УДК 621.391 (002.56)

Р.О. КОЗАК
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

У статті розглянуто засоби забезпечення технічної анонімності в мережі Інтернет, наведено їх коротку характеристику. Для найбільш поширених механізмів анонімності запропоновано поділ на групи: централізовані засоби анонімності, децентралізовані мережі й гібридні схеми анонімності, витоки та розповсюдження деанонімізуючих даних. Для кожного із типових рішень вказано переваги і недоліки.

Ключові слова: анонімність, інформаційна безпека, комп'ютерні мережі, захист інформації, proxy, VPN, SSH, I2P, Tor.

R.O. KOZAK
Ternopil Ivan Pul'uj National Technical University

THE ANALYSIS OF MEANS FOR ANONYMITY MAINTENANCE IN THE INTERNET

Abstract – The article deals with the technical means to ensure the anonymity of the Internet, they are given a brief description. For the most common mechanisms for anonymity proposed division into groups: centralized means of anonymity, decentralized and hybrid circuits of anonymity, sources and distribution un-anonymously data. For each of the standard solutions are advantages and disadvantages.

There are specialized tools that allow users to log on anonymous and usually decentralized network to ensure the anonymity of the Internet. Most of these networks are freeware and open source, which ultimately has both positive and negative consequences. In each of the analyzed mechanisms have their advantages and disadvantages, and the problem of anonymity is reduced to a choice between overlay (overlay) networks and decentralization using cryptography in both cases.

Despite the fact that now there are enough ways to stay anonymous on the Internet network, achieving absolute anonymity impossible - in almost any situation can choice technical means to identify the user, because the only obstacle is the material resources and time.

Keywords: anonymity, information security, computer networks, information security, proxy, VPN, SSH, I2P, Tor.

Вступ

Нині все більше людей перебувають в «онлайн» – соціальні мережі, ведення бізнесу в розподілених системах, використання засобів обміну мультимедійними повідомленнями, організація навчального процесу, – що призводить до швидкого розвитку інтернет-середовища, його стрімкої трансформації відповідно до потреб користувачів, рівня освоєння ними інформаційних технологій, а також популяризації технічних відкриттів. Разом з тим свобода слова та анонімність (в Інтернет) завжди були важливими соціальними проблемами й дискусійними темами численних судових справ. Актуальність цих проблем з кожним днем зростає внаслідок збільшення кількості людей, які «відкривають» для себе світ цифрових технологій і виявляють потребу в анонімності в цьому суспільстві. Зазвичай під анонімністю розуміють ситуацію, коли автор повідомлення невідомий або авторство встановити складно. Найчастіше статус анонімної набуває інформація, що за суттю є питаннями приватного листування, висловлення своєї позиції з ключових проблем суспільства, консультацій без завдання шкоди репутації тощо.

Постановка і обґрунтування проблеми

Останнє десятиліття відзначилося інтенсивними дискусіями в мережі з приводу того, чи бути анонімності в Інтернет-мережі. Хоча свобода слова й анонімність підтримуються більшістю користувачів, існує й інший бік проблеми – розповсюдження контрафактних матеріалів, забороненого контенту, покривання злочинних угруповань, незаконні дії з електронними платежами, – це накладає негативний відбиток на всі анонімні мережі. Тому злам таких мереж часто стає метою спецслужб й інших органів охорони правопорядку [1]. Зрозуміло, що ці питання не залишені без уваги спільнотою науковців та продовжують вивчатися як соціологічними інститутами, так і з психологічної точки зору [2, 3, 4]. Яким би не був результат цієї дискусії можна констатувати, що технології для анонімності в Інтернет і послуги для її забезпечення стали легко доступними.

В більшості випадків для забезпечення певного ступеня анонімності в глобальній мережі застосовують безкоштовне й загальнодоступне програмне забезпечення і віртуальні мережі. Кожен користувач може вибрати для себе оптимальну програму чи мережу для доступу до внутрішніх і зовнішніх інформаційних ресурсів. Однак чим вища захищеність використовуваної технології, тим нижчі швидкісні показники обміну даними і доступність для розуміння принципів її роботи і застосування. Тому вивчення низки властивостей спеціалізованого програмного забезпечення і рівня надання користувачам послуг з анонімності потребує додаткових досліджень.

Очевидним є те, що технічна складова – це лише незначна частина анонімності в Інтернет. Важливо усвідомити, що надійність будь-якої із реалізованих схем анонімності впирається в засоби: матеріальні ресурси і час, які можуть бути затрачені на їх компрометацію.

Анонімність в мережі доцільно розглядати з таких точок зору [5]:

1) Соціальна анонімність – те, що користувач цілеспрямовано чи несвідомо повідомляє про себе в

соціальних мережах, тематичних форумах, спеціалізованих інформаційно-пошукових системах;

2) Технічна анонімність – ті деанонімізуючі дані, які пов'язані з особливостями використання технічних засобів, протоколів роботи та обміну повідомленнями інформаційних систем, програмного забезпечення.

У статті розглянуто лише технічну анонімність, без висвітлення організаційних, соціальних чи юридичних аспектів та труднощів на шляху розкриття анонімності.

У вказаному контексті можна виділити такі групи найбільш поширених механізмів анонімності:

- централізовані засоби забезпечення анонімності: проксі-, SOCKSx, VPN, SSH;
- застосування схем анонімності Tor (гібридні) і I2P (децентралізовані мережі);
- запобігання витокам та розповсюдженню деанонімізуючих даних.

та проаналізувати переваги, недоліки й особливості застосування кожного із механізмів.

Загалом із вказаної класифікації виокремлюються дві умови, що їх необхідно дотримати для вирішення проблеми анонімності:

1) децентралізація мережі, ліквідація серверної частини;

2) стирання межі між користувачем та IP адресою.

Централізовані засоби забезпечення анонімності

В архітектурі централізованих засобів обов'язковим компонентом є один або декілька центральних вузлів, що здійснюють перенаправлення мережного трафіку, приховування реальних адресів і реквізитів користувача, координацію всієї множини вузлів. Ці засоби вирізняються високою швидкістю роботи, однак наділені невисокою надійністю. До них, зокрема, відносять: http-проксі-сервери, SOCKS-проксі-сервери, VPN-сервіси, SSH-тунелі.

В більшості випадків під проксі-сервером розуміють віддалений комп'ютер і комплекс програм на цьому комп'ютері, що виступає посередником між клієнтом і адресатом для забезпечення обміну повідомленнями між ними.

У контексті забезпечення анонімності виділяють такі ***проксі-сервери*** [5]:

- http-проксі-сервери: пропускають через себе лише http-трафік, додаючи інформацію про застосування проксі;
- SOCKS-проксі-сервери, реалізований на сеансовому рівні OSI: передають всю інформацію без додавання інших даних;
- CGI-проксі або «анонімайзер»: пропонує форму для введення необхідної адреси сайту, може застосовувати протокол https для захисту каналу зв'язку до клієнта.

Переваги:

- послуга дешева, доступні безкоштовні проксі-сервери.

Недоліки:

- необхідно довіряти проксі-серверу;
- необхідність налаштування проксі-сервера;
- протоколи проксі не підтримують шифрування між HTTP/SOCKS/Elite/Anonymous-проксі і клієнтом;
- для http-проксі необхідно фільтрувати http-заголовки.

VPN-з'єднання – технологія емуляції з'єднання «точка-точка» через мережу загального призначення, при цьому між клієнтським комп'ютером і провайдером створюється так званий тунель [6]. Віртуальні приватні мережі часто застосовують для створення безпечних і надійних каналів, що поєднують локальні мережі та забезпечують доступ до них користувачам, які постійно змінюють своє місцезнаходження. Канали VPN захищені алгоритмами шифрування, закладеними в стандарти протоколу безпеки IPSec, який забезпечує захист на мережному рівні.

Часто технологію VPN реалізують через ***SSH*** – мережний протокол прикладного рівня, через який можна здійснювати віддалене управління операційною системою й тунелювання TCP-з'єднань [7]. Весь трафік і паролі при цьому зашифровуються з допомогою алгоритмів, доступних для вибору. SSH дає змогу безпечно передавати по незахищеному середовищу практично будь-який інший мережний протокол.

У контексті анонімності, без врахування деяких відмінностей, основний принцип функціонування VPN і SSH однаковий.

Переваги:

- не потрібно додатково налаштовувати програмне забезпечення.

Недоліки:

- необхідно довіряти VPN/SSH-серверу/провайдеру.

Більшість додатків для браузерів і «програм для анонімності» ґрунтуються на роботі проксі-серверів та VPN-серверів з метою приховування ip-адреси користувача.

Схеми анонімності TOR та I2P

Децентралізація – відсутність єдиного центру контролю та єдиної точки відмови в обслуговувані. ***Децентралізовані мережі*** поділяють на структуровані і неструктуровані [8]. У першому випадку топологію мережі будують за певними правилами, з допомогою яких здійснюється швидкий пошук даних за точним збігом. У неструктурованих мережах наперед невідомо, куди можна відправити запит, тому у найпростішому випадку застосовується варіант флуд-запитів. Однак масштабованість неструктурованих

мереж є доволі проблемною.

Сервіс можна вважати повністю децентралізованим, якщо для його запуску достатньо лише завантажити програмне забезпечення без подальшого введення будь-яких даних для підключення. Такий сервіс має задовольняти базовим принципам [9]:

- OpenSource – програмне забезпечення з відкритим вихідним кодом;
- Zero-Config – запуск програмного забезпечення без додаткових налаштувань;
- нульова довіра – захист від атаки MITM на рівні протоколу;
- низький поріг входу для розуміння технології;
- повністю децентралізований алгоритм роботи.

Недоліки:

- необхідні певні алгоритми маршрутизації та пошуку, які часто не гарантують достовірність результату;
- для ввімкнення у таку мережу потрібно знати координати хоча б одного вузла, відповідно і списки з кількістю адресних даних учасників мережі необхідно публікувати в загальнодоступних джерелах.

Переваги:

- відсутність сервера дає змогу мережі бути відмовостійкою, навіть за значної динаміки кількості користувачів;
- вища ступінь захищеності від цензури.

I2P – це анонімна, само організовуюча розподілена мережа, побудована над Інтернет, використовує модифікований DHT Kademlia зі збереженням хешованих адрес вузлів, зашифровані AES IP-адреси, а також публічні ключі шифрування, причому з'єднання також зашифровані [10, 11]. Ця мережа надає програмам простий транспортний механізм для анонімного та захищеного пересилання повідомлень. Всередині I2P функціонує власний каталог сайтів, електронні бібліотеки і торент-трекери. Крім цього існують точки входу (gate) для доступу в мережу I2P безпосередньо з Інтернету. З кожним новим користувачем зростає надійність, анонімність і швидкість I2P загалом.

Переваги:

- високу ступінь анонімності користувача;
- повна децентралізація;
- конфіденційність даних: наскрізне шифрування між клієнтом та адресатом.

Недоліки:

- низька швидкість передачі даних;
- «свій Інтернет»

Незважаючи на останній недолік, кількість клієнтів I2P зростає [12]. Не останню роль у цьому відіграв ажіотаж довкола повідомлення щодо прослуховування користувачів Інтернет зі сторони NSA в рамках програми PRISM та інших програм, розсекречених Едвардом Сноуденом.

Tor – відкрите програмне забезпечення і система проксі-серверів, яка дає змогу встановити анонімне мережеве з'єднання, захищене від прослуховування. Розглядається як анонімна мережа віртуальних тунелів, що передає дані в зашифрованому вигляді [10, 13]. З допомогою Tor користувачі зможуть зберігати анонімність в Інтернет під час відвідування сайтів, публікації матеріалів, відправлення повідомлень. Анонімізація трафіку забезпечується завдяки використання розподіленої мережі серверів, так званих багатошарових маршрутизаторів. Технологія забезпечує також захист від механізмів аналізу трафіку, що загрожують конфіденційності комерційних таємниць і ділових контактів. Загалом технологія Tor забезпечує роботу в Інтернет у достатньо захищеному режимі, однак для більшої її ефективності необхідний потужний канал зв'язку, оскільки запити проходять через численних користувачів.

Переваги:

- висока ступінь анонімності клієнта за умови дотримання усіх правил;
- простота використання.

Недоліки:

- вихідний трафік прослуховується;
- низька швидкість;
- наявність керуючих серверів.

Варто зазначити, що технологія Tor наділена однією особливістю – приховані сервіси [14]. Користувачі Tor можуть надавати різноманітні послуги – веб-доступ, системи миттєвого обміну повідомленнями, – не розкриваючи свого істинного місцезнаходження. Ця можливість реалізується через спеціальні псевдо-домени *.onion* верхнього рівня.

Безперечно існує багато інших проектів, присвячених анонімності в Інтернет, не враховуючи додатків для браузерів та «програм для анонімності» [15]. Наведення їх тут не видається доречним, оскільки деякі з них вже були скомпрометовані, а інші менше вивчені світовою спільнотою експертів, щоб говорити про їхню надійність.

Іншим прикладом анонімних мереж є мережі побудовані на основі Wi-Fi [16]. У той час, коли при традиційному підході транспортні функції будь-якої анонімної мережі виконує Інтернет, використання безпровідникових рішень дає змогу досягти незалежності від Інтернет-провайдерів.

Витоки та розповсюдження деанонімізуючих даних

Існує чимало методів розкриття відомостей про користувача (ідентифікувати користувача в Інтернет) із відкритих джерел. Варто поділяти інформацію про користувача в мережі на дві категорії: те, що він залишає сам, і те, що про нього без попередження повідомляє програмне забезпечення. В останньому випадку ситуація також неоднозначна – передавання даних може відбуватись як документована функція програми, а може бути результатом експлуатації наявних в цьому програмному забезпеченні вразливостей з метою повного доступу до комп'ютера.

Ідентифікаційну інформацію, яку користувач «залишає» про себе під час роботи в мережі Інтернет [17], і пропозиції щодо запобігання витокам даних представлено у вигляді таблиці 1.

Таблиця 1

«Ідентифікатор»	**Зміст ідентифікуючих даних**	**Спосіб анонімізації**
IP-адреса	Як мінімум інформація про провайдера та країну користувача	VPN, Proxy, SSH, Tor, I2P, P2P-анонімайзери
DNS leaks	Витоки інформації від служби доменних імен; протоколювання активності клієнта виникає, якщо програмне забезпечення відправляє DNS-запити через DNS-сервер провайдера	Використання анонімних мереж; під час роботи через VPN використання примусово статичних DNS-серверів, що належать VPN-провайдеру
MAC-адреса	При підключені до публічної Wi-Fi точки доступу фіксується MAC-адрес мережного інтерфейсу користувача	Зміна MAC-адреси до сеансу підключення
«Профілювання»	Співставлення великого обсягу трафіку, який виходить через один вузол, із конкретним користувачем	Відмова від використання постійних схем (ланцюгів) Tor, регулярна зміна вихідних вузлів
Визначення авторства тексту	Порівняння тексту, написаного анонімним користувачем, та тексту, авторство якого відоме	Проблема активно досліджується[2]; приховування тексту, який можна однозначно пов'язати з автором
Соціальна активність в анонімному сеансі	Розкриття особи користувача під час відвідування ним власного профілю соціальної мережі, незважаючи на засоби анонімності	Недопущення неузгодженої активності в анонімному сеансі

Окремої уваги заслуговує факт одночасного підключення комп'ютера до мережі по анонімному і відкритому каналах. До прикладу, в такому випадку внаслідок розриву інтернет-з'єднання станеться розрив обох з'єднань клієнта з одним і тим самим ресурсом. За цим фактом серверу нескладно буде обчислити і співставити два одночасно завершених з'єднання до ресурсу по анонімному і відкритому каналах. Таку ситуацію можна вважати деанонімізуючою інформацією й для забезпечення анонімності варто не допускати.

Ще одним випадком деанонімізації користувача є передавання програмним забезпеченням, зокрема оглядачами (браузерами), різного роду даних, що зазвичай передбачено специфікацією до програмного продукту. Це обумовлено закладеного у проект програм врахування нормальної і ефективної роботи в складних мережних умовах – обходу блокуючих між мережевих екранів, проксі-серверів тощо.

Типовий оглядач містить наступні функціональні компоненти і технологічні категорії [17, 19]:

- cookies – це текстові файли з деякими даними, що їх зберігають прикладні програми для різних задач, наприклад, аутентифікації. Розкриття анонімного клієнта настає, якщо він спочатку відвідав ресурс через відкритий сеанс, браузер зберіг cookies, а потім користувач з'єднався через анонімний сеанс. В результаті серверу доступно співставлення cookies і, як наслідок, деанонімізація клієнта;
- Flash, Java – плагіни, що ґрунтуються на цих технологіях, завантажуються від імені користувача як окреме програмне забезпечення та можуть працювати в обхід проксі, зберігати свої cookies й інші налаштування;
- відбиток (fingerprint) браузера – оглядач представляє серверу десятки категорій даних, що дає змогу сформувати унікальний цифровий відбиток браузера, за яким його можна ідентифікувати серед багатьох інших навіть в анонімному сеансі (найчастіше застосовується з метою цільової реклами);
- скріпти JavaScript – код, що виконується на стороні клієнта, здатен накопичувати для сервера ідентифікуючу інформацію, а також, за умови вразливості цільового для користувача ресурсу, створює умови для проведення успішних атак на інформаційний ресурс;

[2] В останні десятиліття помітною є тенденція пошуку і виявлення характерних структур авторського стилю з допомогою застосування формально-кількісних та статистичних методів, зокрема [18].

- http-referrer – з допомогою цього http-заголовку цільовий для користувач веб-сайт може визначити, ким було сформовано трафік.

Вирішенням цієї проблеми є налаштування параметрів безпеки оглядача, включаючи блокування кожної із наведених категорій ідентифікації даних, та відмова під час анонімного сеансу від неперевіреного програмного забезпечення.

Висновки

Для забезпечення анонімності в Інтернет існують спеціалізовані утиліти, які дають змогу користувачам входити в анонімну та, зазвичай, децентралізовану мережу. Більшість з таких мереж – безкоштовні програми з відкритим кодом, що, зрештою, має як позитивні, так і негативні наслідки. Зокрема, вільний доступ до вихідного коду є позитивним моментом оскільки створює умови для швидкого виокремлення інсайдерського коду, якщо таке має місце. Негативним наслідком безперечно є можливість зламу діючої мережі на основі проблемного коду, що призведе до деанонімізації клієнтів цієї мережі.

У кожного із проаналізованих механізмів є свої переваги та недоліки, а проблема анонімності зводиться до вибору між оверлейними (overlay) мережами та децентралізацією із застосуванням криптографії в обох випадках. Оверлейні мережі, організовані над протоколом TCP/IP, створюють «свій Інтернет», що породжує суттєвий недолік: низька швидкість роботи і не раціональний розхід трафіку.

Централізовані сервіси слабо протидіють як цілеспрямованим атакам, так і ненавмисним впливам зовнішнього середовища, та мають низьку відмовостійкість. Окрім того жодне централізоване рішення не може забезпечити високого рівня анонімності, так як потрібно довіряти центральному вузлові.

Застосування децентралізованих механізмів дає змогу повністю ліквідувати серверну частину, а для того, щоб «зламати» мережу й демаскувати дані, потрібно скористатися технологіями аналізу трафіку, зокрема Deep Packet Inspection. Тому найкращим шляхом досягнення анонімності в глобальній мережі є поєднання технологій: оверлейні мережі, децентралізація мереж, маскування і шифрування трафіку.

Незважаючи на те, що нині існує достатньо способів залишатися анонімним в Інтернет-мережі, досягнення абсолютної анонімності неможливе – практично у будь-якій ситуації можна дібрати технічні засоби для ідентифікації користувача, бо єдиною перешкодою для цього є матеріальні ресурси і час. Однак завжди відкритим залишатиметься питання актуальності та обґрунтованості застосування цих засобів до конкретних користувачів.

Література

1. FBI: We need wiretap-ready Web sites – now: [Електронний ресурс] / Product reviews and prices, software downloads, and tech news – CNET. – Режим доступу: www/ URL: http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

2. Why Do People Seek Anonymity on the Internet? Informing Policy and Design: [Електронний ресурс] / Ruogu Kang, Stephanie Brown, Sara Kiesler. – Режим доступу: www/ URL: http://www.cs.cmu.edu/~xia/resources/Documents/kang-chi13.pdf.

3. Anonymity on the Internet Must be Protected: [Електронний ресурс] / Karina Rigby // Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1995. – Режим доступу: www/ URL: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html.

4. Anonymity on the Internet: [Електронний ресурс] / Jacob Palme, Mikael Berglund. – Режим доступу: www/ URL: http://people.dsv.su.se/~jpalme/society/anonymity.html.

5. Методы анонимности в сети. Часть 1. Просто о сложном: [Електронний ресурс] / – Режим доступу: www/ URL: http://habrahabr.ru/post/190396/.

6. Надежные и безопасные сети?! : [Електронний ресурс] / Скрыпников Сергей // Спецвыпуск Xakep, номер #041 . – Режим доступу: www/ URL: http://www.xakep.ru/magazine/xs/041/030/1.asp.

7. Secure Shell: [Електронний ресурс] / Wikipedia – the free encyclopedia. – Режим доступу: www/ URL: http://en.wikipedia.org/wiki/Secure_Shell.

8. Quang Hieu Vu, Mihai Lupu, Beng Chin Ooi. Peer-to-Peer Computing: Principles and Applications. – 2010. – 336 Pages.

9. Децентрализация: Какие сервисы уже есть? : [Електронний ресурс] / – Режим доступу: www/ URL: http://habrahabr.ru/post/212653/.

10. Анонимность в сети Интернет : [Електронний ресурс] // КомпьютерПресс 9/2010 . – Режим доступу: www/ URL: http://www.compress.ru/article.aspx?id=21613&iid=987.

11. Introducing I2P : [Електронний ресурс] / – Режим доступу: www/ URL: http://geti2p.net/en/docs/how/ tech-intro

12. Statistics website for the I2P network : [Електронний ресурс] / – Режим доступу: www/ URL: http://i2pstats.loria.fr/?sect=historical&subsect_hist=routers.

13. Tor: Overview: [Електронний ресурс] www/ URL: https://www.torproject.org/about/overview.html.en.

14. Включаем Tor на всю катушку : [Електронний ресурс] / Антон Жуков. – Режим доступу: www/ URL: http://www.xakep.ru/post/50516/.

15. Anonymous P2P : [Електронний ресурс] / Wikipedia – the free encyclopedia. – Режим доступу:

www/ URL: http://en.wikipedia.org/wiki/Anonymous_P2P.

16. 5 Wi-Fi security myths you must abandon now : [Електронний ресурс] / Eric Geier // PCWorld – News, tips and reviews from the experts on PCs, Windows, and more. – Режим доступу: www/ URL: http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html.

17. Методы анонимности в сети. Часть 2. Утечки данных : [Електронний ресурс] / – Режим доступу: www/ URL: http://habrahabr.ru/post/190664/.

18. Распознавание автора текста с использованием цепей А. А. Маркова : [Електронний ресурс] / Д. В. Хмелёв // Вестник МГУ, сер.9: Филология, № 2, 2000, с. 115-126. – Режим доступу: www/ URL: http://www.philol.msu.ru/~lex/khmelev/published/vestnik/vestnik2000.html.

19. "Любопытные" браузеры шпионят за пользователями: [Електронний ресурс] / – Режим доступу: www/ URL: http://www.windxp.com.ru/spybr.htm.

References

1. FBI: We need wiretap-ready Web sites – now: [Elektronniy resurs] / Product reviews and prices, software downloads, and tech news – CNET. – Rezhim dostupu: www/ URL: http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

2. Why Do People Seek Anonymity on the Internet? Informing Policy and Design: [Elektronniy resurs] / Ruogu Kang, Stephanie Brown, Sara Kiesler. – Rezhim dostupu: www/ URL: http://www.cs.cmu.edu/~xia/ resources/Documents/kang-chi13.pdf.

3. Anonymity on the Internet Must be Protected: [Elektronniy resurs] / Karina Rigby // Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1995. – Rezhim dostupu: www/ URL: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html.

4. Anonymity on the Internet: [Elektronniy resurs] / Jacob Palme, Mikael Berglund. – Rezhim dostupu: www/ URL: http://people.dsv.su.se/~jpalme/society/anonymity.html.

5. Metody anonimnosti v seti. Chast' 1. Prosto o slozhnom: [Elektronniy resurs] / – Rezhim dostupu: www/ URL: http://habrahabr.ru/post/190396/.

6. Nadezhnye i bezopasnye seti?! : [Elektronniy resurs] / Skrypnikov Sergey // Spetsvypusk Xakep, nomer #041 . – Rezhim dostupu: www/ URL: http://www.xakep.ru/magazine/xs/041/030/1.asp.

7. Secure Shell: [Elektronniy resurs] / Wikipedia – the free encyclopedia. – Rezhim dostupu: www/ URL: http://en.wikipedia.org/wiki/Secure_Shell.

8. Quang Hieu Vu, Mihai Lupu, Beng Chin Ooi. Peer-to-Peer Computing: Principles and Applications. – 2010. – 336 Pages.

9. Detsentralizatsiya: Kakie servisy uzhe est'? : [Elektronniy resurs] / – Rezhim dostupu: www/ URL: http://habrahabr.ru/post/212653/.

10. Anonimnost' v seti Internet : [Elektronniy resurs] // Komp'yuterPress 9/2010 . – Rezhim dostupu: www/ URL: http://www.compress.ru/article.aspx?id=21613&iid=987.

11. Introducing I2P : [Elektronniy resurs] /: www/ URL: http://geti2p.net/en/docs/ how/ tech-intro

12. Statistics website for the I2P network : [Elektronniy resurs] / – Rezhim dostupu: www/ URL: http://i2pstats.loria.fr/?sect=historical&subsect_hist=routers.

13. Tor: Overview: [Elektronniy resurs] /: www/ URL: https://www.torproject.org/ about/overview.html.en.

14. Vklyuchaem Tor na vsyu katushku : [Elektronniy resurs] / Anton Zhukov. – Rezhim dostupu: www/ URL: http://www.xakep.ru/post/50516/.

15. Anonymous P2P : [Elektronniy resurs] / Wikipedia – the free encyclopedia. – Rezhim dostupu: www/ URL: http://en.wikipedia.org/wiki/Anonymous_P2P.

16. 5 Wi-Fi security myths you must abandon now : [Elektronniy resurs] / Eric Geier // PCWorld – News, tips and reviews from the experts on PCs, Windows, and more. – Rezhim dostupu: www/ URL: http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html.

17. Metody anonimnosti v seti. Chast' 2. Utechki dannykh : [Elektronniy resurs] / – Rezhim dostupu: www/ URL: http://habrahabr.ru/post/190664/.

18. Raspoznavanie avtora teksta s ispol'zovaniem tsepey A. A. Markova : [Elektronniy resurs] / D. V. Khmelev // Vestnik MGU, ser.9: Filologiya, № 2, 2000, s. 115-126. – Rezhim dostupu: www/ URL: http://www.philol.msu.ru/~lex/khmelev/published/vestnik/vestnik2000.html.

19. "Lyubopytnye" brauzery shpionyat za pol'zovatelyami: [Elektronniy resurs] / – Rezhim dostupu: www/ URL: http://www.windxp.com.ru/spybr.htm.

Рецензія/Peer review : 20.1.2014 р. Надрукована/Printed : 26.3.2014 р.