https://doi.org/10.31891/2219-9365-2024-79-31
УДК 004.056

КУПЕРШТЕЙН Леонід
Вінницький національний технічний університет
https://orcid.org/0000-0001-6737-7134
kupershtein.lm@gmail.com
КРЕНЦІН Михайло
Вінницький національний технічний університет
https://orcid.org/0000-0002-1792-9401
e-mail: mishatron98@gmail.com

МОДЕЛЬ НУЛЬОВОЇ ДОВІРИ ДЛЯ ГІБРИДНОЇ ПІРИНГОВОЇ МЕРЕЖІ

У статті запропоновано вдосконалену модель нульової довіри для гібридних пірингових мереж, яка враховує динамічність і розподіленість їхньої архітектури. Модель реалізує принципи повної перевірки запитів, найменшого доступу, ізоляції сегментів, постійного моніторингу активності вузлів і захисту даних через шифрування та сегментацію. Запропоновані механізми короткочасних довірених зон забезпечують гнучкість і продуктивність без порушення принципів нульової довіри. Особлива увага приділена самоізоляції вузлів для реагування на загрози, що дозволяє локалізувати інциденти безпеки.

Ключові слова: пірингова мережа, нульова довіра, кіберзагроза, атака, автентифікація, моніторинг, довірена зона, самоізоляція.

.

KUPERSHTEIN Leonid, KRENTSIN Mykhailo
Vinnytsia National Technical University

THE MODEL OF ZERO TRUST FOR HYBRID PEER-TO-PEER NETWORK

In the article an advanced Zero Trust model for hybrid peer-to-peer networks that combine centralized and decentralized management mechanisms was presented. The study addresses the critical need for enhanced security in such networks, characterized by dynamic architectures, the absence of a single control center, heterogeneity of nodes, and increased risks of unauthorized access. Traditional perimeter-based security approaches are insufficient for environments with blurred network boundaries and highly dynamic participants. The proposed model integrates the fundamental principles of the Zero Trust concept, including comprehensive verification of all requests, the principle of least privilege, network segment isolation, continuous activity monitoring, and data security assurance. Authentication and authorization mechanisms ensure the verification of every request, irrespective of its origin or prior interactions. The introduction of short-term trusted zones achieves a balance between increased network performance and strict security requirements by allowing nodes to interact temporarily within protected subnets with minimal latency. A novel approach to data segmentation and the use of diverse encryption algorithms enhances the confidentiality and integrity of information. Special attention is given to the development of self-isolation mechanisms for nodes, enabling rapid responses to potential threats such as DDoS attacks, phishing, or data breaches. These mechanisms localize security incidents and prevent their propagation to other network segments. Additionally, the proposed access control model accounts for the specific characteristics of hybrid P2P architectures, ensuring the protection of nodes and resources from malicious attacks

Keywords: peer-to-peer network, zero trust, cyber threat, attack, authentication, monitoring, trusted zone, self-isolation.

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

Сучасний розвиток інформаційно-комунікаційних технологій та зростання масштабів розподілених обчислювальних інфраструктур сприяють поширенню пірингових (P2P) мереж, які набувають дедалі більшого значення в галузі передачі даних, обміну інформацією та забезпечення розподілених обчислень [1-3]. При цьому гібридні пірингові мережі, що поєднують централізовані та децентралізовані механізми управління, наразі розглядаються як оптимальна архітектурна модель для досягнення більшої ефективності, масштабованості та стійкості до відмов [4, 5]. Їхня актуальність зумовлена здатністю забезпечувати динамічний обмін даними без централізованого контролю, зберігаючи при цьому переваги керованого пошуку та маршрутизації.

У гібридних мережах частина функцій може виконуватися централізованими вузлами (наприклад, сервери для аутентифікації або зберігання даних), тоді як передача даних і взаємодія між користувачами здійснюється через пірингові з'єднання [6, 7]. Така архітектура дозволяє забезпечити масштабованість і ефективність, але створює додаткові точки уразливості, пов'язані з центральними вузлами. У гібридних мережах вузли виконують різноманітні функції: вони можуть бути джерелами даних, ретрансляторами, або кінцевими споживачами. Така гнучкість ускладнює застосування статичних політик безпеки. Дані передаються через кілька проміжних вузлів, що збільшує ризик перехоплення або модифікації інформації [8]. Гібридна архітектура вимагає комплексного шифрування як для транспортного рівня, так і для самих даних. Вузли можуть постійно підключатися або відключатися, а маршрути передачі даних змінюються в реальному часі. Це унеможливлює використання статичних підходів до управління доступом та ідентифікацією загроз.

Однак зростання розміру, складності та різнорідності учасників гібридних пірингових мереж загострює питання безпеки та довіри. Традиційні підходи, орієнтовані на периметрову безпеку, стають неефективними у середовищі, де границі мереж розмиті, а учасники можуть бути потенційно недостовірними. Тут концепція нульової довіри (Zero Trust) набуває особливої ваги. Основна принципова ідея полягає у тому, що жоден елемент мережі не може розглядатися як надійний за замовчуванням, а доступ надається виключно на основі перевірених довірчих відносин та постійного моніторингу поведінки [9].

Враховуючи складну природу гібридних мережевих технологій, що поєднують розподілених та централізованих учасників різного рівня надійності, виникає завдання формування підходів, які б дозволяли динамічно ідентифікувати та підтверджувати довіру до кожного вузла, аналізувати його поведінку та мінімізувати ризики несанкціонованого доступу чи шкідливої активності. Вирішення цього завдання є важливим, оскільки потребує створення нових підходів до безпеки в динамічних та розподілених середовищах для підвищення захищеності сервісів, де гібридні пірингові архітектури відіграють ключову роль [10].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розробка вдосконаленої моделі нульової довіри для гібридних пірингових мереж, що враховує специфіку їхньої динамічної та розподіленої архітектури. Оскільки класичні моделі безпеки, побудовані на концепції периметрового захисту, не здатні ефективно захищати гібридні мережі через відсутність централізованого контролю та обмеженість виявлення внутрішніх і зовнішніх загроз, виникає необхідність застосування нових підходів до забезпечення безпеки.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ

Модель Zero Trust (модель нульової довіри, МНД) є підходом до безпеки, що передбачає відсутність довіри до жодного запиту чи пристрою, які намагаються отримати доступ до мережі або ресурсів за замовчуванням [11]. У контексті пірингової мережі це означає, що жоден вузол не повинен автоматично надавати доступ до ресурсів чи відповідати на запити іншого вузла. Основна ідея цієї моделі полягає в тому, що кожен запит на доступ до мережевих ресурсів має бути перевірений і авторизований до надання доступу, незалежно від того, з якої підмережі він надходить. Ідею нульової довіри сформулював один з перших експертів, Джон Кіндерваг [12].

Реалізація моделі Zero Trust зокрема для децентралізованої мережі може захистити користувачів від атак типу «Людина посередині», вимагаючи автентифікації перед доступом до ресурсів. Також такий підхід може і допомогти захиститися від фішингових атак за рахунок навчання користувачів розпізнавати і уникати підозрілих повідомлень та файлів. Концепція Zero Trust забезпечує захист від DDoS-атак завдяки обмеженню доступу, мікросегментації та аналізу трафіку, а також від атаки Сивілли за рахунок автентифікації та систему репутації. Крім того, практична імплементація моделі може допомагати боротися з атакою «Викрадення сутності» завдяки багатофакторній автентифікації та контролю доступу, а також із атакою «Затемнення» через шифрування та аналітику трафіку. Нульова довіра може бути ефективним захистом від атаки «Забруднення індексу» завдяки автентифікації і контролю доступу, а також забезпечити захист і від інших кіберзагроз в залежності від внутрішнього та зовнішнього середовища мережі.

Основні принципи МНД можна представити так [13, 14]:

- Ніколи не довіряти, завжди перевіряти. Будь-який запит на доступ до ресурсів мережі має бути перевірений, автентифікований та авторизований перед наданням доступу. Zero Trust перевіряє ідентичність та привілеї користувача, а також перевіряє ідентифікацію і безпеку пристрою.
- Принцип найменшого доступу. Вузлу надається лише мінімальний рівень доступу до ресурсів, необхідний для виконання його завдань.
- Принцип ізоляції мережі. Мережеві сегменти та ресурси ізолюються один від одного за допомогою сегментації мережі та застосування мережевих фаєрволів і інших захисних механізмів.
- Модель Zero Trust передбачає постійний моніторинг та перевірку всіх дій і запитів у мережі для виявлення аномальних активностей або вторгнень.
- Безпека на рівні даних. Захист даних здійснюється за допомогою шифрування, маскування та інших методів для забезпечення конфіденційності.

Можна виділити такі переваги застосування концепції Zero Trust у піринговій мережі [15, 16]:

- підвищення захисту мережі від різноманітних атак, як загальних, так і специфічних для пірингових мереж.
- зниження ризиків порушення безпеки, обмежуючи доступ до ресурсів лише тим користувачам, яким це справді необхідно.
- забезпечення прозорості мережі для відстеження транзакцій та доступу до ресурсів.

Окремі елементи концепції нульової довіри реалізовано в деяких децентралізованих застосунках:

- децентралізовані фінансові системи (DeFi). Блокчейн-мережі, такі як Bitcoin та Ethereum, використовують модель нульової довіри для забезпечення безпеки своїх мереж [17, 18] за рахунок підтвердження кожної транзакції:
- P2P-мережі для обміну файлами. Деякі P2P-мережі для обміну файлами, такі як BitTorrent, використовують модель нульової довіри для захисту своїх мереж від атак [19];
- децентралізовані соціальні мережі. Такі платформи, як Mastodon та Diaspora, використовують Zero Trust для забезпечення безпеки даних користувачів. Кожен вузол мережі повинен пройти автентифікацію, а користувачі мають контроль над своїми даними і підтверджують кожну взаємодію [20].

АДАПТАЦІЯ ПРИНЦИПІВ НУЛЬОВОЇ ДОВІРИ ДО ГІБРИДНОЇ ПІРИНГОВОЇ МЕРЕЖІ

Для забезпечення найбільш ефективного захисту мережі важливим є реалізація усіх основних принципів нульової довіри. Далі представимо кожен із принципів нульової довіри в контексті децентралізованої пірингової імплементації, який далі можна адаптувати в залежності від практичної реалізації.

1. Ніколи не довіряти, завжди перевіряти. В контексті гібридної пірингової мережі пропонується взаємна автентифікації $AUTH$ вузлів, адже лише взаємно-автентифіковані вузли повинні мати змогу здійснювати комунікацію у P2P мережі. Крім того, повинна бути забезпечена первинна автентифікація вузла на сервері, який може виконувати ряд сервісних функцій, зокрема саму автентифікацію, ініціалізацію з'єднань, моніторинг безпеки та поведінки, вирішення конфліктів тощо. Також передбачається авторизація $ATHR$ кожної подальшої транзакції T незалежно від попередньої взаємодії вузла. Нехай є дані D над якими необхідно здійснити операцію обміну O між вузлами A_i та A_j. Тоді транзакцію в пірінговій мережі можна представити таким чином:

$$T = O(A_i, A_j, D),$$

При кожному запиті REQ вузол повинен пройти поточну автентифікацію:

$$AR = AUTH(PRM_{auth}, REQ)$$

де PRM_{auth} – параметри автентифікації, а

$$AR = \begin{cases} 1, \text{якщо вузол автентифікований} \\ 0, \text{якщо вузол не автентифікований} \end{cases}.$$

Беручи до уваги необхідність авторизації кожної транзакції маємо результат транзакції:

$$TR = ATHR(PRM_{athr}, T),$$

де PRM_{athr} – параметри авторизації, а

$$TR = \begin{cases} 1, \text{якщо авторизація успішна} \\ 0, \text{якщо авторизація неуспішна} \end{cases}.$$

Для вирішення певних короткострокових завдань, що потребує мінімальних затримок при обміні даними пропонується створювати довірені зони TZ. Це забезпечує гнучкість, коли вузли можуть тимчасово працювати в ізольованих підмережах з високим рівнем довіри, а після завершення роботи або через певний граничний час t_{tz} автоматично розпадатися. Кожен вузол повинен сам визначати коли і з ким створювати довірені зони. Спрощена автентифікація у довіреній зоні досягається за рахунок спеціального токену t_{zb}, який генерується вузлом, що ініціює створення довіренох зони. Цей токен надсилається при кожному запиті та дозволяє не здійснювати поточну автентифікацію $AUTH$ та авторизацію запиту $ATHR$, натомість буде здійснюватись спрощена автентифікація $AUTH'$ та авторизацію запиту $ATHR'$. Токен t_{zb} містить в собі час t_{tz}, аби кожен вузол у довіреній зоні міг припинити вчасно існування цієї зони. Формально, довірена зона представляється наступним виразом:

$$TZ = \{t_{zb}, t_{tz}, AUTH', ATHR'\}.$$

2. Принцип найменшого доступу. Зазвичай пірингові мережі за своєю структурою порушують принцип найменшого доступу, оскільки у P2P мережі всі вузли повинні бути рівні. Проте, пропонується модель контролю доступу CAM, яка дозволить забезпечувати захист ресурсів R та вузлів A від несанкціонованого доступу та атак зловмисників. Модель контролю доступу повинна передбачати

використання токенів T (для здійснення авторизації транзакцій), захищений обмін ключами SKE, валідацію ідентифікаторів VID. В результаті маємо:

$$CAM = \{R, A, T, SKE, VID\}.$$

3. Принцип ізоляції мережі. Цей принцип є досить важливим для захищеності пірингової мережі. Саме тому передбачається розробка моделі P2P мережі таким чином, аби вона була сегментована. Тобто мережа N повинна бути розбита на так звані підмережі:

$$N = \{SN_1, SN_2, \dots, SN_p\},$$

де $p \in [1; \infty)$ - номер підмережі. Кожна SN з яких має бути ізольована одна від одної до тих пір, поки немає необхідності їх об'єднання. Також сама підмережа не повинна представляти собою повнозв'язну топологію, оскільки вузли, що не здійснили взаємну автентифікацію також повинні бути ізольовані від комунікації один з одним. У випадку, коли кожен вузол здійснив взаємну автентифікацію з кожним іншим, то така підмережа буде представлена у вигляді повнозв'язної топології.

4. Постійна перевірка і контроль. Аби забезпечити максимальну захищеність піринговой мережі, модель Zero Trust передбачає моніторинг та перевірку дій вузла. У децентралізованих мережах складніше виявляти аномальну поведінку та контролювати дії вузлів, оскільки немає єдиного довіреного джерела, що буде здійснювати відповідний моніторинг. Проте, передбачається ведення чорних списків BL та виявлення аномальної поведінки UB на достатньому рівні. Кожен вузол повинен вести моніторинг запитів AM, що до нього надходять і у разі виявлення аномальної поведінки певного вузла, його буде додано у чорний список. А сам список буде надіслано всім вузлам підмережі для забезпечення захищеності та стабільності роботи всієї підмережі.

$$BL = \{AM, UB, SL\},$$

де SL – функція надсилання чорного списку іншим вузлам.

Пропонується також впровадити у кожний вузол механізм самоізоляції SI. Атаки на вузол піринговой мережі можна розділити за ознакою наслідків на такі категорії, як:

- атаки на продуктивність та доступність вузла (наприклад, DDoS, переповнення запитів, затемнення тощо). Наприклад, у випадку здійснення DDoS атаки на вузол, продуктивність вузла зменшується, оскільки частина ресурсів спрямована на обробку шкідливих запитів.
- атаки на конфіденційність та цілісність даних (наприклад, людина посередині, викрадення сутності, забруднення індексу, підслуховування). Такі атаки спрямовані на отримання або пошкодження конфіденційних даних.
- атаки на маніпулювання мережею (наприклад, маскарад, раціональна атака, атака Сивілли). Такі атаки дозволяють маніпулювати маршрутизацією чи даними у мережі.

Самоізоляція вузла дозволяє забезпечити швидке реагування на загрози та зменшить ризик поширення атаки по всій мережі. Таким чином, для кожного з вищеперерахованих типів атак самоізоляція дозволить забезпечити продуктивність вузла (якщо вузол не буде зайнятий обробкою шкідливих запитів, то зможе продовжити поточну роботу), конфіденційність даних (якщо вузол самоізолюється, то він зможе обмежити витік конфіденційних даних), виявлення та реагування на загрози з подальшим відновленням роботи вузла.

Додатково самоізоляція дозволяє виявити та усунути внутрішні помилки та провести оновлення за потреби. Вихід із самоізоляції може бути забезпечений двома шляхами:

а) у випадку внутрішньої проблеми InP, вузол може вийти з самоізоляції після усунення проблеми $Fix(InP)$ (наприклад, оновлення програмного забезпечення), де Fix – функція усунення проблеми.

б) якщо проблема зовнішня $OutP$ (наприклад, DDoS), то необхідно з певною періодичністю t_p припиняти самоіляцію та аналізувати трафік далі. Якщо ж шкідлива активність продовжується, то вузол далі продовжує процес самоізоляції. t_p пропонується збільшувати за геометричною прогресією (такий підхід зменшує кількість спроб виходу з ізоляції та є найпростішим з точки зору реалізації).

Виходячи із вищеописаного, функція самоізоляції формалізується наступними параметрами:

$$SI = \{InP, Fix, OutP, t_p\}.$$

5. Безпека на рівні даних. На сьогоднішній день захищеність даних є одним із найголовніших завдань будь-якого програмного забезпечення, адже цілісність, конфіденційність та доступність даних не повинна бути порушена. Саме тому жоден з видів даних, що зберігаються або передаються, не повинен

знаходитись у незашифрованому вигляді. Саме тому передбачається сегментацію даних DS вузла та використання різних алгоритмів шифрування EA у різних сегментах. Тобто, навіть якщо частина даних DS_i вузла буде скомпрометована, то це ніяк не вплине на інші дані. Процес обміну даними DE між вузлами теж повинен бути захищеним, як на транспортному рівні, так і на прикладному. Тоді захищеність даних пірингової мережі представимо таким чином:

$$DSEC = \{DS, EA, DE\}.$$

Розбиття даних на сегменти повинно передбачати розділення на логічні сегменти відповідно до частоти використання певних даних та необхідності забезпечення достатнього рівня конфіденційності, адже, наприклад, дані, які треба використовувати дуже часто, повинні бути зашифровані таким алгоритмом, який забезпечує максимальну швидкодію, а дані, які є конфіденційними, повинні шифруватись алгоритмом, що забезпечує достатній рівень криптостійкості.

Виходячи із вищеописаного, модель нульової довіри піринговой мережі ZTM можна представити таким чином:

$$ZTM = \{AR, TR, TZ\ CAM, SN, BL, DSEC\}.$$

Графічне представлення структурних елементів моделі нульової довіри для піринговой мережі наведено на рис. 1.

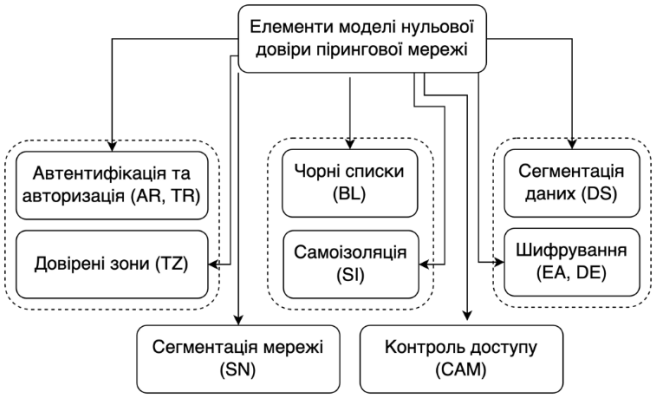

Рис. 1 Елементи моделі нульової довіри

Запропоновані механізми в моделі нульової довіри дозволяють забезпечити захищеність піринговой мережі за рахунок імплементації безпеки на всіх рівнях. Кожен запит вузла на доступ розглядається як потенційно небезпечний і підлягає перевірці, що дозволяє мінімізувати ризики потенційних атак. Запропоновані механізми автентифікації та авторизації, створення короткострокових довірених зон, контроль доступу, сегментація мережі, а також постійний моніторинг та самоізоляція вузлів сприяють підвищенню загального рівня безпеки мережі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У цьому дослідженні було запропоновано модель нульової довіри для піринговой мережі, яка враховує специфіку її динамічної та розподіленої архітектури. Модель передбачає використання механізмів автентифікації та авторизації для забезпечення захищеності транзакцій, впровадження короткочасних довірених зон для підвищення продуктивності мережі, а також реалізацію принципів ізоляції вузлів і сегментації мережі. Особливу увагу приділено постійному моніторингу активності вузлів для виявлення аномальної поведінки та самоізоляції в разі загрози, що дозволяє підвищити рівень безпеки всієї мережі. Крім того, безпека даних забезпечується через шифрування та логічну сегментацію, що знижує ризики компрометації інформації. Запропонована модель сприяє зменшенню ризиків атак та покращенню загальної стійкості мережі.

Подальші дослідження будуть спрямовані на оптимізацію використання ресурсів у межах довірених зон, інтеграцію запропонованої моделі з технологіями штучного інтелекту для автоматичного виявлення загроз, а також оцінку її ефективності в реальних умовах. Особливий інтерес становить адаптація моделі до сучасних технологій, таких як блокчейн та IoT, що дозволить покращити безпеку та масштабованість мереж.

Література

1. The Future of the P2P Model. URL: https://www.linkedin.com/pulse/future-p2p-model-key-trends-statistics-shaping-different-industries.
2. Куперштейн Л.М., Кренцін М.Д. Аналіз тенденцій розвитку пірингових мереж. *Вісник ХНУ. Технічні науки*. 2021. Т. 299, №4. С. 26–29. URL: https://doi.org/10.31891/2307-5732-2021-299-4-26-29.
3. Peer-to-Peer Applications: The Future of Networking. URL: https://www.cisin.com/coffee-break/what-is-the-future-of-peer-to-peer-applications.html.
4. Hybrid Client/Server Peer to Peer Multitier Video Streaming / I. M. Ibrahim et al. 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 25–26 July 2021. 2021. URL: https://doi.org/10.1109/aca52198.2021.9626808.
5. Wu L., Lu W., Chen C. Strengths and weaknesses of client-server and peer-to-peer network models in construction projects. International Journal of Construction Management. 2023. P. 1–15. URL: https://doi.org/10.1080/15623599.2023.2185950 .
6. He Z., Kleinrock L. Optimization of Assisted Search Over Server-Mediated Peer-to-peer NetworksG / *LOBECOM 2022 - 2022 IEEE Global Communications Conference*. 2022. P. 4928-4934. DOI: 10.1109/GLOBECOM48099.2022.10000846.
7. WebRTC.Getting started with peer connections. URL: https://webrtc.org/getting-started/peer-connections
8. Куперштейн Л.М., Кренцін М.Д., Дудатьєв А.В., Каплун В.А. Аналіз проблем безпеки пірінгових мереж. *Інформаційні технології та комп'ютерна інженерія*. 2022. Т. 54, № 2. С. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.
9. Zero Trust Architecture. Official edition. URL: https://doi.org/10.6028/NIST.SP.800-207.
10. Peer-to-Peer (P2P) Service: Definition, Facts, and Examples. URL: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp.
11. Zero Trust Security. Encryption Consulting. URL: https://www.encryptionconsulting.com/education-center/zero-trust-security.
12. Theory and Application of Zero Trust Security: A Brief Survey / H. Kang et al. Entropy. 2023. Vol. 25, no. 12. P. 1595. URL: https://doi.org/10.3390/e25121595
13. Prydybailo O. B. Zero trust architecture: the basics organization principles. Connectivity. 2022. Vol. 159, no. 5. URL: https://doi.org/10.31673/2412-9070.2022.051620.
14. Zero Trust | Steps to create a Zero Trust Security System». AppViewX. URL: https://www.appviewx.com/education-center/zero-trust-security.
15. Від нуля до переможця: як безпека нульової довіри може врятувати вашу мережу. InfoTel. URL: https://infotel.ua/news/ot-nulya-k-pobeditelyu-kak-bezopasnost-nulevogo-doveriya-mozhet-spasti-vashu-set.
16. Holmes D. The Definition Of Modern Zero Trust / Forrester, 24 January 2022. URL: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust.
17. What is Zero-Trust Architecture? A Guide to Blockchain Security». BeInCrypto. URL: https://beincrypto.com/learn/zero-trust-architecture-guide.
18. Blockchain-based Zero Trust Cybersecurity in the Internet of Things / S. Li et al. *ACM Transactions on Internet Technology*. 2023. Vol. 23, no. 3. P. 1–3. URL: https://doi.org/10.1145/3594535
19. BitTorrent File System (BTFS) | Scalable Decentralized File Storage. URL: https://www.bittorrent.com/token/bittorrent-file-system.
20. De Salve A., Mori P., Ricci L., Di Pietro R. Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions. *Computer Communications*, 2023. P. 199–225. URL: https://doi.org/10.1016/j.comcom.2023.02.023.

References

1. The Future of the P2P Model. URL: https://www.linkedin.com/pulse/future-p2p-model-key-trends-statistics-shaping-different-industries.
2. Kupershtein L., Krentsin M. Analysis of peer-to-peer networks trends. *Herald of khmelnytskyi national university*. 2021. Vol. 299, no. 4. P. 26–29. URL: https://doi.org/10.31891/2307-5732-2021-299-4-26-29. URL: https://doi.org/10.31891/2307-5732-2021-299-4-26-29.
3. Peer-to-Peer Applications: The Future of Networking. URL: https://www.cisin.com/coffee-break/what-is-the-future-of-peer-to-peer-applications.html.
4. Hybrid Client/Server Peer to Peer Multitier Video Streaming / I. M. Ibrahim et al. 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 25–26 July 2021. 2021. URL: https://doi.org/10.1109/aca52198.2021.9626808.
5. Wu L., Lu W., Chen C. Strengths and weaknesses of client-server and peer-to-peer network models in construction projects. International Journal of Construction Management. 2023. P. 1–15. URL: https://doi.org/10.1080/15623599.2023.2185950 .
6. He Z., Kleinrock L. Optimization of Assisted Search Over Server-Mediated Peer-to-peer NetworksG / *LOBECOM 2022 - 2022 IEEE Global Communications Conference*. 2022. P. 4928-4934. DOI: 10.1109/GLOBECOM48099.2022.10000846.
7. WebRTC.Getting started with peer connections. URL: https://webrtc.org/getting-started/peer-connections
8. Kupershtein L., Krentsin M. et al. Analysis of security problems of peer-to-peer networks. Information technology and computer engineering. 2022. Vol. 54, № 2. P. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.

9. Zero Trust Architecture. Official edition. URL: https://doi.org/10.6028/NIST.SP.800-207.
10. Peer-to-Peer (P2P) Service: Definition, Facts, and Examples. URL: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp.
11. Zero Trust Security. Encryption Consulting. URL: https://www.encryptionconsulting.com/education-center/zero-trust-security.
12. Theory and Application of Zero Trust Security: A Brief Survey / H. Kang et al. Entropy. 2023. Vol. 25, no. 12. P. 1595. URL: https://doi.org/10.3390/e25121595.
13. Prydybailo O. B. Zero trust architecture: the basics organization principles. Connectivity. 2022. Vol. 159, no. 5. URL: https://doi.org/10.31673/2412-9070.2022.051620.
14. Zero Trust | Steps to create a Zero Trust Security System». AppViewX. URL: https://www.appviewx.com/education-center/zero-trust-security
15. Vid nulia do peremozhtsia: yak bezpeka nulovoi doviry mozhe vriatuvaty vashu merezhu. InfoTel. URL: https://infotel.ua/news/ot-nulya-k-pobeditelyu-kak-bezopasnost-nulevogo-doveriya-mozhet-spasti-vashu-set.
16. Holmes D. The Definition Of Modern Zero Trust / Forrester, 24 January 2022. URL: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust.
17. What is Zero-Trust Architecture? A Guide to Blockchain Security». BeInCrypto. URL: https://beincrypto.com/learn/zero-trust-architecture-guide.
18. Blockchain-based Zero Trust Cybersecurity in the Internet of Things / S. Li et al. *ACM Transactions on Internet Technology*. 2023. Vol. 23, no. 3. P. 1–3. URL: https://doi.org/10.1145/3594535
19. BitTorrent File System (BTFS) | Scalable Decentralized File Storage. URL: https://www.bittorrent.com/token/bittorrent-file-system
20. De Salve A., Mori P., Ricci L., Di Pietro R. Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions. *Computer Communications*, 2023. P. 199–225. URL: https://doi.org/10.1016/j.comcom.2023.02.023