ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕОРІЯ КОДУВАННЯ

УДК 004.77+004.056

Л. М. Куперштейн, М. Д. Кренцін, А. В. Дудатьєв, В. А. Каплун

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ ПІРИНГОВИХ МЕРЕЖ

Вінницький національний технічний університет, Вінниця

Анотація. Проаналізовано базові поняття пірингових мереж. Вказано на актуальні напрямки їх використання, а саме файлообмінні сервіси, системи телеконференцій, ігрові та торгівельні сервіси та ін. Розглянуто різновиди структурної організації та визначено їх переваги та недоліки. За ступенем централізації виділено чисту, гібридну та федеративну архітектури. Також подано класифікацію однорангових пірингових мереж за способом з'єднання та функціями. Аналіз поширеності пікринових мереж у сучасному світі довів затребуваність і актуальність використання децентралізованої мережевої технології, особливо у сфері фінансів. Проаналізовано можливі типи атак на пірингові мережі. Виділено атаки як загального характеру, так і специфічні. Специфічні атаки орієновані на користувача, додаток або мережу. Наведено способи та механізми захисту для кожної із досліджуваних типів атак. Результати аналізу систематизовано, а саме для кожної атаки визначено вплив на дані, ступінь небезпеки та рівень захисту. Також вказано на напрям порушення інформаційної безпеки кожної атаки, а саме цілісність, доступність, конфіденційність. Не менш цікавою вона виявилася і для зловмисників, про що свідчить значна кількість зламів. Дослідження атак на P2P мережі показало їх широкий спектр як загального характеру, так і спеціалізованих. При цьому атаки диференційовано за ступенем небезпеки та аспектом порушення рівня безпеки. Найбільш небезпечними виявилися атаки, що можуть призвести до порушення конфіденційності та цілісності даних. До них відносяться такі атаки: розподілена відмова в обслуговуванні, отруєння індексу, атака Сивілли, атака затемнення, ботнети, маскарад. Проведене дослідження є базою для подальшого дослідження недоліків захисту пірингових мереж та розробки нових безпечних механізмів обміну даними в децентралізованих структурах.

Ключові слова: пірингова мережа, центральний сервер, вузол, маршрутизація, аутентифікація, брандмауер.

Abstract. The basic concepts of peer-to-peer networks are analyzed. The current areas of their use are indicated, namely file-sharing services, teleconferencing systems, gaming and trade services, etc. The types of structural organization are considered, and their advantages and disadvantages are determined. According to the degree of centralization, pure, hybrid and federal architectures are distinguished. The classification of peer-to-peer peer networks by connection method and function is also given. Analysis of the prevalence of peer-to-peer networks in the modern world has proved the demand and relevance of the use of decentralized network technology, especially in the field of finance. Possible types of attacks on peer-to-peer networks are analyzed. Both general and specific attacks are highlighted. Specific attacks are oriented on user, application or network. Methods and mechanisms of protection for each of the studied types of attacks are given. The results of the analysis are systematized, namely for each attack the impact on the data, the degree of danger and the level of protection is determined. It also indicates the direction of violation of information security of each attack, namely the integrity, accessibility, confidentiality. It turned out to be no less interesting for malefactors, as evidenced by the significant number of hacks. The research of attacks on P2P networks showed a wide range of both general and specialized. At the same time, attacks are differentiated according to the degree of danger and the aspect of security breach. The most dangerous were attacks that could violate the confidentiality and integrity of data. These include the following attacks: distributed denial of service, index poisoning, sibyl attack, eclipse attack, botnets, masquerade. The research is the basis for further study of the shortcomings of the protection of peer-to-peer networks and the development of new secure mechanisms for data exchange in decentralized structures.

Key words: peer-to-peer network, central server, peer, routing, authentication, firewall.
DOI: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.

Вступ

Концепція однорангової або пірингової (peer-to-peer (P2P) мережі була вперше використана в 1969 р. В свою чергу P2P розглядається як мережевий протокол, що забезпечує можливість створення мережі однорангових вузлів та їх взаємодію [1]. У багатьох випадках мережі P2P використовують існуючі протоколи стеку TCP/IP для передачі, а саме TCP, UDP або їх обгортки. Першою реальною реалізацією однорангової мережі стала мережа Usenet (1979 р.) [2]. У цій мережі, хоча клієнти кінцевих користувачів все ще отримують доступ до ресурсів через сервери, самі сервери взаємодіють як мережа P2P і спілкуються один з одним без центральних повноважень. Це означає, що суть однорангової мережі полягає в тому, що мережа не має центрального керуючого вузла і всі її учасники рівні [3]. Проте незалежно від того, що стан кожного вузла однаковий, їх можливості можуть значно відрізнятися.

Після створення «Usenet» однорангові мережі почали стрімко розвиватись. Змінилось кілька поколінь мереж, поки вони не набули поточного стану. Їх використання не обмежується обміном файлами, як це було раніше. Найбільшого поширення P2P мережі набули в областях, де важливий обмін конфіденційними даними між людьми. Це системи відеозв'язку та відеомовлення (P2PTV), IP-телефонія та системи інтернет-телебачення, фінансовий сектор тощо [4].

Актуальність

Подібно до традиційного Інтернету P2P мережі відкриті до багатьох як загальних мережевих атак, так і специфічних. Це пов'язано з тим, що на відміну від клієнт-серверних застосунків, P2P вузли мають рівні права, а також відсутнє класичне управління правами доступу (як в централізованих системах). Найпоширенішими атаками на пірингові мережі є «відмова в обслуговуванні» (danial of service − DoS) та її розподілена модифікація (distributed danial of service - DDoS), «людина посередині» (man-in-the-middle − MITM), «поширення хробака» (worm propagation), «атака забруднення» (pollution attack), «отруєння індексу» (index poisoning), «раціональна атака» (rational attack), «атака затемнення» (eclipse attack), «атака

Сивілли» (Sybil attack) та ін. [5]. Всі ці атаки відрізняються складністю реалізації та технологіями захисту від них.

Із появою піринговоі технології блокчейн та реалізації на її основі фінансових сервісів, у тому числі криптовалютних, закікавленість ними зловмисників значно зросла. Останнім часом офіційно зафіксовано ряд «гучних» інцидентів. Так у березні 2022 року було зареєстровано крипто-злам, що був націлений на ігровий сервіс на основі мережі блокчейнів. При цьому хакери зламали мережу «Ronin Network» та незалежний і сумісний з Ethereum ланцюг блоків. В загальному втрати склали 625 млн. доларів США. [6]. Ще одним не менш масштабнішим зламом такого типу було у січні 2022 викрадення 80 млн. доларів США у DeFi-платформи Qubit Finance, що побудована на Binance Smart Chain (блокчейн, створений для криптовалюти BNB). Злам було проведено 2022 року. При цьому хакери використали вразливість мосту Qubit (децентралізованої платформи грошового обміну) [7].

Також у вересні 2021 року було зареєстровано DDoS атаки на провайдера VoIP.ms. Атака була спрямована на всю інфраструктуру телефонії, унеможливлюючи здійснення дзвінків [8].

Виходячи з вищеописаного, доцільним та актуальним є аналіз та систематизація знань про загрози P2P системам, методів їх попередження та виявлення для оцінки їх потенціалу, а також вдосконалення та розробки нових перспективних превентивних механізмів.

Метою дослідження є аналіз проблем безпеки піринговых мереж та прикладних систем на їх основі для розробки класифікації потенційних загроз, що дозволить більш чітко спрямовувати вектори підходів до їх захисту, а також методики тестування на проникнення.

Загальна характеристика піринговых мереж

Пірингова мережа – це технологія, що реалізує об'єднання однорангових вузлів рівного статусу з собі подібними. Кожен вузол є і приймачем, і надавачем послуг. Такі вузли можуть обмінюватись інформацією безпосередньо. За ступенем централізації P2P мережі бувають трьох типів [9]:

− чиста, яка передбачає поєднання всіх вузлів один з одним. На сьогоднішній день повністю чисті пірингові мережі майже не використовуються. Представниками чистих P2P мереж є IPFS та Orbit-DB.

− гібридна, що використовує центральний сервер для того, щоб надати вузлу інформацію про адресу іншого вузла в мережі. Використовується в системах обміну файлами, що працюють з протоколом BitTorrent та мережах по доставці контенту (CDN).

− федеративна, суть якої полягає в тому, що мережа поділена на групи, в кожній з яких є головний. Всередині групи вузли поєднані один з одним, але в межах всієї мережі групи поєднані за допомогою головних вузлів. Використовується в деяких іграх та соціальних мережах (Aether, DarkCrystal) [10].

Однорангові мережі також розподіляються за способом з'єднання: структуровані та неструктуровані [11]. Структурована мережа P2P використовує єдиний алгоритм, який гарантує те, що будь-який вузол може ефективно передати запит іншому вузлу, який має шуканий файл (дані), навіть, якщо файл рідкісний. Неструктурована пірингова мережа передбачає довільне встановлення з'єднання. Такі мережі легко створюються, але їх недоліком є те, що запити не завжди оброблюються.

Мережі P2P диференціюються за базовим функціональним призначенням:

– Файлообмін. Найпоширеніша функція. Дуже актуальним є для передачі великих файлів при невеликій пропускній здатності мережі. Прикладами таких програм є uTorrent, BitTorent, FrostWire та ін. [12].

– Співпраця. Це може бути наприклад обмін повідомленнями, онлайн ігри, сумісна робота над документами. Прикладами таких систем є CASA, GENI, P2P cloud [13].

– Розподілені обчислення. Обчислювальна проблема розподіляється на невеликі незалежні частини. Прикладом такої системи є SETI@Home [14].

Класифікація атак на пірингові мережі

В загальному атаки на пірингові мережі поділяються на дві великі категорії: активні та пасивні [15]. Активну атаку можна визначити як таку, що спрямована на один або декілька вузлів P2P мережі. Основний мотив активної атаки − викликати пошкодження вузлів. Пасивні атаки спрямовані виключно на саму мережу, а не на її вузол. Основний мотив пасивної атаки – це порушення доступності, щоб учасники були обмежені у використанні конкретних послуг. На сьогодні відомо ряд поширених атак та загальні способи захисту від них [16]. Проте в залежності від прикладного застосування технології P2P як механізм атак так і методи захисту можуть суттєво відрізнятися.

1. Атака «Відмова в обслуговуванні» (Denial of service, DoS) – це атака на комп'ютер або мережу, що робить неможливим подальше використання сервісів мережі. Існує два способи виконати таку атаку: наповнювати мережу фіктивними пакетами (при цьому цільова доставка істинного трафіку ускладнюється) або ж змусити вузли працювати над складними (вибагливими по ресурсам) обчисленнями, аби у вузла не було змоги відповісти на інші запити, що надходять [17].

Захист: Для того, щоб захистити мережу від такої атаки використовують так зване «ціноутворення». Оскільки неможливо відрізнити справжні важкі обчислення, що можуть виконуватись вузлом, від фікти-

вних, тому неможливо вчасно виявити і запобігти атаці. Тому вузол, що надає послугу, повинен надавати своїм клієнтам так звані «головоломки», адже лише у випадку її вирішення клієнту можна довіряти та відповідати на запит. Проте недоліком цього методу є те, що деякі справжні клієнти (наприклад мобільні пристрої) можуть швидше розряджатись, вирішуючи ці «головоломки». Також можна блокувати вразливі порти, на які можуть здійснюватися атаки. Ще одним способом є додавання спеціальних правил до брандмауера та використання спеціалізованих маршрутизаторів [18] .

2. Коли в атаці залучено кілька хостів, тоді вона називається «розподілена відмова в обслуговуванні» (Distributed denial of service, DDoS). В цьому випадку атакуючі комп'ютери часто є персональними комп'ютерами з широкосмуговою мережею з'єднання, що були зламані вірусом або трояном. Злочинець при цьому може дистанційно керувати цими машинами (їх називають зомбі) і спрямувати атаку на будь-який хост чи мережу.

Захист: Існує три кроки, щоб запобігти DDoS-атакам: Спочатку необхідно пропускати інтернет-трафік через брокерську компанію, що допоможе клієнтам відфільтрувати серію шкідливої інформації. По-друге, необхідно використовувати моніторинг взаємодії вузлів для виявлення DDoS атак. Також у брокерів можуть бути свій власний чорний та/або білий список, які дозволяють брокерам припинити роботу трафіку у чорному списку до того, як він потрапив до кінцевого користувача, при цьому брокери завжди дозволяють трафік із білого списку [19].

3. Атака «Людина посередині» (Man-in-the-middle) – це атака, коли зловмисник непомітно вставляється між двома вузлами та керує їхньою комунікацією. Це може бути зміна, видалення чи вставка повідомлень. У багатьох випадках – це розсилання неправдивої інформації. Така атака є досить серйозною для більшості протоколів, особливо, коли є форма аутентифікації [20].

Захист: В піринговых мережах неможливо виявити атаку «Людина посередині», адже вони не мають центрального серверу, що здатен перевіряти та контролювати трафік. Проте для запобігання майбутніх атак слід використовувати шифрування інформації, що передається. Також необхідно по можливості використовувати методи аутентифікації для перевірки автентичності та валідності користувача.

4. Атака «Поширення хробака» (Worm propagation) полягає в тому, що хробак передає свої копії від одного вузла до іншого через мережеве підключення і працює окремо. Хробак може поширюватися через файли, електронну пошту, веб-сервер тощо. Існує ряд факторів, які дозволяють мережам P2P стати вразливими для такого роду атак [21]:

– Мережі P2P складаються із комп'ютерів, на яких виконуються однакові програми. Таким чином атакуючий може з першого дня зібрати всі вузли, які зможуть скомпрометувати всю мережу, знайшовши одне слабке місце в мережі.

– Вузли P2P, як правило, з'єднуються з багатьма іншими вузлами. Тому хробак не буде втрачати час на сканування інших жертв, а просто отримує список сусідніх вузлів та поширюється ними.

– P2P-програми також використовуються для передачі великих файлів. Деякі хробаки мають обмежувати їхній розмір, щоб передаватись одним TCP-пакетом. Це може призвести до реалізації більш складних атак.

– Програми P2P часто доступні на комп'ютерах співробітників замість серверів. Таким чином, зловмиснику легше отримати доступ до важливих даних (паролі, номера карток тощо).

– Користувачі P2P часто передають незаконний вміст (наприклад, захищена авторським правом музика), і вони схильні не повідомляти про незвичайну поведінку мережі.

Як тільки «хробаки» закінчують розмножуватися, їх метою зазвичай є запуск масової DDoS атаки в політичних або комерційних цілях.

Захист: Одним із методів захисту є використання брандмауера. У більшості випадків «хробак» сканує певний порт у комп'ютера для зараження, а брандмауери можуть заблокувати порт, який потребує хробак. Крім того, слід використовувати антивірусне програмне забезпечення, щоб захистити комп'ютери. До складу антивірусного програмного забезпечення входить сигнатура вірусу, якщо деякі атрибути файлу відповідають атрибутам в сигнатурі вірусу, антивірусне програмне забезпечення може видалити або ізолювати цей файл. Антивірусне програмне забезпечення може бути також вбудованим в операційну систему.

5. Атака «Забруднення» (Pollution attack) полягає в заміні файлу в мережі помилковим, і цей забруднений файл стає непридатним. Зловмисник створює цільовий вміст непридатним для використання шляхом зміни вмісту або його частини на інший незалежно від вмісту, а потім робить цей вміст доступним для обміну [22]. Щоб залучити людей до завантаження забрудненого файлу, його потрібно замаскувати як корисний вміст, наприклад, мати той самий формат і аналогічний розмір. Він також повинен підтримувати високу пропускну здатність з'єднання.

Захист: З боку користувача завантажений файл, який був забруднений, є нешкідливим для інших комп'ютерів, але він просто витрачає зайву пам'ять. Тому, як тільки користувач дізнається, що завантажені файли є забрудненими, він повинен видалити їх із системи P2P.

6. Раціональні атаки (Rational attacks). Щоб P2P-послуги були ефективними, вузли-учасники повинні співпрацювати, але в більшості сценаріїв вузол представляє зацікавлену сторону, і співпраця неможлива. Розумним припущенням є те, що велика частка P2P-вузлів є раціональними і намагатимуться максимізувати споживання системних ресурсів при мінімізації використання власних. Наприклад, вузли можуть зрозуміти, що, не надавши спільного доступу, вони заощаджують пропускну здатність для завантаження необхідних їм даних [26]. Якщо велика кількість вузлів є такими, що відмовляються від внесків (тобто лише хочуть отримувати дані і нічого не віддавати іншим вузлам), система може дестабілізуватись. У цьому випадку, якщо достатньо вузлів, що зацікавляться, система не може гарантувати належний рівень завантажень і вивантаження даних.

Захистом від такої атаки є алгоритм, що може гарантувати розумний рівень взаємності завантаження та вивантаження. Якщо вузли просто завантажують і ніколи не вивантажують, вони повинні бути «оштрафовані».

7. Атака «Сивілли» (Sybil attack). У багатьох піринговых системах передбачено надлишкове резервне копіювання, що є механізмом захисту цілісності та конфіденційності. P2P система повинна переконатися, що кожен ідентифікатор мережевого об'єкта вказує лише одну сутність. Якщо сутність діє як декілька множинних об'єктів, то зловмисник може контролювати частину мережі. Такий напад визначається як атака «Сивілли». Вона знищить резервне копіювання в одноранговій мережі P2P. Наприклад, коли звичайний вузол A робить резервне копіювання, він вибирає групу вузлів, таких як B, C, D, E, що мають різні ідентифікатори. Але насправді вузли C, D та E не існують, оскільки вони є шкідливими вузлами, створеними зловмисником, тому резервне копіювання не може завершитися, а система перестає нормально працювати.

Захист: Для того, щоб захиститись від атаки «Сивілли» необхідно використовувати метод самореєстрації [22, 27]. Це може бути включення IP-адреси вузла до його ідентифікатора. Таким чином, зловмисний вузол не зможе підробити справжні вузли, оскільки він буде прив'язаний до обмеженої кількості IP-адрес, і його можна помітити, якщо він створить більше сутностей. Але це рішення далеко не просте, оскільки, наприклад, можна генерувати підроблені ідентифікатори для інших вузлів, а потім система буде їх бачити як зловмисні. Ще одним способом захисту є використання складного протоколу на основі публічно-приватного ключа. Кожен вузол повинен підписувати своє повідомлення та час від часу відповідати на запити з боку якогось центрального вузла (проте це дає інші слабкі місця).

8. Атака «Затемнення» (Eclipse attack) передбачає виконання певних підготовчих дій. Спочатку зловмисник повинен отримати контроль над певною кількістю вузлів уздовж стратегічних маршрутів. Після цього атакуючий може розділити мережу на різні підмережі. Таким чином, якщо вузол хоче спілкуватися з вузлом з іншої підмережі, його повідомлення має у певний момент бути маршрутизованим через один із вузлів зловмисника. Зловмисник таким чином «затемнює» кожну підмережу іншою. У певному сенсі, атаки затемнення є розширеним варіантом атаки «Людина посередині», а також може бути продовженням атаки «Сивілли». В цьому випадку, зловмисник намагатиметься розмістити свої вузли на стратегічних маршрутах. Зловмисник може повністю контролювати підмережу з іншого боку підмережі [22]. Якщо зловмиснику вдається атака Eclipse, він може атакувати мережу набагато ефективніше:

- неефективно перенаправляти кожне повідомлення вузлу, якому воно не призначене;
- ігнорувати всі вхідні повідомлення, таким чином повністю відокремлюючи обидві підмережі;
- використовувати атаку «Забруднення» для того, щоб засмітити обидві підмережі, зробивши їх непридатними для подальшої взаємодії.

Захист. На відміну від атак «Людина посередині», дуже ретельно підібрані криптографічні протоколи можуть стати гарною спробою зупинити таку атаку. Ціноутворення також може допомогти проти версії з використанням атаки Sybil. Проблема таких рішень полягає в тому, що вони створюють серйозне уповільнення та перешкоджають нормальній масштабованості мережі. Основним захистом від атак «Затемнення» є використання чистої піринговой мережі [27]. Ще кращим рішенням було б додатково використовувати алгоритм рандомізації для визначення розташування вузлів. Якщо вузли в чистій P2P мережі розподілені випадковим чином, нападник не може контролювати позиції своїх вузлів. Тому було б майже неможливо відокремити дві підмережі одна від одної.

9. Атака «Отруєння індексу» (Index poisoning attack). Багато сучасних систем P2P мають індекси, що дозволяють користувачам знайти місця розташування бажаного контенту. Атака «Отруєння індексу» спрямована на процес індексного запиту користувачів і ускладнює пошук правильного вмісту в мережі P2P. Зловмисники просто вставляють велику кількість недійсних індексів в загальну таблицю, щоб завадити користувачам знайти правильний ресурс.

Захист: є два заходи захисту від атаки «Index poisoning». Перший з них – це аутентифікація версій і рекламні оголошення [23]. Як і деякі рейтингові веб-сайти та форуми, вміст повинен бути промодерований. Другий метод – рейтинг джерел. Якщо ці вузли є джерелами даних високого попиту, які надають і завантажують файли, то вони мають високий рейтинг. Якщо це джерела «сміттєвих» даних, що забруднюють систему, то відповідні однорангові вузли будуть у чорному списку.

10. Ботнети (Botnets). Однією з найбільш значущих загроз для Інтернету сьогодні є загроза ботнетів, які є скомпрометованими мережами під контролем зловмисника (мережа керується автономною програмою, що приховано встановлюється на комп'ютери-жертви та маскується під системний процес чи корисне ПЗ). Ботнет створює значні загрози для структурованих P2P мереж [24]. Порівняно з іншими шкідливими програмами в Інтернеті, ботнети відрізняються від традиційних атак в тому, що вони діють як скоординована атакуюча група. Машини, які часто беруть участь у ботнеті мають віруси, хробаки та трояни.

Захист: сьогодні існує ряд спеціальних методів виявлення та зупинки ботнетів (наприклад, розділення вузлів і проектування наборів тестів Тюрінга або головоломок, які користувачі повинні розгадати, щоб отримати доступ до перевантажених ресурсів).

11. Атака підслуховування (Eavesdropping attack) – це ще один вид атаки на мережі. Зловмисники можуть отримати доступ до даних у мережі та прослуховувати трафік. Одна з найбільших проблем безпеки, з якою стикаються користувачі, це здатність зловмисників моніторити мережі, а саме визначати паролі та ключі, отримати MAC-адресу, отримати IP-адресу, і в результаті, призвести до збою мережі [26]. У таких атаках можуть застосовуватись засоби прослуховування (для того, щоб почути чиїсь паролі для входу), моніторингу через камери відеонагляду (для того, щоб побачити паролі для входу) тощо.

Захист: першим кроком у запобіганні атаки підслуховування є використання міцної фізичної безпеки, а наступний крок – використання шифрування будь-якої важливої інформації.

12. Маскарадна атака – це тип атаки, в якій юридична особа нелегітимно представляє собою іншу сутність, яка має доступ до конфіденційної інформації чи системи. Маскарадні атаки надзвичайно серйозні. Вони можуть відбуватися різними способами. Зловмисники можуть отримати доступ до облікового запису законного користувача через викрадення пароля, обхід процесу авторизації або через IP-адресу. Якщо процес авторизації не повністю захищений, він може стати надзвичайно вразливим для маскарадної атаки [26].

Захист: поширеним методом обмеження цього типу атаки є фільтрація вхідних пакетів, які надходять із внутрішньої IP-адреси та фільтрація вихідних пакетів, які виходять з недійсної локальної IP-адреси.

13. Неправильне оновлення маршруту. Зловмисник може пошкодити таблиці маршрутизації, надсилаючи іншим вузлам недійсні дані або ж спрямовувати запити до невідповідних або до неіснуючих вузлів.

Захист: для запобігання такій атаці необхідно виконувати певні умови, наприклад, враховувати час обміну в обидва боки, щоб віддати перевагу найкоротшому шляху. Або ж, наприклад, у таблицях має передувати правильний префікс, який не може бути відтворений шкідливими вузлами [25].

14. Неправильний пошук маршруту. Пошук ключів у структурованих мережах P2P виконується шляхом маршрутизації запитів через серію вузлів. Кожен з цих вузлів використовує локальну таблицю маршрутизації для пересилання запиту до вузла, відповідального за ключ. Цей механізм використовується для зберігання, отримання, тиражування та аутентифікації даних. Оскільки шкідливий вузол може пошкодити цей механізм через систему оновлення маршрутизації, він може пересилати повідомлення неправильному або неіснуючому вузлу (таким чином не надавши правильному вузлу інформацію) [11].

Захист: запобігти такій атаці можна двома способами. По-перше, запитувач повинен переконатися, що кінцевий вузол підтверджує те, що він є правильною точкою завершення запиту. По-друге, система повинна призначити ключі вузлам у верифікований спосіб.

15. Атака «Викрадення сутності». Така атака спрямована на мережі, де вузол знає лише про деяку частину сусідніх вузлів, а інформацію необхідно надіслати до незнайомого вузла (таким чином вузол довіряє іншим у правильній маршрутизації даних). Однак зловмисник може використовувати цю довіру, щоб почати атаку на крадіжку особистих даних. Коли шкідливий вузол на шляху повідомлення стверджує, що це бажаний вузол призначення, то він може захопити маршрут і, наприклад, знищити чи перенаправити дані.

Захист: запропоновано метод, у якому використовуються докази, чорні списки та зловмисну маршрутизацію, і було показано, що він ефективно виявляє, позначає та перенаправляє трафік від зловмисника. Метод полягає в тому, що вузли підписують сертифікати доказу життя для часткових ідентифікаторів вузлів і розповсюджують їх випадково вибраним менеджерам доказів у мережі. Вихідні вузли можуть уникати зловмисників, запитуючи докази у кількох менеджерів доказів [26].

16. Атака відтоку. Ця атака спрямована на структуровані пірингові мережі. Ця характеристика робить таку систему привабливою для великої кількості користувачів і водночас уразливою до явищ відтоку [11]. Суть атаки полягає в тому, що до мережі підключається та відключається одночасно велика кількість вузлів, що створює ефект, який називається відтоком. Зловмисник може використати цю атаку, щоб досить швидко зіпсувати найкращу функцію мережі.

Захист: мережі P2P мають бути спроектовані так, щоб легко масштабуватись та витримувати сплеск навантаження.

17. Співставлення ідентифікаторів. У структурованих піринговых мережах є випадковий розподіл ідентифікаторів вузлів. Це випадкове розподілення дозволяє зловмиснику отримати певну інформацію про ідентифікатор і отримати контроль над певними ресурсами. Ця атака тісно пов'язана з атакою Сивілли. Але основна відмінність полягає в тому що атака Сивілли використовується для створення великої кількості випадкових ідентифікатори, у той час як ця атака спрямована на отримання деяких конкретних.

Захист: найкраще рішення, щоб уникнути атаки співставлення ідентифікатора – це використовувати централізований орган, який розповсюджує ідентифікатори, але це непрактично, оскільки мережі P2P є масштабованими та децентралізованими. Тому захиститись від такої атаки можна лише якщо ідентифікатор залежить від деякої інформації за межами керування вузлом [27]. Наприклад, змусити вузол отримати свій ідентифікатор з IP-адреси, номера порту якоїсь хеш-функції.

18. Атака зберігання та отримання тісно пов'язана з раціональною атакою, оскільки зловмисники відмовляються надавати послуги іншим вузлам або заперечують існування даних. Ця атака може бути небезпечною в системі, яка не призначає вузлам ідентифікатори, які можна верифікувати. У такій системі вузол може взяти на себе відповідальність за дані, які він бажає сховати чи відмовитись надавати [11].

Захист: щоб запобігти цій атаці, система повинна забезпечити реплікацію. Реплікація має бути оброблена таким чином, щоб кілька вузлів відповідали за реплікацію.

19. Атака «Переповнення запитів». Структурована P2P мережа складається з великої кількості вузлів, які не підключені до всіх інших вузлів. Якщо вузол виконує запит до сусідніх вузлів на отримання даних, а ті, в свою чергу, не маючи її, роблять запити своїм сусіднім вузлам, то мережа породжує дуже багато запитів. Таким чином зловмисник може генерувати подібні запити у великій кількості, перешкоджаючи при цьому основному трафіку всередині мережі [28].

Захист: обмежувати кількість вхідних запитів від одного вузла за одиницю часу.

20. Атака «Порушення анонімності». У контексті структурованих мереж P2P, кожен вузол має таблицю маршрутизації, що містить набір відповідних однорангових вузлів відносно певного ключа. Таким чином запит надходить від одного вузла до іншого через проміжні вузли. А це в свою чергу виключає повну анонімність. Зловмисник може контролювати всю інформацію, що проходить через нього, щоб отримати знання інших про інші вузли, які його оточують. У цьому випадку, зловмисник може взнати більшість файлів, запити про які проходять через нього [26].

Захист: проблема анонімності зводиться до захисту ідентифікаторів вузлів, що запитують дані та вузла, що надає інформацію про ключ доступу до іншого вузла.

21. Атака «Порушення конфіденційності». Сьогодні P2P-мережі стають все більшими популярними, адже вони призначені для спільного використання ресурсів і надання послуг. Проблема конфіденційності полягає в тому, що користувачі можуть випадково або несвідомо дозволити їх приватні або особисті файли, до яких буде відкрито доступ. У цій ситуації вони ризикують розкрити свою приватну інформацію іншим користувачам мережі.

Захист: користувач повинен бути уважним при наданні доступу до файлів.

Зведену характеристику атак та методів захисту від них наведено у таблиці 1.

Таблиця 1 – Характеристика атак на P2P мережі та методів захисту від них

№	Назва атаки	Поведінка	Що порушує	Стратегії захисту	Ступінь небезпеки	Рівень захисту
1	Відмова в обслуговуванні	1. Закидання в мережу підробних пакетів. 2. Завантаження вузла вибагливим обчисленням	Доступність	Ціноутворення, брандмауер, спеціалізовані маршрутизатори	Середній	Легкий
2	Розподілена відмова в обслуговуванні	Хакер контролює контрольних зомбі, а через тих «зомбі» відбувається контроль атакуючих «зомбі»	Доступність	Через надійний сервер, забезпечити систему оповіщення. Створити чорний і білий списки для довірених відвідувань	Високий	Важкий
3	Людина посередині	Зловмисник вставляє себе непомітно між двома вузлами та перехоплює, змінює та надсилає дані між цими двома вузлами	Цілісність, доступність, конфіденційність	Механізм шифрування і технологія аутентифікації	Середній	Середній
4	Розповсюдження хробака	Передає свої копії від одного вузла до інших автоматично	Цілісність, доступність, конфіденційність	Брандмауер, антивірус, безпечна операційна система	Середній	Середній
5	Атака забруднення	Поділіться файлом, який не використовується	Цілісність, доступність	Забрати такий файл	Низький	Легкий
6	Раціональна атака	Лише завантажувати дані і ніколи не вивантажувати інші	Доступність	Штрафна система	Середній	Середній

Продовження таблиці 1

7	Отруєння індексу	Змінюється індексація інформації, щоб вузлу було важко знайти правильний зміст	Доступність	Аутентифікація версій і реклама, рейтинг джерела	Високий	Середній
8	Атака Сивілли	Контролює кількість сутностей	Цілісність, конфіденційність	Алгоритм самореєстрації	Високий	Важкий
9	Атака затемнення	Шкідливі вузли працюють разом, щоб обдурити добрі вузли	Цілісність, доступність	Indegree і Outdegree методи	Високий	Важкий
10	Ботнети	Зараження комп'ютерів автономною програмою, що використовує ресурси на свій лад	Цілісність, доступність, конфіденційність	Розділення вузлів та тести Тьюринга	Високий	Важкий
11	Атака підслуховування	Викрадення конфіденційної інформації за допомогою засобів «підслуховування»	Цілісність, конфіденційність	Фізичні методи захисту та шифрування даних	Середній	Середній
12	Маскарад	Одна особа видає себе за іншу, що має доступ до даних	Цілісність, конфіденційність	Фільтрація вхідних та вихідних пакетів даних	Високий	Середній
13	Неправильне оновлення маршруту	Пошкодження таблиць маршрутизації	Доступність	Префікси у таблицях індексації, найкоротший шлях обміну даними	Низький	Легкий
14	Неправильний пошук маршруту	Пересилання таблиць маршрутизації неправильним вузлам	Доступність	Призначення ключів у верифікований спосіб та взаємопідтвердження при запитах	Низький	Легкий
15	Викрадення Сутності	Шкідливий вузол перехоплює маршрут та видає себе за кінцевий, якому належить інформація	Цілісність, конфіденційність	Докази, чорні списки, зловмисна маршрутизація	Середній	Середній
16	Атака відтоку	Одночасне підключення та відключення великої кількості вузлів	Доступність	Правильне проектування мережі	Низький	Легкий
17	Співставлення ідентифікаторів	Визначення ідентифікатора вузла для контролю його ресурсів	Цілісність, доступність, конфіденційність	Залежність ідентифікатора вузла від зовнішніх для вузла даних	Середній	Середній
18	Атака зберігання та отримання	Перехоплення ідентифікатора вузла та відмова у наданні даних	Цілісність, доступність, конфіденційність	Реплікація даних	Середній	Легкий
19	Переповнення запитів	Надсилання запитів про пошук інформації у великій кількості	Доступність	Обмеження кількості вхідних запитів від вузла	Середній	Легкий
20	Порушення анонімності	Отримання проміжної інформації про запити та місцезнаходження даних через проміжні вузли	Конфіденційність	Захист ідентифікаторів вузлів різними методами	Низький	Середній
21	Порушення конфіденційності	Випадкове надання користувачем доступу до конфіденційної інформації	Конфіденційність	Уважність користувача при роботі з системою	Низький	Легкий

Також, коли йдеться про безпеку, людський фактор завжди має враховуватися. Зростання клієнтів різноманітних пірингових мереж відбулось завдяки простоті установки та використання, невисокій вартості та перспективного результату. Початківці та не лише не відчувають великих труднощів з використанням таких додатків щоб завантажити файли. Проте ці файли можуть бути «забрудненими» тощо. Ще одна проблема безпеки, яку створюють додатки P2P – це те, що людина помилково може почати вивантажувати в систему купу непотрібних файлів окрім запитуваного, а це, в свою чергу, спричиняє непотрібне нагромадження даних в системі. Також користувач може бути вразливим місцем для зловмисника, через що той може отримати доступ до мережі для спричинення інших видів атак. Тому, враховуючи вищеописані проблеми, необхідно бути уважним при розробці та користуванні P2P системою.

Висновки

Аналіз поширеності піринговых мереж у сучасному світі довів затребуваність і актуальність використання децентралізованої мережевої технології, особливо у сфері фінансів. Не менш цікавою вона виявилася і для зловмисників, про що свідчить значна кількість зламів. Дослідження атак на P2P мережі показало їх широкий спектр як загального характеру, так і спеціалізованих. При цьому атаки диференційовано за ступенем небезпеки та аспектом порушення рівня безпеки. Найбільш небезпечними виявилися атаки, що можуть призвести до порушення конфіденційності, цілісності та доступності (атаки «людина по середині», «хробаки», «ботнет» та ін.). Не дивлячись на ряд механізмів захисту від потенційних загроз залишається актуальною атака нульового дня. Тому завжди актуальним буде розробка нових та вдосконалення існуючих методів захисту піринговых сервісів. Отримані результати дослідження ляжуть в основу розробки класифікації загроз P2P мереж.

Список літератури

[1] J. Buford, H. Yu, E. K. Lua, *P2P Networking and Applications*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008, p. 408.

[2] The Social Forces Behind the Development of Usenet By Michael Hauben. [Online]. Available: http://www.columbia.edu/~hauben/book/ch106.x03. Accessed on: January 20, 2022.

[3] P2P Networking. [Online]. Available: https://nakamoto.com/p2p-networking/. Accessed on: January 20, 2022.

[4] Peer-To-Peer VOiP. [Online]. Available: https://www.tmcnet.com/voip/0907/feature-articles-peer-to-peer-voip.htm. Accessed on: January 20, 2022.

[5] All.Net [Online]. Available: http://all.net/. Accessed on: February 10, 2022.

[6] Axie Infinity's Ronin network suffers hack and theft of over $600 million – CNN. [Online]. Available: https://edition.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html. Accessed on: January 22, 2022.

[7] Hackers Steal Cryptocurrency Worth $80 Million From Decentralised Finance Platform Qubit Finance [Online]. Available: https://www.ndtv.com/business/cryptocurrency-worth-80-million-stolen-from-defi-platform-qubit-finance-2737888. Accessed on: Jan. 22, 2022.

[8] HackRead | Latest Cyber Crime − InfoSec-Tech − Hacking News. [Online]. Available: https://www.hackread.com/canadian-voip-ms-hit-by-extortion-ddos-attacks/. Accessed on: April 10, 2022.

[9] Л. М. Куперштейн, М. Д. Кренцін, "Аналіз тенденцій розвитку піринговых мереж", *Вісник Хмельницького національного університету*, № 4, с. 25-29, 2021.

[10] Decentralized Social Networks. Comparing federated and peer-to-peer… | by Jay Graber | Stories from the Decentralized Web | Medium. [Online]. Available: https://medium.com/decentralized-web/decentralized-social-networks-e5a7a2603f53. Accesses on: December 15, 2021.

[11] A. Cabani, S. Ramaswamy, M. Itmi, S. Al-Shukri, J. Pécuchet. "Distributed Computing Systems: P2P versus Grid Computing Alternatives" in *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering*. Springer, Dordrecht, 2007, pp. 47-52. doi: 10.1007/978-1-4020-6268-1_9.

[12] Best 10 Peer to Peer (P2P) File Sharing Programs and Applications XtendedView. [Online] Available: https://xtendedview.com/internet/best-p2p-file-sharing-programs/5684/. Accesses on: December 25, 2021.

[13] H.M.N.D. Bandara, A. P. Jayasumana, "Collaborative applications over peer-to-peer systems–challenges and solutions". *Peer-to-Peer Netw. Appl*, № 6, pp. 257–276, 2013. doi: 10.1007/s12083-012-0157-3.

[14] SETI@home. [Online]. Available: http://setiathome.ssl.berkeley.edu/. Accessed on: April 4, 2022.

[15] Md. Sadek Ferdous, Farida Chowdhury, Md. Moniruzzaman. "A Taxonomy of Attack Methods on Peer-to-Peer Network" in *Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security*, India, 2007, pp. 132-138.

[16] Roger Wattenhofer. "Attacks on Peer-to-Peer Networks" in Semester Thesis of Swiss Federal Institute of Thechnolog, 2005, Zurich, pp.1-36.

[17] O. P. Voitovych, Y. V. Baryshev, L. M. Kupershtein, E. I. Kolibabchuk, "Investigation of Simple Denial-of-Service Attacks", *Third International IEEE Conference "Problems of Infocommunications. Science and Technology"*, 2016, Kharkiv, Ukraine, pp. 1-4.

[18] L. Kupershtein, T. Martyniuk, O. Voitovych, B. Kulchytskyi, A. Kozhemiako et al. "DDoS-attack detection using artificial neural networks in Matlab," *Proc.SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-EnergyPhysics Experiments*, 2019. doi: 10.1117/12.2536478.

[19] Н. В. Багнюк, В. М. Мельник, О. В. Клеха, І. А. Невідомський, "Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack", *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, № 18, 2015, с. 6-12.

[20] Elakrat Mohamed Abdallah, Jung, Jae Cheon, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication net-work", *Nuclear Engineering and Technology*, no. 50, pp. 780–787, June 2018. doi:10.1016/j.net.2018.01.018.

[21] X. Fan, and Y. Xiang, "Propagation Modeling of Peer-to-Peer Worms", in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Central Queensland University, Rockhampton, Australia, 2010, pp. 1128-1135.

[22] W. Stallings, Cryptography and Network Secrity: Principles and Practices, 6th ed. Prentice Hall, Upper Saddle River, NJ, 2013, 752 pp.

[23] J. Liang, N. Naoumov, and K.W. Ross, "The Index Poisoning Attack in P2P File Sharing Systems" in *25th IEEE International Conference on Computer Communications. Polytechnic Univerisy*, Brooklyn, NY, 2006, pp. 1-12.

[24] C. Schiller, J. Binkley, D. Harley, G. Evron, T. Bradley, C. Willems, M. Cross, "Botnets − The Killer Web App", Syngress, Rockland, 2007, 482pp. ISBN-10: 1-59749-135-7.

[25] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, D. Wallach, "Secure routing for structured peer-to-peer overlay networks", *SIGOPS Oper. Syst. Rev*, vol. 36, December 2003, pp. 299-314. doi:10.1145/844128.844156.

[26] D. Stutzbach, R. Rejaie, "Understanding churn in peer-to-peer networks" in *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, New York, 2006, pp. 189-202.

[27] A. Vasudeva, M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks", *Journal of Network and Computer Applications*, vol. 120, pp. 78-118, 2018. doi: 10.1016/j.jnca.2018.07.006.

[28] W. Ai, L. Xinsong and L. Kejian, "Efficient flooding in peer-to-peer networks," *2006 7th International Conference on Computer-Aided Industrial Design and Conceptual Design*, 2006, pp. 1-6, doi: 10.1109/CAIDCD.2006.329410.

Стаття надійшла: 04.05.2022.

References

[1] J. Buford, H. Yu, E. K. Lua, *P2P Networking and Applications*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008, p. 408.

[2] The Social Forces Behind the Development of Usenet By Michael Hauben. [Online]. Available: http://www.columbia.edu/~hauben/book/ch106.x03. Accessed on: January 20, 2022.

[3] P2P Networking. [Online]. Available: https://nakamoto.com/p2p-networking/. Accessed on: January 20, 2022.

[4] Peer-To-Peer VOiP. [Online]. Available: https://www.tmcnet.com/voip/0907/feature-articles-peer-to-peer-voip.htm. Accessed on: January 20, 2022.

[5] All.Net [Online]. Available: http://all.net/. Accessed on: February 10, 2022.

[6] Axie Infinity's Ronin network suffers hack and theft of over $600 million – CNN. [Online]. Available: https://edition.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html. Accessed on: January 22, 2022.

[7] Hackers Steal Cryptocurrency Worth $80 Million From Decentralised Finance Platform Qubit Finance [Online]. Available: https://www.ndtv.com/business/cryptocurrency-worth-80-million-stolen-from-defi-platform-qubit-finance-2737888. Accessed on: Jan. 22, 2022.

[8] HackRead | Latest Cyber Crime − InfoSec- Tech − Hacking News. [Online]. Available: https://www.hackread.com/canadian-voip-ms-hit-by-extortion-ddos-attacks/. Accessed on: April 10, 2022.

[9] L. M. Kupershtein, M. D. Krentsin, "Analiz tendentsii rozvytku pirynhovykh merezh", *Visnyk Khmelnytskoho natsionalnoho universytetu*, № 4, pp. 25-29, 2021 [in Ukrainian].

[10] Decentralized Social Networks. Comparing federated and peer-to-peer… | by Jay Graber | Stories from the Decentralized Web | Medium. [Online]. Available: https://medium.com/decentralized-web/decentralized-social-networks-e5a7a2603f53. Accesses on: December 15, 2021.

[11] A. Cabani, S. Ramaswamy, M. Itmi, S. Al-Shukri, J. Pécuchet, "Distributed Computing Systems: P2P versus Grid Computing Alternatives" in *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering*. Springer, Dordrecht, 2007, pp. 47-52. doi: 10.1007/978-1-4020-6268-1_9.

[12] Best 10 Peer to Peer (P2P) File Sharing Programs and Applications XtendedView. [Online] Available: https://xtendedview.com/internet/best-p2p-file-sharing-programs/5684/. Accesses on: December 25, 2021.

[13] H.M.N.D. Bandara, A. P. Jayasumana, "Collaborative applications over peer-to-peer systems–challenges and solutions". *Peer-to-Peer Netw. Appl*, № 6, pp. 257–276, 2013. doi: 10.1007/s12083-012-0157-3.
[14] SETI@home. [Online]. Available: http://setiathome.ssl.berkeley.edu/. Accessed on: April 4, 2022.
[15] Md. Sadek Ferdous, Farida Chowdhury, Md. Moniruzzaman. "A Taxonomy of Attack Methods on Peer-to-Peer Network" in *Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security*, India, 2007, pp. 132-138.
[16] Roger Wattenhofer, "Attacks on Peer-to-Peer Networks" in Semester Thesis of Swiss Federal Institute of Thechnolog, 2005, Zurich, pp.1-36.
[17] O. P. Voitovych, Y. V. Baryshev, L. M. Kupershtein, E. I. Kolibabchuk, "Investigation of Simple Denial-of-Service Attacks", *Third International IEEE Conference "Problems of Infocommunications. Science and Technology"*, 2016, Kharkiv, Ukraine, pp. 1-4.
[18] L. Kupershtein, T. Martyniuk, O. Voitovych, B. Kulchytskyi, A. Kozhemiako et al. "DDoS-attack detection using artificial neural networks in Matlab," *Proc.SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-EnergyPhysics Experiments*, 2019. doi: 10.1117/12.2536478.
[19] N. V. Bahniuk, V. M. Melnyk, O. V. Klekha, I. A. Nevidomskyi, "Vydy DDoS-atak ta alhorytm vyiavlennia DDoS-atak typu flood-attack", Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo, vol. 18, 2015, pp.6-12 [in Ukrainian].
[20] Elakrat Mohamed Abdallah, Jung, Jae Cheon. "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication net-work", *Nuclear Engineering and Technology*, no. 50, pp. 780–787, June 2018. doi:10.1016/j.net.2018.01.018.
[21] X. Fan, and Y. Xiang, "Propagation Modeling of Peer-to-Peer Worms", in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Central Queensland University, Rockhampton, Australia, 2010, pp. 1128-1135.
[22] W. Stallings, Cryptography and Network Security: Principles and Practices, 6th ed. Prentice Hall, Upper Saddle River, NJ, 2013, 752 pp.
[23] J. Liang, N. Naoumov, and K.W. Ross, "The Index Poisoning Attack in P2P File Sharing Systems" in *25th IEEE International Conference on Computer Communications. Polytechnic Univerisy*, Brooklyn, NY, 2006, pp. 1-12.
[24] C. Schiller, J. Binkley, D. Harley, G. Evron, T. Bradley, C. Willems, M. Cross, "Botnets − The Killer Web App", Syngress, Rockland, 2007, 482pp. ISBN-10: 1-59749-135-7.
[25] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, D. Wallach, "Secure routing for structured peer-to-peer overlay networks", *SIGOPS Oper. Syst. Rev*, vol. 36, December 2003, pp. 299-314. doi:10.1145/844128.844156.
[26] D. Stutzbach, R. Rejaie, "Understanding churn in peer-to-peer networks" in *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, New York, 2006, pp. 189-202.
[27] A. Vasudeva, M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks", *Journal of Network and Computer Applications*, vol. 120, pp. 78-118, 2018. doi: 10.1016/j.jnca.2018.07.006.
[28] W. Ai, L. Xinsong and L. Kejian, "Efficient flooding in peer-to-peer networks," *2006 7th International Conference on Computer-Aided Industrial Design and Conceptual Design*, 2006, pp. 1-6, doi: 10.1109/CAIDCD.2006.329410.

Відомості про авторів

Куперштейн Леонід Михайлович – кандидат технічних наук, доцент кафедри захисту інформації.

Кренцін Михайло Дмитрович – аспірант кафедри захисту інформації.

Дудатьєв Андрій Веніамінович – кандидат технічних наук, доцент кафедри захисту інформації.

Каплун Валентина Аполінаріївна – старший викладач кафедри захисту інформації.

L. M. Kupershtein, M. D. Krentsin, A. V. Dudatyev, V. A. Kaplun

ANALYSIS OF SECURITY PROBLEMS OF PEER-TO-PEER NETWORKS

Vinnytsia National Technical University, Vinnytsia