гібридні схеми, де поєднані передові підходи до обміну ключами та методи шифрування з імовірнісними гарантіями безпеки.

– Автентифікація вузлів. Значна увага приділяється розробці ефективних механізмів автентифікації учасників піринговых мереж, оскільки класичні рішення, розроблені для клієнт-серверних архітектур, виявляються малоефективними у децентралізованому середовищі [8, 9]. Дослідники пропонують застосування схем автентифікації на основі розподілених реєстрів, криптографічних доказів із нульовим розголошенням (Zero-Knowledge Proofs) та механізмів криптографічних підписів з використанням групових та порогових схем. Такі підходи дозволяють забезпечити цілісність даних та надійно ідентифікувати вузли без необхідності централізованого контролю.

– Захист від атак та вразливостей. Чільне місце серед дослідницьких пріоритетів посідає розробка інструментів для проактивного виявлення та нейтралізації загроз [10, 11]. Використання методів машинного навчання, глибокого аналізу трафіку, аномалійної детекції та формальних методів верифікації безпеки стає дедалі поширенішим. Такі рішення дозволяють не лише виявляти атаки типу «людина посередині», фальшування повідомлень та несанкціонований доступ до ресурсів, але й сприяють побудові стійких до нападів мережевих структур, здатних до швидкого відновлення та адаптації.

Результати попередніх досліджень засвідчують тенденцію до поглиблення комплексного підходу у сфері безпеки піринговых мереж. Це включає інтеграцію криптографічних механізмів, удосконалення методів автентифікації та впровадження розвинених стратегій виявлення та попередження атак. Такий багатовимірний підхід слугує підґрунтям для створення надійних децентралізованих середовищ, здатних забезпечити сталу роботу й захист інформаційних ресурсів у сучасних умовах постійно еволюціонуючих кіберзагроз.

Формулювання цілей статті

Метою роботи є аналіз та узагальнення сучасних підходів і механізмів забезпечення конфіденційності, доступності та цілісності даних у піринговых мережах. Це включає вивчення таких аспектів, як використання криптографічних методів для захисту передавання даних, механізмів автентифікації учасників мережі та методів виявлення й запобігання атакам, таким як «людина по середині» та відмова в обслуговуванні.

Виклад основного матеріалу

Використання піринговых мереж у сучасних інформаційних системах дедалі розширюється, завдяки їхній високій стійкості, масштабованості та автономності. Водночас, враховуючи децентралізований характер таких мереж, вони залишаються вразливими до дій зловмисників, які можуть спричинити витік конфіденційної інформації, порушення цілісності або недоступність критично важливих даних. З огляду на це, питання розробки й удосконалення методів захисту, орієнтованих на забезпечення конфіденційності, доступності та цілісності у піринговых мережах, є надзвичайно актуальним.

Методи забезпечення конфіденційності у піринговых мережах охоплюють широкий спектр підходів, серед яких провідну роль відіграють криптографічні методи шифрування, анонімізація метаданих та надійна автентифікація вузлів.

Використання криптографії є базовим інструментом для збереження конфіденційності даних у піринговых мережах [12]. Використовуються такі основні типи шифрування:

- симетричні алгоритми забезпечують високу швидкість обробки даних, проте вимагають безпечного розповсюдження спільного ключа, що ускладнює початкову фазу обміну інформацією.

- асиметричні схеми використовують пару ключів (публічний та приватний), що спрощує процес передачі ключів та підвищує безпеку комунікаційних сесій. Часто на практиці застосовується гібридний підхід: симетричний ключ для шифрування інформації, а асиметричний – для безпечної передачі цього ключа.

- наскрізне шифрування, при якому ключі відомі лише відправнику та отримувачу, унеможливлюючи доступ до інформації для проміжних вузлів або серверів.

Анонімізація та псевдонімізація користувачів та їхньої активності у мережі дозволяють приховати справжню ідентичність вузлів та суттєво ускладнюють відстеження комунікаційних ланцюжків [13]. Використання таких механізмів особливо важливе в контексті захисту метаданих, оскільки саме вони часто стають цінною мішенню для зловмисників, що прагнуть виявити модель взаємодії та структуру мережі.

Забезпечення автентифікації учасників пірингової мережі слугує перевіркою достовірності джерела даних, запобігаючи втручанню підроблених або скомпрометованих вузлів [14]. Для цього застосовуються цифрові сертифікати безпеки та інфраструктура відкритих ключів, механізми багатофакторної автентифікації для зниження ймовірності несанкціонованого доступу, криптографічні підписи запитів, які гарантують цілісність та справжність даних.

Таким чином, розвиток комплексних рішень, що поєднують ефективне шифрування, анонімізацію метаданих та надійну автентифікацію учасників, є важливим напрямом удосконалення безпеки пірингових мереж. Ці підходи закладають підґрунтя для формування більш захищених децентралізованих комунікаційних платформ, здатних витримувати сучасні виклики у сфері інформаційної безпеки.

У забезпеченні цілісності даних у пірингових мережах особливу роль відіграють механізми контролю їхнього стану та походження, що дозволяють вчасно виявити будь-які спроби підробки чи несанкціонованої модифікації інформації. Серед найважливіших підходів у цій сфері виокремлюють використання криптографічних геш-функцій, цифрових підписів та децентралізованих реєстрів (блокчейн).

Криптографічні геш-функції слугують одним із базових інструментів перевірки цілісності даних [15]. Їх суть полягає у формуванні унікального геш-значення для заданого повідомлення чи файлу. Будь-яка, навіть незначна зміна вихідних даних, призводить до кардинальної зміни гешу, що миттєво сигналізує про можливу спробу модифікації або підробки інформації. Наприклад, при передаванні файлу відправник обчислює його геш, а отримувач після приймання повторно визначає геш та порівнює зі значенням, наданим відправником. Невідповідність гешів свідчить про порушення цілісності переданих даних.

Цифрові підписи є потужним засобом одночасного забезпечення цілісності та автентичності джерела даних [16]. Процес включає створення підпису з використанням приватного ключа відправника та подальшу його верифікацію за допомогою відповідного публічного ключа. Алгоритмічно процедура може бути розділена на декілька етапів:

- відправник обчислює геш повідомлення;
- цей геш шифрується приватним ключем, формуючи цифровий підпис;
- отримувач, отримавши повідомлення та підпис, розшифровує підпис публічним ключем відправника та порівнює отриманий геш з гешем самого повідомлення. Якщо ці геш-значення співпадають, це гарантує відсутність змін під час передавання й підтверджує справжність джерела даних.

Такий підхід широко використовується в корпоративних системах, де важливо забезпечити контроль походження документів та недоторканність їхнього вмісту.

Технологія блокчейн забезпечує децентралізований механізм фіксації подій, транзакцій та обміну даними у вигляді послідовності блоків, кожен з яких містить геш попереднього [17, 18]. Цей підхід гарантує неможливість непомітної модифікації будь-якого блоку без порушення цілісності всього ланцюжка. Таким чином, спроба змінити інформацію в одному блоці призводить до розбіжностей у гешах та порушення консенсусу в мережі, що миттєво фіксується учасниками. Блокчейн-технологія виявляється особливо корисною у середовищах, де важливо зберігати історію дій чи транзакцій у незмінному та прозорому вигляді, без необхідності довіри до центрального сервера або третьої сторони.

Загалом, сукупність механізмів контролю цілісності формує надійну основу для захисту інформації, що циркулює у пірингових мережах. Поєднання цих підходів із іншими безпековими засобами сприяє створенню сталої та безпечної децентралізованої інфраструктури, здатної ефективно протистояти різноманітним загрозам.

Механізми забезпечення доступності даних у пірингових мережах відіграють ключову роль у підтриманні стабільності, надійності та безперервності функціонування децентралізованих систем. Ефективні стратегії спрямовані на мінімізацію часу простою, оперативне відновлення після збоїв та оптимальний розподіл ресурсів між вузлами мережі.

Одним із найпоширеніших методів підвищення доступності інформаційних ресурсів у пірингових мережах є реплікація, тобто збереження копій даних на декількох вузлах одночасно [19]. Такий підхід дає змогу знизити ризик втрати даних у разі виходу окремого вузла з ладу або непередбаченої відмови обладнання. Завдяки наявності множинних копій, користувачі отримують доступ до необхідної інформації навіть у критичних ситуаціях, забезпечуючи тим самим високу надійність мережі.

У децентралізованих мережах кожен вузол володіє автономією в керуванні власними ресурсами, що

створює гнучку та саморегульовану інфраструктуру [20]. Такий підхід дає можливість швидко реагувати на зміни робочого навантаження, адаптуватися до нових умов і розподіляти ресурси між вузлами відповідно до актуальних потреб, уникаючи «вузьких місць» та підвищуючи доступність системи в цілому.

Механізми автоматичного відновлення спрямовані на швидку реанімацію вузлів після непередбачених збоїв та помилок [21]. Наприклад, у разі виходу одного з вузлів з ладу, мережа автоматично перенаправляє трафік до інших доступних вузлів, мінімізуючи час простою та втрати даних. Така динамічна реакція дозволяє підтримувати безперебійну роботу децентралізованого середовища навіть за несприятливих умов.

Тимчасове збереження найчастіше запитуваних даних на проміжних вузлах сприяє скороченню часу доступу та зниженню навантаження на основні вузли мережі [22]. Кешування забезпечує підвищення ефективності роботи системи, оскільки вузли можуть надавати дані без необхідності повторних звернень до першоджерела. Це особливо важливо в умовах високого трафіку та при непередбачених збоях, коли швидке отримання інформації стає критичним фактором.

Поєднання цих стратегій дає змогу користувачам мати безперервний та надійний доступ до даних навіть за умов змінних робочих навантажень, атак на мережу чи збоїв у обладнанні.

Механізми виявлення та протидії атакам у піринговых мережах відіграють вирішальну роль у збереженні безпеки та стабільності децентралізованих середовищ [23]. Наявність потенційних зловмисників, які намагаються отримати несанкціонований доступ до даних, порушити цілісність або завадити доступності мережі, вимагає ефективних рішень для ідентифікації аномальної активності, блокування підозрілих вузлів та динамічної оптимізації маршрутів передачі даних.

Один із ключових методів виявлення атак полягає у моніторингу поведінкових патернів вузлів мережі [24]. На підставі параметрів, таких як частота запитів, обсяг переданих даних, наявність збоїв або перевантаження ресурсів, система може визначити, чи відповідає активність конкретного вузла нормальному режиму роботи. Застосування алгоритмів машинного навчання та нечіткої логіки дозволяє виявляти складні нетипові ситуації [25]. Таким чином, раптове зростання обсягу трафіку від окремого вузла, надмірна кількість запитів або збільшена затримка у відповідях можуть бути класифіковані як індикатори потенційної атаки, що дає підстави для вжиття відповідних заходів безпеки.

У разі виявлення зловмисної активності вузли мережі можуть автоматично вносити підозрілі адреси до чорних списків, блокуючи тим самим будь-які майбутні спроби взаємодії з ними [26]. Додатково, окремі вузли здатні переходити в режим самоізоляції, тимчасово від’єднуючись від мережі з метою запобігти поширенню атак або конфіденційних даних. Такий підхід дає змогу швидко й ефективно локалізувати загрозу та вивести зловмисний вузол з подальшої взаємодії.

Атаки типу «людина посередині» становлять особливу загрозу цілісності та конфіденційності обміну інформацією в піринговых мережах [27]. Щоб протидіяти подібним діям, система може динамічно змінювати маршрути передачі даних між вузлами, перенаправляючи трафік через альтернативні шляхи. Це ускладнює для зловмисника спроби несанкціонованого перехоплення або модифікації інформації, оскільки маршрути варіюються залежно від актуальних показників надійності та безпеки.

Сукупність механізмів протидії загрозам створюють багатоешелонний комплекс засобів для ефективного виявлення, локалізації та протидії атакам у піринговых мережах. Поєднання цих підходів сприяє зміцненню надійності, безпеки та стійкості децентралізованих середовищ у сучасних умовах динамічних кіберзагроз. Для посилення цих традиційних підходів доцільним є застосування моделі нульової довіри як доповнення до існуючих механізмів. На відміну від класичних методів, які передбачають певний рівень довіри між вузлами, модель нульової довіри підходить до кожного вузла та запиту як до потенційно небезпечного [28, 29]. Це означає постійну перевірку автентичності, моніторинг активності та обмеження доступу на основі принципу найменших привілеїв. Поєднання нульової довіри з механізмами реплікації даних, децентралізованим управлінням та автоматичним відновленням після збоїв значно підвищить стійкість піринговых мереж до внутрішніх і зовнішніх загроз.

Висновки

Пірингові мережі виступають перспективним елементом сучасних комунікаційних систем завдяки їхній децентралізованій архітектурі, стійкості до відмов та високій гнучкості у використанні. Однак забезпечення належного рівня безпеки даних у таких мережах потребує застосування комплексного підходу, що охоплює питання конфіденційності, цілісності та доступності інформаційних ресурсів.

Інтеграція криптографічних методів, використання геш-функцій, цифрових підписів, анонімізації, а також формування децентралізованих механізмів забезпечення доступності та гнучких систем виявлення й протидії атакам створює сталу основу для зміцнення безпеки піринговых мереж. Кожен з розглянутих підходів робить свій внесок у побудову надійних децентралізованих комунікацій, здатних протистояти сучасним загрозам та залишатися ефективними навіть у мінливих умовах мережевого середовища.

Подальший розвиток цього напряму досліджень має бути спрямований на оптимізацію існуючих технологій та створення нових алгоритмів, які враховуватимуть специфіку різних типів піринговых систем, особливості їх реалізації в реальних умовах та вимоги до продуктивності, масштабованості та витривалості до появи нових типів загроз. Таким чином, пошук збалансованих рішень у сфері захисту децентралізованих мереж залишається актуальним викликом, який потребує подальших міждисциплінарних досліджень та інноваційних підходів.

Література

1. Ansari M. S. A. Revisiting of peer-to-peer traffic: taxonomy, applications, identification techniques, new trends and challenges / Md Sarfaraj Alam Ansari, Kunwar Pal, Mahesh Chandra Govil // Knowledge and Information Systems. – 2023. DOI:10.1007/s10115-023-01915-5

2. Suryono R. R. Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review / Ryan Randy Suryono, Betty Purwandari, Indra Budi // Procedia Computer Science. – 2019. – Т. 161. – С. 204–214. DOI: 10.1016/j.procs.2019.11.116.

3. Md. Sadek Ferdous, Farida Chowdhury, та Md. Moniruzzaman. «A Taxonomy of Attack Methods on Peer-to-Peer Network» у *Proceedings of the 1st Indian Conference on Computational Intel-ligence and Information Security*,. – 2007. – С. 132-138.

4. Secure Communication in Peer-to-Peer Network Based on Trust-Based Model / Vijay Paul Singh [та ін.] // Studies in Computational Intelligence. – Singapore, 2022. – С. 157–170. DOI:10.1007/978-981-16-8012-0_13

5. Rahimi N. Security Consideration in Peer-to-peer Networks with A Case Study Application / Nick Rahimi // International Journal of Network Security & Its Applications. – 2020. – Т. 12, № 2. – С. 1–16. DOI:10.5121/ijnsa.2020.12201

6. Jawad M. Protecting Data Privacy in Structured P2P Networks / Mohamed Jawad, Patricia Serrano-Alvarado, Patrick Valduriez // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2009. – С. 85–98. DOI:10.1007/978-3-642-03715-3_8.

7. Privacy-Preserving P2P Information Sharing Protocol for Mobile Social Networks / Eric Ke Wang [та ін.] // International Journal of Computer and Communication Engineering. – 2013. – С. 338–342. – Режим доступу: DOI:10.7763/ijcce.2013.v2.200.

8. Survey of Anonymity and Authentication in P2P Networks / Xiaoliang Wang [та ін.] // Information Technology Journal. – 2010. – Т. 9, № 6. – С. 1165–1171. DOI:10.3923/itj.2010.1165.1171.

9. Jagdale B. N. A novel authentication and authorization scheme in P2P networking using location-based privacy / B. N. Jagdale, J. W. Bakal // Evolutionary Intelligence. – 2020. DOI:10.1007/s12065-020-00375-y.

10. Xu X. Defending Against sybil-attacks in Peer-to-Peer Networks / Xiang Xu, Huijuan Lu, Lianna Chen // International Journal of Security and Its Applications. – 2014. – Т. 8, № 4. – С. 329–340. DOI:10.14257/ijsia.2014.8.4.30.

11. A Peer-to-Peer Architecture for Detecting Attacks from Network Traffic and Log Data / Francesco Folino // 2017 International Conference on High Performance Computing & Simulation (HPCS), Генуя, Італія, 17–21 лип. 2017 р. DOI:10.1109/hpcs.2017.116.

12. Краліна Г. Шифрування: типи та алгоритми / Ганна Краліна, Нікіта Баков // Спеціалізовані та багатодисциплінарні наукові дослідження. 2020. DOI: 10.36074/11.12.2020.v2.36

13. Технології анонімних мереж / Б. М. Гавриш [та ін.] // Наукові записки (Українська академія друкарства). – 2022. – Т. 2, № 65. – С. 42–56. DOI: 10.32403/1998-6912-2022-2-65-42

14. Anonymous and Distributed Authentication for Peer-to-Peer Networks / Pasan Tennakoon at el/ // Journal of Computer Science. – 2023. – Т. 19, № 1. – С. 1–10. DOI:10.3844/jcssp.2023.1.10.

15. Криптографічні хеш-функції [Електронний ресурс] // Львівський національний університет. – Режим доступу: https://ami.lnu.edu.ua/wp-content/uploads/2022/06/Cryptology9.pdf.

16. Standardizations and considerations on P2P-based contents distribution for digital signage service / Wook Hyun [та ін.] // 2015 17th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang, South Korea, 1–3 лип. 2015 р. – 2015. DOI: 10.1109/icact.2015.7224846.

17. Ray B. Extending the Blockchain: Ensuring Transactional Integrity in Relational Data via Blockchain Technology / Brian Ray. Office of Scientific and Technical Information (OSTI), 2019. DOI:10.2172/1557484

18. Ferrag M. A. The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial / Mohamed Amine Ferrag, Lei Shu // IEEE Internet of Things Journal. – 2021. – Т. 8, № 24. – С. 17236 - 17260. DOI:10.1109/jiot.2021.3078072

19. Distributed caching in unstructured peer-to-peer file sharing networks / Guoqiang Gao [та ін.] // Computers & Electrical Engineering. – 2014. – Т. 40, № 2. – С. 688–703. DOI:10.1016/j.compeleceng.2013.12.001.

20. Герасименко О. Ю. Децентралізоване управління ресурсами захищеної розподіленої комп'ютерної системи на базі мережоцентричного підходу [Електронний ресурс] : – Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/5124.

21. Lam S. S. Failure recovery for structured p2p networks: Protocol design and performance under churn / Simon S. Lam, Huaiyu Liu // Computer Networks. – 2006. – Т. 50, № 16. – С. 3083–3104. DOI:10.1016/j.comnet.2005.12.009.

22. Gao G. Collaborative Caching in P2P Streaming Networks / Guoqiang Gao, Ruixuan Li // Journal of Network and Systems Management. – 2019. – Т. 27, № 3. – С. 815–836. DOI:10.1007/s10922-018-09485-6

23. Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks / Yan Li [та ін.] // International Journal of Robust and Nonlinear Control. – 2021. – Т. 32, № 3. – С. 1633–1653. DOI:10.1002/rnc.5899

24. Gheorghe G. Security and privacy issues in P2P streaming systems: A survey / Gabriela Gheorghe, Renato Lo Cigno, Alberto Montresor // Peer-to-Peer Networking and Applications. – 2010. – Т. 4, № 2. – С. 75–91.

– Режим доступу: DOI:10.1007/s12083-010-0070-6.

25. Chenfeng Vincent Zhou S. K. A Peer-to-Peer Collaborative Intrusion Detection System / Shanika Karunasekera Chenfeng Vincent Zhou // 2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic, Kuala Lumpur, Malaysia. DOI:10.1109/icon.2005.1635451.

26. Liang J. Efficient Blacklisting and Pollution-Level Estimation in P2P File-Sharing / Jian Liang, Naoum Naoumov, Keith W. Ross // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2005. – С. 1–21. DOI:10.1007/11599593_1.

27. Linnolahti J. QoS routing for P2P networking [Електронний ресурс] . – Режим доступу: http://www.cse.hut.fi/fi/opinnot/T-110.5190/2004/papers/Linnolahti.pdf.

28. Alevizos L. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review / Lampis Alevizos, Vinh Thong Ta, Max Hashem Eiza // SECURITY AND PRIVACY. – 2021. – Т. 5, № 1. DOI:10.1002/spy2.191.

29. Zero Trust Architecture. Official edition. [Електронний ресурс] : – Режим доступу: https://doi.org/10.6028/NIST.SP.800-207.

References

1. Ansari M. S. A. Revisiting of peer-to-peer traffic: taxonomy, applications, identification techniques, new trends and challenges / Md Sarfaraj Alam Ansari, Kunwar Pal, Mahesh Chandra Govil // Knowledge and Information Systems. – 2023. DOI:10.1007/s10115-023-01915-5.
2. Suryono R. R. Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review / Ryan Randy Suryono, Betty Purwandari, Indra Budi // Procedia Computer Science. – 2019. – Vol. 161. – P. 204–214. DOI:10.1016/j.procs.2019.11.116.
3. Md. Sadek Ferdous, Farida Chowdhury, та Md. Moniruzzaman. «A Taxonomy of Attack Methods on Peer-to-Peer Network» in *Proceedings of the 1st Indian Conference on Computational Intel-ligence and Information Security*, India. – 2007. – P. 132-138.
4. Secure Communication in Peer-to-Peer Network Based on Trust-Based Model / Vijay Paul Singh [et al.] // Studies in Computational Intelligence. – Singapore, 2022. – P. 157–170. DOI:10.1007/978-981-16-8012-0_13
5. Rahimi N. Security Consideration in Peer-to-peer Networks with A Case Study Application / Nick Rahimi // International Journal of Network Security & Its Applications. – 2020. – Vol. 12, no. 2. – P. 1–16. DOI:10.5121/ijnsa.2020.12201
6. Jawad M. Protecting Data Privacy in Structured P2P Networks / Mohamed Jawad, Patricia Serrano-Alvarado, Patrick Valduriez // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2009. – P. 85–98. DOI:10.1007/978-3-642-03715-3_8.
7. Privacy-Preserving P2P Information Sharing Protocol for Mobile Social Networks / Eric Ke Wang [et al.] // International Journal of Computer and Communication Engineering. – 2013. – P. 338–342. DOI:10.7763/ijcce.2013.v2.200.
8. Survey of Anonymity and Authentication in P2P Networks / Xiaoliang Wang [et al.] // Information Technology Journal. – 2010. – Vol. 9, no. 6. – P. 1165–1171. DOI:10.3923/itj.2010.1165.1171.
9. Jagdale B. N. A novel authentication and authorization scheme in P2P networking using location-based privacy / B. N. Jagdale, J. W. Bakal // Evolutionary Intelligence. – 2020. DOI:10.1007/s12065-020-00375-y.
10. Xu X. Defending Against sybil-attacks in Peer-to-Peer Networks / Xiang Xu, Huijuan Lu, Lianna Chen // International Journal of Security and Its Applications. – 2014. – Vol. 8, no. 4. – P. 329–340. DOI:10.14257/ijsia.2014.8.4.30.
11. A Peer-to-Peer Architecture for Detecting Attacks from Network Traffic and Log Data / Francesco Folino [et al.] // 2017 International Conference on High Performance Computing & Simulation (HPCS), Genoa, Italy, 17–21 July 2017. DOI:10.1109/hpcs.2017.116.
12. Kralina G. Encryption: types and algorithms / Anna Kralina, Nikita Bakov // Specialized and multidisciplinary scientific researches. – 2020. DOI:10.36074/11.12.2020.v2.36.
13. Technology of anonymous networks / B. M. Havrysh [et al.] // Scientific Papers (Ukrainian Academy of Printing). – 2022. – Vol. 2, no. 65. – P. 42–56. DOI:10.32403/1998-6912-2022-2-65-42-56.
14. Anonymous and Distributed Authentication for Peer-to-Peer Networks / Pasan Tennakoon [et al.] // Journal of Computer Science. – 2023. – Vol. 19, no. 1. – P. 1–10. DOI:10.3844/jcssp.2023.1.10.
15. Cryptographic hash functions [Electronic resource] // Lviv National University. – Mode of access: https://ami.lnu.edu.ua/wp-content/uploads/2022/06/Cryptology9.pdf.
16. Standardizations and considerations on P2P-based contents distribution for digital signage service / Wook Hyun [et al.] // 2015 17th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang, South Korea, 1–3 July 2015. DOI:10.1109/icact.2015.7224846.
17. Ray B. Extending the Blockchain: Ensuring Transactional Integrity in Relational Data via Blockchain Technology / Brian Ray. Office of Scientific and Technical Information (OSTI), 2019. DOI:10.2172/1557484.
18. Ferrag M. A. The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial / Mohamed Amine Ferrag, Lei Shu // IEEE Internet of Things Journal. – 2021. – Vol. 8, no. 24. – P. 17236 - 17260. DOI:10.1109/jiot.2021.3078072.
19. Distributed caching in unstructured peer-to-peer file sharing networks / Guoqiang Gao [et al.] // Computers & Electrical Engineering. – 2014. – Vol. 40, no. 2. – P. 688–703. DOI:10.1016/j.compeleceng.2013.12.001.
20. Gerasimenko O. U. Decentralized resource management of a protected distributed computer system based on a network-centric approach [Electronic resource]: Mode of access: http://dspace.kntu.kr.ua/jspui/handle/ 123456789/5124.
21. Lam S. S. Failure recovery for structured p2p networks: Protocol design and performance under churn / Simon S. Lam, Huaiyu Liu // Computer Networks. – 2006. – Vol. 50, no. 16. – P. 3083–3104. DOI:10.1016/j.comnet.2005.12.009.
22. Gao G. Collaborative Caching in P2P Streaming Networks / Guoqiang Gao, Ruixuan Li // Journal of Network and Systems Management. – 2019. – Vol. 27, no. 3. – P. 815–836. DOI:10.1007/s10922-018-09485-6.
23. Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks / Yan Li [et al.] // International Journal of Robust and Nonlinear Control. – 2021. – Vol. 32, no. 3. – P. 1633–1653. DOI:10.1002/rnc.5899.
24. Gheorghe G. Security and privacy issues in P2P streaming systems: A survey / Gabriela Gheorghe, Renato Lo Cigno, Alberto Montresor // Peer-to-Peer Networking and Applications. – 2010. – Vol. 4, no. 2. – P. 75–91. DOI:10.1007/s12083-010-0070-6.
25. Chenfeng Vincent Zhou S. K. A Peer-to-Peer Collaborative Intrusion Detection System / Shanika Karunasekera Chenfeng Vincent Zhou // 2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic, Kuala Lumpur, Malaysia. DOI:10.1109/icon.2005.1635451.
26. Liang J. Efficient Blacklisting and Pollution-Level Estimation in P2P File-Sharing Systems / Jian Liang, Naoum Naoumov, Keith W. Ross // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2005. – P. 1–21. DOI:10.1007/11599593_1.
27. Linnolahti J. QoS routing for P2P networking [Electronic resource] / Janne Linnolahti // TKK - Tietotekniikan laitos. – Mode of access: http://www.cse.hut.fi/fi/opinnot/T-110.5190/2004/papers/Linnolahti.pdf .
28. Alevizos L. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review / Lampis Alevizos, Vinh Thong Ta, Max Hashem Eiza // SECURITY AND PRIVACY. – 2021. – Vol. 5, no. 1. DOI:10.1002/spy2.191.
29. Zero Trust Architecture. Official edition. [Electronic resource]: Mode of access: https://doi.org/10.6028/NIST.SP.800-207.