УДК 009.4

ТЕХНОЛОГІЇ АНОНІМНИХ МЕРЕЖ

Б. М. Гавриш[1], О. В. Тимченко[2,3], Ю. О. Борзов[4], А. Т. Кобевко[2]

[1]Національний університет «Львівська політехніка»,
вул. Степана Бандери, 12, Львів, 79013, Україна,

[2]Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна,

[3]Uniwersytet Warmińsko-Mazurski w Olsztynie,
ul. Michała Oczapowskiego, 2, Olsztyn, 10-719, Polska

[4] Львівський державний університет безпеки життєдіяльності,
вул. Клепарівська, 35, Львів, 79007, Україна

Подано огляд анонімних мереж, які сьогодні використовуються, побудованих на основі технології цибулевої маршрутизації і піринговых мереж. Описано ключові особливості мереж, наведено їхню порівняльну характеристику. Основна мета будь-якої анонімної мережі — захистити інформацію від зловмисників і забезпечити користувачам високий рівень анонімності. Усі анонімні мережі можна зарахувати до двох класів: з цибулевою маршрутизацією та її модифікації і звичайні однорангові мережі. У першому класі основним представником є Tor, який базується на другому поколінні цибулевої маршрутизації. З іншого боку, мережі P2P можна розділити на 2 класи: традиційні однорангові та friend-to-friend. Friend-to-friend — це тип маршрутизації, коли користувачі підключаються лише до тих користувачів, які вважаються друзями. Перший клас однорангових мереж містить Tarzan, MorphMix, Freenet, I2P, Netsukuku. Другий клас представлений такими мережами, як Turtle, RetroShare. У цій статті увага зосереджена лише на тих мережах, які були успішними на практиці або мають сильний вплив на анонімні системи. Сьогодні користувачі мають широкий спектр різноманітних рішень, які можна використовувати для захисту анонімності в Інтернеті. Анонімні мережі відрізняються архітектурою, типом маршрутизації та цільовою аудиторією. На жаль, не існує жодного рішення, яке гарантувало б 100-відсотковий захист. Кожна технологія має свої слабкі місця та вразливості, що дає змогу зловмиснику якось деанонімізувати певного користувача. Актуальність дослідження анонімних мереж зумовлена необхідністю розробки методів деанонімізації та атак на такі мережі, оскільки ці мережі широко використовують терористи та продавці нелегальних товарів.

Ключові слова: *анонімні мережі, цибулева маршрутизація, невидимий Інтернет, оверлейні мережі, пірингові мережі, шарувате шифрування.*

Постановка проблеми. Сьогодні збільшується контент у мережі «Інтернет» завдяки великій кількості блогів, відео, музики, персоналізованих вебсторінок та програм. Веб 2.0 забезпечив людей такими технологіями, як вікі, подкасти, новинні стрічки, соціальні мережі, хостинг-сервіси та пошукові системи. Доки користувачі створюють контент у відкритих джерелах, будь-якого автора можна відстежити, встановити його особистість, зреагувати вчасно на передачу планів про скоєння злочину або мінування. Але якщо людина хоче приховати своє авторство, передати непомітно для спецслужб якісь цифрові файли і звести до мінімуму свій слід у глобальній мережі?

У такому разі варто говорити про анонімні мережі. Вони дають змогу анонімізувати інтернет-комунікації, зробити складною можливість пов'язати учасників взаємодії (наприклад, користувача та вебсервер, який він відвідав).

Цілком зрозуміло, навіщо такі мережі потрібні зловмисникам, але навіщо вони потрібні звичайним людям? Найбільш очевидною причиною використання інструментів для анонімізації в мережі є запобігання можливості стеження рекламними компаніями за користувачами в мережі, отримання доступу до заблокованих мережевих ресурсів. Уряди використовують анонімні мережі для розвідки та стеження, а люди у країнах, позбавлених свободи слова, використовують їх для спілкування один з одним [1].

Актуальність дослідження анонімних мереж зумовлена необхідністю розроблення методів деанонімізації та атак на такі мережі, оскільки ці мережі широко використовують терористи та продавці нелегальних товарів. Уряди різних країн використовують як технічні механізми протидії анонімності мереж, фінансуючи програми з кібербезпеки, так і юридичні.

Аналіз останніх досліджень та публікацій. *Цибулева маршрутизація.* Так звана цибулева маршрутизація (далі — ЦМ) була розроблена в середині 1990-х років у U.S. Naval Research Laboratory для захисту комунікацій у мережі розвідки США [2]. Згодом компанія Advanced Research Projects Agency її доопрацьовувала та запатентувала у 1998 році [3].

ЦМ — це інфраструктура загального призначення для приватних комунікацій у громадській мережі. ЦМ має інтерфейси для стороннього програмного забезпечення через спеціалізований проксі, що дає змогу без проблем інтегрувати її з наявними системами. Перші прототипи використовували ще з липня 1997 року.

ЦМ працює через динамічну побудову анонімних з'єднань за допомогою міксів Чаума [4] у реальному часі. Мережа з цибулевих маршрутизаторів є розподіленою та контрольованою кількома адміністративними доменами, так що жодний одиничний цибулевий маршрутизатор не може зруйнувати всю мережу або скомпрометувати приватність користувача.

Анонімні сполучення ЦМ є протокол-незалежними та існують у трьох фазах:

- встановлення з'єднання;
- просування даних;
- закриття з'єднання.

Встановлення починається, коли ініціатор створює так звану цибулину, що визначає шлях з'єднання через мережу. Цибулина — це рекурсивна шарувата структура даних, що специфікує властивості сполуки у кожній точці, тобто вона здійснює криптографічний контроль інформації. Кожен цибулевий маршрутизатор протягом маршруту використовує свій публічний ключ для дешифрування всієї цибулини, яку він отримує. Ця операція дає змогу виявити наступний цибулевий маршрутизатор і вбудовану цибулину. Цибулевий маршрутизатор підганяє вбудовану цибулину відповідно до фіксованого розміру і посилає її в наступний цибулевий маршрутизатор. Після встановлення з'єднання дані можна надсилати в обох напрямках. Дані від ініціатора щоразу повторно шифруються з використанням алгоритмів та ключів, встановлених у цибулині. Під час руху даних через анонімне з'єднання кожен цибулевий маршрутизатор прибирає один шар шифрування, заданий криптографічним контролем інформації в цибулині, що встановила маршрут, так що адресат дані отримує вже простим текстом.

Вся інформація (цибулини, дані, мережевий контроль) надсилається через мережу порціями однакового розміру. Всі комірки надходять у цибулевий маршрутизатор через фіксовані інтервали часу і змішуються разом. Цибулина та осередки з даними на різних ділянках мережі мають різний вигляд внаслідок шаруватого шифрування.

Часові та ємнісні характеристики розгортання ЦМ досить малі. Так, час встановлення з'єднання зазвичай не перевищує однієї секунди. Обчислювально складне шифрування з відкритим ключем використовується тільки для передачі симетричного секретного ключа під час фази встановлення з'єднання. Фаза просування даних використовує тільки AES-шифрування (Advanced Encryption Standard) з переданим ключем, що набагато швидше, ніж шифрування з відкритим ключем. Затримка даних визначається кількістю цибулевих маршрутизаторів протягом з'єднання і може відрізнятися залежно від довжини маршруту [5, 6, 7].

Мета статті — дослідження анонімних мереж, що зумовлене необхідністю розроблення методів деанонімізації та атак на такі мережі.

Виклад основного матеріалу дослідження. *Tor (The Onion Router) — цибулева маршрутизація другого покоління.* Tor була створена в центрі високопродуктивних обчислювальних систем дослідницької лабораторії Військово-морських сил США в рамках проєкту Free Haven спільно з DARPA (Defense Advanced Research Projects Agency) на федеральне замовлення. У 2002 р. ця розробка була розсекречена, вихідні тексти передані незалежним розробникам, які створили клієнт-серверний додаток і опублікували його під вільною ліцензією.

Проєкт підтримує правозахисна організація *Electronic Frontier Foundation*, суттєву фінансову допомогу надають Міністерство оборони та Державний департамент США, Національний науковий фонд. Сьогодні TorProject фінансують кілька держав, які зацікавлені у впровадженні технологій анонімізації у повсякденне життя громадян.

Система ЦМ другого покоління має низку переваг порівняно з оригінальною версією: властивість досконалої прямої секретності; контроль навантаження; сервери

каталогів; перевірка цілісності; налаштовуються політики виходу і практичний дизайн для сервісів з прихованою локацією. Tor працює в глобальній мережі «Інтернет», не потребує спеціальних привілеїв та модифікацій ядра, вимагає невеликої синхронізації між вузлами та пропонує розумний компроміс між анонімністю, зручністю використання та ефективністю [8].

Мережа Tor є групою волонтерських серверів. Користувачі Tor використовують цю мережу через підключення до серії віртуальних тунелів, що дає змогу ділитися інформацією через публічні мережі без компрометування приватності.

Розглядаючи відмінні риси браузера Tor поряд з аналогічними проєктами з функціоналом анонімності, найактуальнішим є відкритий вихідний код, що дає змогу здійснювати підключення до мережі навіть через мобільні платформи iOS та Android [8].

Tor, порівняно з іншими браузерами, що використовують VPN, має значну перевагу, що полягає в забезпеченні високої захищеності мережі завдяки своїм особливостям.

По-перше, Tor повністю децентралізований, тобто для нього не існує єдиного централізованого сервера, який контролював би всю мережу цілком, і кожен вузол підключення наданий самому собі.

По-друге, він може працювати поверх будь-якої іншої мережі, у такий спосіб забезпечуючи ергономічність використання цієї платформи.

По-третє, розробники та дослідники браузера відкрили ключовий принцип дії Tor, який полягає у формуванні в маршрутизації волонтерських вузлів, що дає можливість будь-якій людині, яка використовує цю мережу, надати вузол свого підключення як новий вузол мережі іншим користувачам, у такий спосіб сприяючи розростанню мережі та збільшенню її пропускної здатності.

Аналізуючи ці особливості, необхідно зробити висновок, що кількість доступних мережевих вузлів прямо пропорційна кількості користувачів, підключених до мережі, внаслідок чого відбувається підвищення рівня анонімності користувача.

Ще однією відмінністю браузера Tor є технологічність в ланцюжку ретрансляторів. При стандартних налаштуваннях браузера ланцюг підключення складатиметься з трьох вузлів (рис.), проте кількість вузлів можна змінювати через конфігурації підключення.

Першим у ланцюзі підбирається вхідний (сторожовий) вузол, що має доступ до IP-адреси користувача, і тому до технічних параметрів цього вузла виставляються особливі вимоги: він має бути в мережі досить тривалий час (від кількох днів до тижнів), мати високу пропускну спроможність, а також гарантувати стабільність роботи [9].

Другий вузол — проміжний (передаточний), вибирається у випадковому порядку і використовується для передачі трафіку на вихідний вузол. Проміжна адреса не знає як користувача, так і кінцеву точку призначення [9].

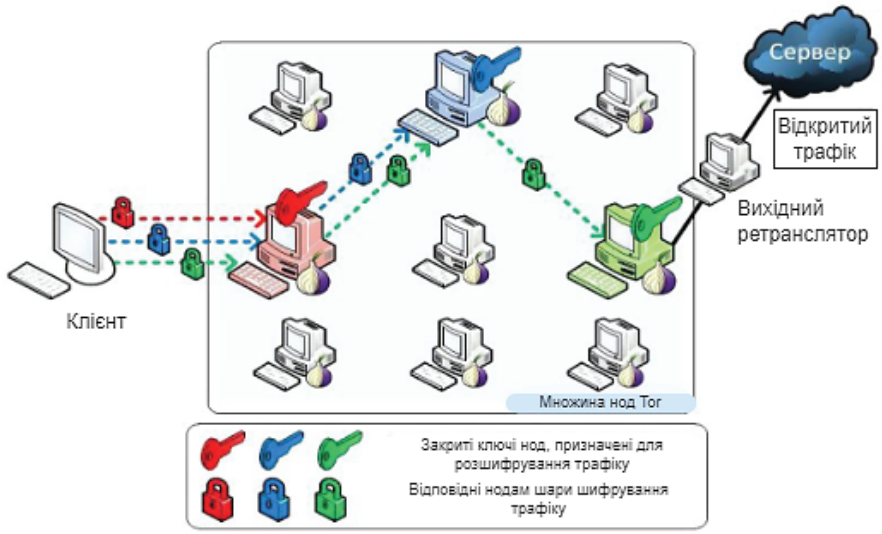

Рис. Принцип функціонування ланцюга Tor

І, нарешті, третім у ланцюзі підключення є вихідний вузол, що обирається мережею за методом, аналогічним вибірці проміжного вузла. Принцип дії та основне завдання вихідного вузла полягає у надсиланні трафіку до пункту призначення, який потрібен конкретному користувачеві.

На кожному з вузлів трафік шифрується, завдяки чому забезпечується шарувате, або по-іншому цибулеве шифрування. Кожні 10 хвилин або за кожного нового під'єднання всі вузли ланцюжка змінюються, внаслідок чого ускладнюється деанонімізація конкретного користувача мережі.

У шляху трафіку по вузлам підключення найбільш вразливим місцем розробники виділяють останній вихідний вузол, на якому будь-який користувач може перехопити пакети HTTP-протоколів, який містить інформацію про історію відвідування сторонніх ресурсів.

Дані містяться у заголовку запиту Referer, який може містити URL-адресу запиту. Для вирішення цієї проблеми можна використовувати протокол HTTPS при підключенні до сайту, якщо є така можливість.

Отже, враховуючи вищезгадані особливості, звернення користувачів до сайту буде приховано навіть на останньому рівні шифрування [9].

Користувачі Tor є тією частиною, яка робить його настільки захищеним. Tor ховає користувача між іншими користувачами у мережі. Таким чином, що більша користувацька база Tor, то сильніше захищається їхня анонімність. На сьогодні кількість людей, які щомісяця використовують Tor, наблизилась до 2 млн, а кількість волонтерських серверів у мережі щодня перевищує 6000.

Мережа Tor є оверлейною. Кожен цибулевий маршрутизатор запускається як нормальний процес на рівні користувача без будь-яких спеціальних привілеїв. Кожен користувач запускає локальне програмне забезпечення, зване цибулевим

проксі (далі — ЦП), для отримання директорій, встановлення ланцюга та забезпечення ланцюга з'єднань. Ці ЦП приймають TCP (Transmission Control Protocol) — потоки та розмножують їх через ланцюги. Цибулевий маршрутизатор з іншого боку ланцюга з'єднується із запитаною кінцевою точкою і передає дані.

Трафік проходить через з'єднання у повідомленнях фіксованого розміру. Кожне повідомлення має довжину 512 байт і складається із заголовка та корисної інформації. Заголовок містить ідентифікатор ланцюга, який специфікує приналежність ланцюга (багато ланцюгів можуть бути розмножені в одному TLS-з'єднанні (Transport Layer Security).

Оригінальна цибулева маршрутизація будувала один ланцюг для кожного TCP-потоку, однак у Tor кожен ланцюг може бути поділений між кількома потоками TCP.

Для створення приватного шляху проходження через мережу за допомогою ЦМ програмне забезпечення користувача або клієнт послідовно будують ланцюги захищених з'єднань через ретранслятори в мережі. Кожен ретранслятор на шляху знає лише те, який ретранслятор надіслав йому дані і якому ретранслятору він повинен їх передати. Ніякий окремий ретранслятор не знає повного шляху, який проходить пакет даних всередині мережі.

Як тільки ланцюг встановлюється, користувач отримує можливість анонімно користуватися інтернетом та переглядати приховані служби Tor.

Зауважимо, що найбільш частою помилкою серед користувачів є їхнє помилкове судження щодо забезпечення анонімності інших програмних продуктів при одночасному їхньому використанні з браузером Tor. Наприклад, користувач встановлює і запускає Tor, а потім запускає інший браузер, наприклад Chrome, і вважає, що його трафік анонімізований на всіх майданчиках.

Але це не так, оскільки Tor захищає ті програми, які працюють через нього. Розробники TorProject паралельно з браузером Tor рекомендують браузер Firefox з плагіном Torbutton. Цей плагін дає змогу відстежувати статус мережі Tor та відключати потенційно небезпечні плагіни (Flash, ActiveX, Java тощо), які можуть порушити анонімність користувача.

Щоб повністю убезпечити свої дії в інтернеті, просунуті користувачі використовують ОС LinuxTails (TheAmne sicIncognitoLiveSystem). Ця операційна система дає можливість запускати анонімайзери практично на будь-якому комп'ютері з USB-накопичувача, а також зберігати конфіденційність та анонімність усіх підключень, які проходять через мережу Tor, і не залишати слідів на технічному пристрої, на якому використовується цей анонімайзер [10, 11, 12].

Пірингові (P2P – Peer-to-Peer) анонімні мережі — це однорангова мережа, що складається з групи рівноправних комп'ютерів. У такій мережі кожен комп'ютер може бути клієнтом, сервером або вузлом для поширення інформації в групі. Мережі P2P поділяють на централізовані та децентралізовані. Своєю чергою децентралізовані мережі ділять на структуровані, неструктуровані та гібридні [13, 14]. Пірингові анонімні мережі є децентралізованими та гібридними. Розрізняють три покоління пірингових мереж [15].

Tarzan — стійка до відмов, масштабована і легкокерована мережа, що є піринговим анонімізувальним оверлейном [16]. Ініціатор повідомлення обирає шлях для пакетно-орієнтованої маршрутизації через псевдовипадково обрані вузли обмеженої топології, таким чином Tarzan надає анонімність клієнту і серверу. Tarzan дає змогу програмам-клієнтам взаємодіяти з інтернет-серверами через спеціальні тунелі.

MorphMix забезпечує просте підключення до системи будь-кого, хто має доступ до інтернету і ефективно оперує великою кількістю вузлів, незважаючи на динамічне середовище і наявність ненадійних вузлів [17]. Сьогодні мережі Tarzan і MorphMix, які належать до пірингових мереж першого покоління, не використовують.

Freenet оперує як мережа ідентичних вузлів, які забезпечують місце зберігання даних і маршрутизацію запитів до них. Враховується бажання користувача фізично розмістити дані у певному домені [18]. Трансляційний пошук або централізований каталог не використовується. Позначення файлів не дають змоги визначити їхнє фізичне розташування, тому неможливо виявити першоджерело або пункт призначення файлу, який просувається через мережу. Кожен вузол має своє власне сховище даних, яке він робить доступним для читання та запису в мережі. Freenet дає можливість користувачам ділитися своїм вільним простором на диску.

Запити для ключів пересилаються від вузла до вузла через ланцюжки проксі-запитів, в яких кожен вузол приймає рішення про те, куди надсилати запит далі. Маршрут визначається залежно від затребуваного ключа. Алгоритми маршрутизації для зберігання та отримання даних були спеціально розроблені для адаптивного налаштування маршрутів у реальному часі.

Кожному запиту виділяється ліміт виходу із проміжного з'єднання, аналогічний часу життя IP-з'єднання. Час життя зменшується у кожному вузлі для запобігання виникнення нескінченних ланцюгів. Будь-якому запиту приписується псевдоунікальний випадковий ідентифікатор. Тому вузли можуть запобігати циклам за допомогою відмови виконувати ті запити, які вони вже обробляли. При виникненні такої ситуації вузол вибирає інший вузол для подальшого з'єднання. Цей процес триває доти, доки запит не буде виконаний або не вичерпає свого часу життя.

I2P (Invisible Internet Project) — мережа є повністю розподіленою, автономною, масштабованою, еластичною та безпечною [19]. Усі компоненти мережі постачаються з відкритим вихідним кодом. Примітною особливістю *I2P*-мережі є те, що вона може бути як оверлейна мережа, що використовується як надбудова над Інтернетом, так і працювати автономно, незалежно від Інтернету.

Мережа не потребує інформації про пункт призначення повідомлення. Аналогічно, отримуючи повідомлення, надіслане через I2P, ніхто не знає, звідки воно надійшло або хто його надіслав, проте відправник може активувати цю інформацію. Окрім того, у машин, що направляють лист зі свого комп'ютера у точку призначення, немає інформації про відправника повідомлення та точку призначення.

У мережі використовується локальна незалежність. Це означає, що під час відправлення до пункту призначення мережі неважливо, де він знаходиться фізично. I2P містить не тільки мережеве програмне забезпечення, але й I2P SDK (Software

Development Kit), у якого є API (Application Programming Interface) кількома мовами, є реалізація маршрутизаторів, які підтримують комунікації тільки з локальними кінцевими точками. Кожен вузол I2P є маршрутизатором, тому немає чітких відмінностей між сервером і клієнтом [20].

Замість посилань на інші роутери та послуги I2P використовує криптографічні ідентифікатори, при цьому відсутній DNS-подібний сервіс (Domain Name System).

Криптографічний ідентифікатор маршрутизатора відрізняється від ідентифікатора сервісу, тому, якщо сервіс буде запущений на якомусь маршрутизаторі, встановлення зв'язку між цими двома ідентифікаторами є практично неможливим. I2P використовує покращений варіант цибулевої маршрутизації, який називають часниковою маршрутизацією (Garlic Routing) [19].

Багато сервісів, наприклад Bittorent, eDonkey тощо, можуть знаходитися всередині мережі I2P [21]. Основні програми, доступні в мережі I2P: Susimail — поштовий клієнт [22], SusiDNS — DNS-клієнт [23], I2Psnark — торрент-клієнт [24], iMule — вільний анонімний клієнт файлообмінної мережі [25, 26].

Netsukuku — це комірчаста мережа з P2P-протоколом, що генерує і підтримує себе автономно. Цей протокол розроблено для оброблення необмеженої кількості вузлів з мінімальним навантаженням на процесор та пам'ять [27].

Мережа встановлюється через комп'ютери, з'єднані один з одним фізично, таким чином вона не є оверлейною. Netsukuku будує маршрути, які з'єднують всі комп'ютери в мережі і є самокерованою і автономною. При додаванні вузла до Netsukuku мережа автоматично переписує топологію, прокладаючи найшвидші та найефективніші маршрути для комунікацій із новоприбулими вузлами. При збільшенні кількості вузлів у мережі вона стає ефективнішою. У Netsukuku немає різниці між приватними та публічними мережами.

Ця мережа є децентралізованою та розподіленою. IP-адреса, що визначає комп'ютер, вибирається випадково, тому неможливо асоціювати його з якимось конкретним фізичним місцем. Маршрути, створені величезною кількістю вузлів, мають високу складність та щільність. Єдиний спосіб контролювати мережу — отримати над нею фізичний контроль, оскільки кожен вузол мережі є її частиною.

Сьогодні маршрутизаторами інтернету керують різні протоколи, такі як OSPF (Open Shortest PathFirst), RIP або BGP, що базуються на різних класичних алгоритмах, здатних знайти кращий шлях для досягнення вузла в мережі.

Ці алгоритми підходять виключно для створення невеликих та середніх мереж, оскільки потребують великих витрат процесорного часу та пам'яті. Жоден з цих протоколів не може бути використаний у такій мережі, як Netsukuku, де кожен вузол є маршрутизатором, оскільки карта всіх маршрутизаторів потребує місця на кожному комп'ютері, підключеному до мережі (приблизно 10 ГБ).

У мережі Netsukuku використовується власний алгоритм, що називається QSPN (Quantum Shortest Path Netsukuku) [28]. У цьому алгоритмі вся мережа подана у вигляді фрактала для обчислення маршрутів, необхідних для підключення вузла до решти. Завдяки фрактальній структурі потрібно лише кілька кілобайт, щоб зберігати всю карту Netsukuku.

Крім мережі Netsukuku, є ще кілька подібних рішень. Так, наприклад, мережа *Hyperboria* є автономною, піринговою бездротовою комірчастою мережею в діапазоні 2,4 ГГц. У такій мережі кожен користувач є сам собі провайдером: з вами не можна розірвати договір про користування інтернетом і підслухати повідомлення спеціальним обладнанням. Мережа є самоналаштовувальною, і кожен клієнт, що під'єднується до мережі, збільшує її ємність. Сучасні протоколи для побудови цієї мережі, такі, наприклад, як мережевий протокол Cjdn, гарантують шифрування всього трафіку, що проходить через мережу [29]. Для держави така мережа має подвійне значення: з одного боку, такий тип мереж дає змогу за менші кошти підключати віддалені регіони до мережі, а з іншого боку — трафік у таких мережах не може бути перехоплений і проаналізований.

Turtle — це мережа F2F (Friend-to-Friend), специфічна форма мережі P2P, у якій користувачі можуть здійснювати прямі з'єднання для обміну інформацією лише з друзями чи користувачами, яким вони довіряють [30]. Передбачається, що у кожного вузла мережі є власник, який має персональний набір даних і бажає отримати доступ до інших даних у мережі.

Кожен набір даних має свій набір властивостей, що складається з пар, які містять атрибут і значення, що використовуються під час оброблення запитів користувачів. Запити складаються із певної кількості пар (атрибут, значення), пов'язаних логічними операторами AND, OR, NOT.

Кожен користувач встановлює криптозахищене з'єднання між своїм вузлом та всіма дружніми вузлами в наборі.

Під час поширення запиту генерується дерево передачі запиту з коренем у вузлі, який направив запит. Дерево будується на основі зв'язків довіри між користувачами і використовується для доставлення відповіді на запит. Щоб зіставити запити з відповідями, кожен вузол зберігає таблицю із запитами, які він ретранслював, але для яких процес відповіді на запит ще не завершений.

Відповідь на запит складається з адреси вузла запиту, фінального біта, ідентифікатора запиту, значення лічильника проміжних з'єднань, відповіді. Фінальний біт використовується для диференціації між частковими та остаточними відповідями. Вузол, що отримує позитивну відповідь від одного зі своїх дітей-вузлів у дереві трансляції запиту, негайно доповість вузлу-батьку. Запит завершується після того, як вузол запиту отримує фінальну відповідь від усіх своїх друзів. Вузол запиту збирає всі частини пакетів відповіді разом, сортує всі часткові відповіді для встановлення окремих наборів атрибутів даних. Як тільки користувач вибирає результат, у якому він зацікавлений, відбувається видача даних.

Мережа RetroShare — нове покоління файлового обміну P2P має T2T-архітектуру. Ця мережа дає змогу встановити шифроване з'єднання між автентифікованими друзями [31]. З'єднання використовується для різних комунікаційних сервісів та файлообміну. Воно не залежить від корпоративної системи або центрального сервера, тому всі дані надсилаються тільки друзям і можуть ретранслюватись через них їхнім друзям, що робить RetroShare децентралізованою соціальною файлообмінною мережею.

RetroShare надає такі комунікаційні послуги:
- приватні чати з друзями;
- приватні або публічні чати;
- листи друзям;
- форуми;
- передача голосу через IP.

Існують інші файлообмінні мережі, наприклад *Guntella*, яка є повністю децентралізованою мережею другого покоління [32], мережі *AntsP2P* [33], *MUTE* [34], *OneSwarm* [35] належать до мереж третього покоління і відрізняються підвищеною безпекою.

Висновки. У статті проведено аналіз анонімних мереж, що успішно застосовуються. На сьогодні користувачі мають широкий вибір рішень, що дають змогу зберегти свою анонімність у глобальній мережі «Інтернет» і навіть розгорнути власний анонімний сервіс. Мережі розрізняються за своєю архітектурою, типом маршрутизації, призначенням і цільовою аудиторією. Однак, попри все різноманіття рішень, немає жодного, яке могло б надати абсолютний захист від зовнішнього спостерігача, оскільки існують більш чи менш ефективні технології деанонімізації.

Підсумовуючи проведене дослідження, зазначимо, що, навіть використовуючи мережу з великою кількістю ретрансляторів і високим рівнем шифрування даних, неможливо забезпечити повну анонімність у мережі «Інтернет». Однак способи та інструкції, запропоновані вище, допоможуть підвищити рівень анонімності та захистити своє підключення під час перегляду певних вебсторінок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Security Strategy. *Whitehouse* [Official website]. URL: https://www.whitehouse.gov/sites/default/ files/docs/2015_national_security_strategy.pdf.
2. Goldschlag D., Reed M., Syverson P. Onion Routing for Anonymous and Private Internet Connections. *Onion Routing* [Official website]. January 28, 1999. URL: http://www.omon-router.net/Publications/CACM-1999.pdf.
3. Patent US 6266704 — Onion routing network for securely moving data through communication networks. *Google* [Official website]. URL: http://www.google.com/patents/ US6266704.
4. Chaum D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Free Haven* [Official website]. URL: http://www.freehaven.net/anonbib/cache/chaum- mix.df.
5. Feigenbaum J., Johnson A., Syverson P. A Model of Onion Routing with Provable Anonymity. *Yale* [Official website]. URL: http://www.cs.vale.edu/homes/if/FJS.pdf.
6. *Onion Routing* [Official website]. URL: http://www.onion-router.net.
7. Feigenbaum J., Johnson A., Syverson P. Probabilistic Analysis of Onion Routing in a Black-box Model. *Yale* [Official website]. URL: http://www.cs.yale.edu/homes/jf/WpES07-Aaron.pdf.
8. Dingledine R., Mathewson N., Syverson P. Tor: The Second-Generation Onion Router. *Tor-project* [Official website]. URL: https://svn.torproject.org/svn/projects/design-paper/tordesign.pdf.

9. Who uses Tor? *Torproject* [Official website]. URL: https://www.torproiect.org/about/torusers.html.en.
10. Biryukov A., Pustogarov I., Weinmann R.-P. Content and popularity analysis of Tor hidden services. *Cryptome* [Official website]. July 29, 2013. URL: https://cryp- tome.org/2013/09/tor-analysis-hidden-services.pdf.
11. Tor Metrics. *Tor project* [Official website]. URL: https://metrics.torproiect.org.
12. Chaabane A., Manils P., Kaafar M. A. Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network. *IEEE* [Official website]. URL: http://ieeexplore. ieee.org/xpl/logmosp?tp=&amumber=5636000&url-http%3A%2F%2 Fieeexplore.ieee.org%2Fxpls%2Fabs_alljsp%3Famumber%3D5636000.
13. Scalable and Secure P2P Overlay Networks. *Wayne State University* [Official website]. URL: http://www. cs.wayne.edu/~weisong/papers/shen04-overlay.pdf.
14. Peer-to-Peer Overlay Networks: A Survey. *California state university Northridge* [Official website]. URL: http://www.csun.edu/~andrzei/COMP529-S05/papers/TR-P2P.pdf.
15. Freedman M. J., Morris R. Tarzan: A Peer-to-Peer Anonymizing Network Layer. *MIT* [Official website]. URL: http://pdos.csail.mit.edu/tarzan/docs/tarzan-ccs02.pdf.
16. Rennhard M., Plattner B. Introducing MorphMix: Peer-to- Peer based Anonymous Internet Usage with Collusion Detection. *Free haven* [Official website]. URL: http:// www.freehaven.net/anonbib/cache/morphmix:wpes2002.pdf.
17. Clarke I., Sandberg O., Wiley B., Hong T. W. Freenet: A Distributed Anonymous Information Storage and Retrieval System. *Stanford University* [Official website]. URL: http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf.
18. Astolfi F., Kroese J., Oorschot J. I2P — The Invisible Project. *Media Technology* [Official website]. URL: http://mediatechnology.leiden.edu/images/uploads/docs/wt2015_i2p.pdf.
19. Maymounkov P., Mazieres D. Kademlia: A Peer-to-peer Information System Based on the XOR Metric. *MIT* [Official website]. URL: http://pdos.csail.mit.edu/~petar/pa-pers/maymounkov-kademlia-lncs.pdf.
20. Supported Applications. *I2P* [Official website]. URL: https://geti2p.net/en/docs/applications/supported#email.
21. *Susimail* [Official I2P website]. URL: http://127.0.0.1:7657/susimail/susimail.
22. *Susidns* [Official I2P website]. URL: http://127.0.0.1:7657/susidns/.
23. *I2psnark* [Official I2P website]. URL: http://127.0.0.1:7657/i2psnark/.
24. IMule. *I2P forum* [Official I2P website]. URL: http://forum.i2p/viewtopic.php?t=2213.
25. Crenshaw A. Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts. *Irongeek* [Official website]. URL: http://www.irongeek.com/Lphp? page=security/darknets-i2p-identifying-hidden-servers.
26. The Netsukuku Wired. *Netsukuku* [Official website]. URL: http://netsukuku.freaknet.org.
27. Quantum Shortest Path Netsukuku. *Arxiv* [Official website]. URL: http://arxiv.org/pdf/0705.0817v1.pdf.
28. Hyperboria — The privacy-friendly network without borders. *Hyperboria* [Official website]. URL: https:// hyperboria.net.
29. Popescu B. C., Crispo B., Tanenbaum A. S. Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System. *NLnet* [Official website]. URL: https://nlnet.nl/project/turtle/2004-cspw.pdf.

30. Retroshare — secure communications for everyone. *Retroshare* [Official website]. URL: http://retroshare. sourceforge.net.
31. Gnutella site archive. *Internet archive Wayback machine* [Official website]. URL: https://web. archive.org/ web/20080525005017/http://www.gnutella.com/.
32. *Ants P2P* [Official website]. URL: http://antsp2p.sourceforge.net.
33. Simple, Anonymous File Sharing. *MUTE* [Official website]. URL: http://mute-net.sourceforge. net.
34. OneSwarm — Privacy preserving peer-to-peer data sharing. *OneSwarm* [Official website]. URL: http:// www.oneswarm.org/index.html.

REFERENCES

1. National Security Strategy. *Whitehouse*. Retrieved from https://www.whitehouse.gov/sites/ default/ files/docs/2015_national_security_strategy.pdf (in English).
2. Goldschlag, D., Reed, M., & Syverson, P. (January 28, 1999). Onion Routing for Anonymous and Private Internet Connections. *Onion Routing*. Retrieved from http://www.omon-router. net/Publications/CACM-1999.pdf (in English).
3. Patent US 6266704 — Onion routing network for securely moving data through communication networks. *Google*. Retrieved from http://www.google.com/patents/ US6266704 (in English).
4. Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Free Haven*. Retrieved from http://www.freehaven.net/anonbib/cache/chaum- mix.df (in English).
5. Feigenbaum, J., Johnson, A., & Syverson, P. A Model of Onion Routing with Provable Anonymity. *Yale*. Retrieved from http://www.cs.vale.edu/homes/if/FJS.pdf (in English).
6. *Onion Routing*. Retrieved from http://www.onion-router.net (in English).
7. Feigenbaum, J., Johnson, A., & Syverson, P. Probabilistic Analysis of Onion Routing in a Black-box Model. *Yale*. Retrieved from http://www.cs.yale.edu/homes/jf/WpES07-Aaron.pdf (in English).
8. Dingledine, R., Mathewson, N., & Syverson, P. Tor: The Second-Generation Onion Router. *Torproject*. Retrieved from https://svn.torproject.org/svn/projects/design- paper/tor-design. pdf (in English).
9. Who uses Tor? *Torproject*. Retrieved from https://www.torproiect.org/about/torusers.html.en (in English).
10. Biryukov, A., Pustogarov, I., & Weinmann, R.-P. **(**July 29, 2013). Content and popularity analysis of Tor hidden services. *Cryptome*. Retrieved from https://cryp- tome.org/2013/09/ tor-analysis-hidden-services.pdf (in English).
11. Tor Metrics. *Tor project*. Retrieved from https://metrics.torproiect.org (in English).
12. Chaabane, A., Manils, P., & Kaafar, M. A. Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network. *IEEE*. Retrieved from http://ieeexplore.ieee.org/xpl/ logmosp?tp=&amumber=5636000&url-http%3A%2F%2 Fieeexplore.ieee.org%2Fxpls%2Fabs_ alljsp%3Famumber%3D5636000 (in English).
13. Scalable and Secure P2P Overlay Networks. *Wayne State University*. Retrieved from http:// www. cs.wayne.edu/~weisong/papers/shen04-overlay.pdf (in English).
14. Peer-to-Peer Overlay Networks: A Survey. *California state university Northridge*. Retrieved from http://www.csun.edu/~andrzei/COMP529-S05/papers/TR-P2P.pdf (in English).

15. Freedman, M. J., & Morris, R. Tarzan: A Peer-to-Peer Anonymizing Network Layer. *MIT*. Retrieved from http://pdos.csail.mit.edu/tarzan/docs/tarzan-ccs02.pdf (in English).
16. Rennhard, M., & Plattner, B. Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. *Free haven*. Retrieved from http:// www.freehaven.net/ anonbib/cache/morphmix:wpes2002.pdf (in English).
17. Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. Freenet: A Distributed Anonymous Information Storage and Retrieval System. *Stanford University*. Retrieved from http://snap. stanford.edu/class/cs224w-readings/clarke00freenet.pdf (in English).
18. Astolfi, F., Kroese, J., & Oorschot, J. I2P — The Invisible Project. *Media Technology*. Retrieved from http://mediatechnology.leiden.edu/images/uploads/docs/wt2015_i2p.pdf (in English).
19. Maymounkov, P., & Mazieres, D. Kademlia: A Peer-to-peer Information System Based on the XOR Metric. *MIT*. Retrieved from http://pdos.csail.mit.edu/~petar/pa-pers/maymounkov-kademlia-lncs.pdf (in English).
20. Supported Applications. *I2P*. Retrieved from https://geti2p.net/en/docs/applications/sup-ported#email (in English).
21. *Susimail*. Retrieved from http://127.0.0.1:7657/susimail/susimail (in English).
22. *Susidns*. Retrieved from http://127.0.0.1:7657/susidns/ (in English).
23. *I2psnark*. Retrieved from http://127.0.0.1:7657/i2psnark/ (in English).
24. IMule. *I2P forum*. Retrieved from http://forum.i2p/viewtopic.php?t=2213 (in English).
25. Crenshaw, A. Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts. *Irongeek*. Retrieved from http://www.irongeek.com/Lphp? page=security/ darknets-i2p-identifying-hidden-servers (in English).
26. The Netsukuku Wired. *Netsukuku*. Retrieved from http://netsukuku.freaknet.org (in English).
27. Quantum Shortest Path Netsukuku. *Arxiv*. Retrieved from http://arxiv.org/pdf/0705.0817v1. pdf (in English).
28. Hyperboria — The privacy-friendly network without borders. *Hyperboria*. Retrieved from https:// hyperboria.net (in English).
29. Popescu, B. C., Crispo, B., & Tanenbaum, A. S. Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System. *NLnet*. Retrieved from https://nlnet.nl/project/turtle/ 2004-cspw.pdf (in English).
30. Retroshare — secure communications for everyone. *Retroshare*. Retrieved from http:// retroshare. sourceforge.net (in English).
31. Gnutella site archive. *Internet archive Wayback machine*. Retrieved from https://web.archive. org/ web/20080525005017/http://www.gnutella.com/ (in English).
32. *Ants P2P*. Retrieved from http://antsp2p.sourceforge.net (in English).
33. Simple, Anonymous File Sharing. *MUTE*. Retrieved from http://mute-net.sourceforge.net (in English).
34. OneSwarm — Privacy preserving peer-to-peer data sharing. *OneSwarm*. Retrieved from http:// www.oneswarm.org/index.html (in English).

doi: 10.32403/1998-6912-2022-2-65-42-56

TECHNOLOGY OF ANONYMOUS NETWORKS

B. M. Havrysh[1], O. V. Tymchenko[2,3], Yu. O. Borzov[4], A. T. Kobevko[2]

[1]National University «Lviv Polytechnic»,
12, S. Bandera St., Lviv, 79013, Ukraine

[2]Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine

[3] University of Warmia and Mazury in Olsztyn,
2, Michala Oczapowskiego St., Olsztyn, 10-719, Poland

[4] Lviv State University of Life Safety,
35, Kleparivska St., Lviv, 79007, Ukraine
dana.havrysh@gmail.com
o_tymch@ukr.net

This paper is an overview of currently used anonymous networks based on technology of onion routing and peer-to-peer networking. It describes key features of the networks and their comparative characteristics. The main purpose of every anonymous network is to protect the information from the adversaries and provide users with a great level of anonymity. All networks can be clustered on two classes: onion routing and its modifications and plain-old peer-to-peer networks. In the first class, the major participant is Tor, which is based on the second generation of onion routing. On the other hand, P2P networks can be divided on 2 classes: traditional peer-to-peer and friend-to-friend. Friend-to-friend is a type of routing where users connect only to those users, who are considered as friends. The first class of peer-to-peer networks contains: Tarzan, MorphMix, Freenet, I2P, Netsukuku. The second class is represented by such networks as: Turtle, RetroShare. Current paper is focused only on those networks, which are successful on practice, or have strong impact on anonymous systems. Nowadays users have a wide spectre of different solutions which can be used for protecting anonymity on the Internet. Anonymous networks differ by architectures, routing types and target audiences. Unfortunately, there is no any solution, which guarantees 100 % defence from adversaries. Every technology has its own weaknesses and vulnerabilities, allowing an attacker to somehow deanonimize a particular user.

It is clear why cybercriminals need such networks, but why do ordinary people need them? The most obvious reason for using tools for anonymization in the network is to prevent the possibility of advertising companies tracking users in the network, gaining access to blocked network resources. Governments use anonymous networks for intelligence and surveillance, and people in countries deprived of free speech use them to communicate with each other.

The relevance of the study of anonymous networks is caused by the need to develop methods of de-anonymization and attacks on such networks, since these networks are widely used by terrorists and sellers of illegal goods. Governments of various countries use both technical mechanisms to counteract the anonymity of networks, financing cyber security programs, and legal

Keywords: *anonymous networks, onion routing, peer-to-peer, layered encryption, invisible internet, overlay networks.*

Стаття надійшла до редакції 16.06.2022.
Received 16.06.2022.