Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: **Методи та програмно-апаратні засоби забезпечення протидії відстеженню та ідентифікації користувачів комп'ютерних мереж при роботі з Інтернет- ресурсами**

Виконав: студент(ка) 6 курсу, групи СІм-61
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

(підпис) Карабан Д.Р. (прізвище та ініціали)

Керівник (підпис) Жаровський Р.О. (прізвище та ініціали)

Нормоконтроль (підпис) Луцик Н.С. (прізвище та ініціали)

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) Козак Р. О. (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« » 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Карабану Дмитру Руслановичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи та програмно-апаратні засоби забезпечення протидії відстеженню та ідентифікації користувачів комп'ютерних мереж при роботі з Інтернет- ресурсами*

Керівник роботи *Жаровський Руслан Олегович, кандидат технічних наук*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*01*» *грудня* *2023* року №1132
2. Термін подання студентом завершеної роботи *26.12.2023 р.*
3. Вихідні дані до роботи *Методи і засоби призначені для анонімного використання Інтернет-ресурсів, методи шифрування трафіку.*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналітичний огляд методів ідентифікації і відслідковування користувачів в мережі інтернет
2 Засоби протидії відстеженню та ідентифікації користувачів комп'ютерних мереж
3 Апробація методів протидії відстеженню і відслідковування користувачів
4 Охорона праці та безпека в надзвичайних ситуаціях
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Актуальність і мета дослідження.
2. Задачі дослідження, об'єкт і предмет, наукова новизна і практична цінність дослідження.
3. Способи ідентифікації та відстеження користувачів в мережі інтернет
4. Засоби протидії відстеженню та ідентифікації користувачів комп'ютерних мереж
5. Компоненти системи протидії відстеження і ідентифікації користувачів
6. Дані про систему без активованої системи блокування відстеження
7. Результати експериментального дослідження.
8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Осухівська Г. М., зав. кафедри КС*		
Безпека в надзвичайних ситуаціях	*Стадник І. Я., професор кафедри ОХ*		

7. Дата видачі завдання *20.11.2023*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз сучасних технічних проблем забезпечення протидії відстеженню та ідентифікації користувачів комп'ютерних мереж*	*01.12.2023*	*виконано*
2	*Визначення задач кваліфікаційної роботи*	*03.12.2023*	*виконано*
3	*Методи забезпечення забезпечення протидії відстеженню та ідентифікації користувачів при роботі в мережі Інтернет*	*10.12.2023*	*виконано*
4	*Проектування і тестування запропонованих засобів забезпечення п забезпечення протидії відстеженню та ідентифікації користувачів*	*16.12.2023*	*виконано*
5	*Охорона праці та безпека в надзвичайних ситуаціях*	*18.12.2023*	*виконано*
6	*Оформлення пояснювальної записки і графічного матеріалу*	*19.12.2023*	*виконано*
7	*Попередній захист кваліфікаційної роботи магістра*	*20.12.2023*	*виконано*
8	*Захист кваліфікаційної роботи магістра*	*26.12.2023*	

Студент _____ *Карабан Дмитро Русланович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Жаровський Руслан Олегович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та програмно-апаратні засоби забезпечення протидії відстеженню та ідентифікації користувачів комп’ютерних мереж при роботі з Інтернет- ресурсами // Кваліфікаційна робота магістра // Карабан Дмитро Русланович // ТНТУ, комп’ютерна інженерія, група СІм-61 // Тернопіль, 2023 // с. – 89, рис. – 29, табл. – 2, бібліогр. – 22.

Ключові слова: ідентифікація, анонімність, захист від відстеження, Tor, VPN, Інтернет.

У кваліфікаційній роботі магістра проведено дослідження методів та алгоритмів протидії відслідковуванню і ідентифікації користувачів комп’ютерних мережі при роботі в мережі Інтернет.

Для вирішення поставленого завдання був проведений аналіз основних методів, які використовуються різноманітними сервісами з метою отримання даних про користувачів.

Також розглянуті засоби протидії ідентифікації і відслідковування користувачів. Проведено їх детальний аналіз з метою виявлення переваг і недоліків.

Сформульовано вимоги до розроблюваної системи блокування відслідковування і ідентифікації. Запропоновано поєднання системи Tor і засобів VPN.

Проведені експериментальні дослідження показали ефективність даної системи.

ABSTRACT

Methods and hardware-software tools for countering tracking and user identification in computer networks when working with Internet resources // Master's graduation thesis // Karaban Dmytro Ruslanovych // TNTU, Computer engineering, group CIm-61 // Ternopil, 2023 // p. – 89, fig. - 29, tab. - 2, bibliography. - 22.

Keywords: identity, anonymity, anti-tracking, Tor, VPN, Internet.

In the Master's thesis, research was carried out on methods and algorithms for combating the tracking and identification of computer network users when working on the Internet.

To solve the task, an analysis of the main methods used by various services to obtain user data was carried out.

Means of combating user identification and tracking are also considered. Their detailed analysis was carried out in order to identify advantages and disadvantages.

The requirements for the developing tracking and identification blocking system have been formulated. A combination of the Tor system and VPN tools is offered.

The conducted experimental studies showed the effectiveness of this system.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ 8

ВСТУП 9

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД МЕТОДІВ ІДЕНТИФІКАЦІЇ І ВІДСЛІДКОВУВАННЯ КОРИСТУВАЧІВ В МЕРЕЖІ ІНТЕРНЕТ 13

1.1. Потреба анонімності та захисту від відстеження і ідентифікації користувачів 13

1.2. Способи ідентифікації та відстеження користувачів в мережі Інтернет 17

1.3. Ідентифікація і відслідковування користувачів з використанням браузерів 19

1.4. Методи і види атак які використовуються для відстеження і ідентифікації користувачів в мережі Інтернет 23

РОЗДІЛ 2 ЗАСОБИ ПРОТИДІЇ ВІДСТЕЖЕННЮ ТА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ..... 27

2.1. TOR 29

2.2. Віртуальна приватна мережа 32

2.3. Використання VPS 38

2.4. Операційні системи для анонімної роботи..... 39

2.4.1. Whonix..... 40

2.4.2. TAILS 41

РОЗДІЛ 3 АПРОБАЦІЯ МЕТОДІВ ПРОТИДІЇ ВІДСТЕЖЕННЮ І ВІДСЛІДКОВУВАННЯ КОРИСТУВАЧІВ..... 44

3.1. Вибір ПЗ та необхідної конфігурації системи 44

3.2. Архітектура системи..... 46

3.3. Налаштування сервера..... 49

3.3.1. Встановлення та налаштування OpenVPN та Easy-RSA..... 50

3.3.2. Генерування сертифікатів 52

3.4. Налаштування клієнтської частини 57

3.5. Тестування запропонованої системи блокування відстеження і ідентифікації 60

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 69

4.1. Охорона праці 69

4.2. Безпека в надзвичайних ситуаціях 72

4.2.1. Фактори, що впливають на функціональний стан користувачів комп'ютерів. 72

4.2.2. Негативний вплив радіоактивного забруднення місцевості після ядерного вибуху на виробничу діяльність промислового підприємства та організації 74

ВИСНОВКИ 76

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 77

Додаток А. Тези конференцій 79

Додаток Б. Установки конфігурації браузера Firefox 85

Додаток В. Конфігураційні файли 87

Додаток Д. Онлайн засоби для тестування системи протидії відстеженню і ідентифікації 89

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ

VPN — Virtual Private Network (віртуальна приватна мережа)

TLS - Transport Layer Security (Протокол захисту транспортного рівня)

VPS – Virtual Private Server (віртуальний приватний сервер)

SSH - Secure Shell (безпечна оболонка), протокол віддаленого доступу

DPI - Deep Packet Inspection (система глибокого аналізу пакетів)

ВМ – віртуальна машина

ПЗ - програмне забезпечення

ВСТУП

Актуальність теми. Проблема розробки та використання ефективних програмно-апаратних засобів спрямованих на запобігання відстеженню та ідентифікації користувачів комп’ютерних мереж у процесі роботи в Інтернеті, залишається актуальною. На сьогоднішній день існує значна кількість аналогічних інструментів, а VPN-сервіси та інші засоби анонімізації набувають популярності. Однак практично всі вони мають свої недоліки.

По-перше, надійне запобігання відстеженню та ідентифікації користувачів є складним завданням, яке включає безліч факторів, і багато сервісів можуть вирішувати це завдання лише частково. Існують випадки ідентифікації користувачів у мережі TOR, яка рекламується як найбезпечніша. Деякі VPN-провайдери також можуть свідомо відстежувати та зберігати історію дій користувачів.

По-друге, використання таких інструментів часто супроводжується зниженням зручності роботи через повільне з'єднання та обмежену функціональність браузера. Для надійного захисту може знадобитися відключення деяких потенційно небезпечних функцій, які є необхідними для багатьох інтернет-сайтів, але при цьому можуть призвести до витоку даних та розкриття особистості користувача.

По-третє, сам факт використання засобів протидії відстеженню та ідентифікації може призводити до різних ознак, які викликають зайву увагу до користувача, що може ускладнювати його роботу та призводити до обмежень доступу на деяких сайтах. Непомітність є ще одним важливим критерієм для ефективного захисту, але більшість існуючих рішень не забезпечують цього.

Крім того, не всі інструменти протидії відстеженню та ідентифікації користувачів комп’ютерних мереж можуть вважатися легкими у налаштуванні та використанні, оскільки вони повинні бути доступними для будь-якого користувача Інтернету, а не лише для тих, хто володіє глибокими технічними знаннями. Надійність складних схем значно залежить від рівня кваліфікації користувача та його розуміння принципів налаштування. Тим не менше, надійна мережева система протидії ідентифікації є важливою для різних категорій користувачів залежно від їх

потреб у безпеці.

Дефіцит актуальних наукових публікацій, зокрема україномовних, у цій галузі також є проблемою, адже багато інформації знаходиться в онлайн-ресурсах та форумах, включаючи анонімні мережі.

Тому необхідним є розробка нових методів які ефективно зможуть запобігати відстеженню та ідентифікації користувачів комп'ютерних мереж у процесі роботи в Інтернеті

Метою кваліфікаційної роботи є оцінка та дослідження засобів спрямованих на запобігання відстеженню та ідентифікації користувачів комп'ютерних мереж, які ефективно поєднують такі важливі характеристики, як надійність, зручність використання, непомітність і простота налаштування. Ці якості часто вважаються несумісними, і важливо визначити граничні можливості їхнього поєднання та шляхи реалізації цього завдання.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

–зібрати та проаналізувати інформацію про різноманітні засоби та методи забезпечення анонімності в Інтернеті, які є актуальними на даний момент;

–уточнити та розглянути фактори, які можуть використовуватися для відстеження користувачів під час роботи в мережі;

–проаналізувати різні шляхи витоку даних, що можуть призвести до порушення анонімності користувачів;

–визначити можливості забезпечення аспектів захисту без втрати зручності роботи з інтернет-сайтами;

–вивчити ознаки, які можуть вказувати на використання засобу анонімізації з боку Інтернет-ресурсів або інших спостерігачів;

–виявити нетехнічні фактори, які можуть призводити до втрати анонімності, зокрема помилки у поведінці анонімного користувача в Інтернеті;

–розробити рекомендації з технічної анонімізації та правил поведінки для різних моделей загроз, щоб надати конкретні рекомендації щодо збереження анонімності та безпеки в Інтернеті.

Об'єкт дослідження: програмно – апаратні засоби спрямовані на запобігання

відстеженню та ідентифікації користувачів комп'ютерних мереж при роботі в мережі Інтернет.

Предмет дослідження: розробка системи запобігання відстеження та ідентифікації користувачів комп'ютерних мереж.

Методи дослідження: Для вирішення поставлених завдань використовуються методи аналізу засобів запобігання відстеження та ідентифікації, методи передачі даних в комп'ютерних мережах, методи тестування для перевірки запропонованих рішень.

Наукова новизна одержаних результатів полягає в розробці методу протидії відстеженню та ідентифікації користувачів комп'ютерних мереж з забезпеченням зручності використання, з точки зору користувача і з мінімальним зменшенням швидкості передачі даних.

Практичне значення результатів кваліфікаційної роботи. Розроблений метод можна використовувати для протидії відстеженню та ідентифікації користувачів при роботі в мережі Інтернет для забезпечення їх анонімності.

Публікації. Результати дослідження апробовано на XI науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології», XII міжнародній науково-технічній конференція молодих учених та студентів «Актуальні задачі сучасних технологій», у вигляді тез конференцій.

1. Карабан Д., Жаровський Р. Методи забезпечення анонімності в Інтернеті.. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 237

2. Карабан Д., Жаровський Р. Аналіз проблем забезпечення анонімності користувачів при використанні мережі Інтернет. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 456.

Структура роботи. До складу кваліфікаційної роботи магістра входить розрахунково-пояснювальна записка та графічний матеріал. Розрахунково-

пояснювальна записка містить вступ, 4 розділи, загальні висновки, список використаних джерел і додатки. Обсяг роботи: розрахунково-пояснювальної записки – 89 арк. формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД МЕТОДІВ ІДЕНТИФІКАЦІЇ І ВІДСЛІДКОВУВАННЯ КОРИСТУВАЧІВ В МЕРЕЖІ ІНТЕРНЕТ

Існує безліч наукових публікацій, присвячених потенційним уразливим анонімним мережам, методикам ідентифікації пристроїв, розробці нових засобів для захисту від найсучасніших технік відстеження тощо.

В роботі [1], описано інструмент для випадкової заміни деяких даних про браузер, доступних через JavaScript, для боротьби з його ідентифікацією. У 2017 році група дослідників зі США опублікувала статтю [2], яка описує техніку розпізнавання комп'ютерів з високою точністю незалежно від браузера, причому автори радять використовувати Tor Browser для протидії таким методам ідентифікації. Стаття дає гарне уявлення про сучасні способи так званого «фінгерпринтінга». Значна частина параметрів пов'язані з обробкою тривимірної графіки WebGL.

В роботах [3, 4, 5] автори описують деякі можливі атаки в мережі Tor і демонструють одну з таких. В роботі [6] розглядається поведінку складних ланцюжків проксі-серверів.

У роботі [7] автори проводить дослідження методів відстеження, які застосовуються в сучасному Інтернеті. Розглядають різні аспекти, такі як шифрування файлів та їх безпечне видалення, використання менеджерів паролів, захист від вірусів, безпечне спілкування за допомогою наскрізного шифрування, анонімні мережі та інше. В книзі також детально описано роботу з системою Tails та інструментами PGP.

1.1.Потреба анонімності та захисту від відстеження і ідентифікації користувачів

Проблема забезпечення анонімності в Інтернеті стала особливо актуальною в 2013 році після розкриття Едвардом Сноуденом інформації про програми масового

збору даних, таких як PRISM. Перед тим анонімність користувачів була не менш важливою, але події цього року привернули до неї особливу увагу.

Визначаючи поняття анонімності в Інтернеті, слід зазначити, що це означає неможливість пов'язати активність користувача з його реальною особистістю та місцем розташування. Формально відзначається різниця між повною анонімністю і "псевдонімом".

Анонімне підключення до сервера означає, що сервер не може визначити початкове походження користувача, таке як його справжній IP-адреса, і не може його ідентифікувати. У випадках, коли є будь-які ідентифікатори (наприклад, Cookie-файли чи унікальні відбитки браузера), які дозволяють серверу визначити, що цей клієнт підключався раніше, ми маємо справу з "псевдо-анонімністю". Велика частина випадків використання Інтернету може обходитися "псевдонімом", і немає потреби робити кожне підключення абсолютно унікальним. Проте тривале використання того самого "псевдоніму" може призвести до накопичення профілюючої інформації про користувача, тому його рекомендується періодично змінювати.

Враховуючи ці аспекти, можна зрозуміти, що використання систем блокування відстеження і ідентифікації користувачів у Інтернет важлива, оскільки вона дозволяє користувачам залишатися невидимими для сторонніх осіб чи систем, запобігаючи асоціації їхньої активності з конкретною особою чи місцем.

При розгляді питань роботи систем блокування відстеження і ідентифікації в Інтернеті важливо усвідомлювати, що анонімність не завжди означає повну відсутність даних користувача. В ряді випадків це технічно неможливо або недоцільно забезпечити. Два приклади цього:

– IP-адреса. Користувач може приховати свій справжній IP-адрес під час відвідування сайту, але технічно неможливо забезпечити абсолютну відсутність IP-адреси. IP-адресу можна лише замаскувати або змінювати, але сервер завжди буде знаходити спосіб визначити IP-адресу, яка надсилає запити інформації.

– User-agent браузера. Замінити User-agent на порожній рядок технічно можливо, але небажано. Такий браузер буде виділятися серед інших і може втратити

анонімність через унікальність. При цьому, багато сайтів може некоректно працювати з таким "псевдонімним" браузером.

Відстеженням користувачів займаються й багато інтернет-компаній (Google є одним з таких прикладів [8]) і більшість веб-сайтів. Тим часом історія дій користувача в Мережі відноситься до особистих даних і не призначена для сторонніх очей, як і особисте листування.

Деякі користувачі використовують системи блокування відстеження і ідентифікації через специфіку їхньої роботи. Тут показовою є інформація про використання Tor у легальних цілях. Корпорації використовують його як безпечний спосіб проведення аналізу на конкурентному ринку, а також як доповнення до VPN. Деякі громадські організації рекомендують використовувати системи блокування відстеження і ідентифікації для забезпечення безпеки своїх членів.

Отже, в умовах сучасного світу надійна Інтернет-анонімність може знадобитися практично будь-якій людині. Однак необхідний та достатній рівень безпеки для різних категорій користувачів буде різним: наприклад, одній людині життєво необхідно ховатися від ідентифікації і відстеження, а іншій потрібна система просто для доступу до заблокованих веб-сайтів. Відповідно, вибір методу забезпечення анонімності починається з чіткого розуміння, навіщо саме потрібна ця анонімність.

Зрозуміло, що досягнення ідеальної безпеки в Інтернеті неможливе, оскільки будь-яке заходження в цю сферу вимагає певних компромісів. Неодноразово зазначається, що ідеальної системи блокування відстеження та ідентифікації в Інтернеті не існує. Тим не менше, можливість забезпечити анонімність у мережі залишається актуальною у випадках, коли це необхідно. Важливо мати на увазі наступне:

– Прослуховування трафіку: Інтернет-провайдер чи власник точки доступу Wi-Fi часто може моніторити частину трафіку, але, як правило, не зацікавлений у активному відстежуванні та деанонімізації користувача. З іншого боку, власники веб-ресурсів використовують різноманітні методи відстеження, такі як витік DNS,

Flash-плагіни, банерні мережі та файли Cookies, з метою ефективної ідентифікації та комерційного використання даних користувачів.

– Витоки інформації: Існує багато каналів витоку інформації, таких як раптове відключення VPN, використання реальної IP через WebRTC чи Flash-плагіни браузера, а також відправка серійного номера програми під час оновлення. Застереженням є те, що постійно з'являються нові шляхи витоку, і спроба блокування кожного з них унікальними методами може бути неефективною.

– Різноманітність засобів підключення до Інтернету: Крім браузера, користувачі часто використовують месенджери, поштові клієнти, торрент-клієнти та інші програми. Інформація, яку вони передають через мережу, може перетинатися, створюючи можливість зв'язку між ними. Наприклад, .torrent-файл, завантажений з веб-сайту, може потрапити в торрент-клієнт, а посилання з листа чи повідомлення може відкриватися в браузері. До цього долучається факт, що операційна система та багато програм регулярно взаємодіють з мережею для оновлень та інших потреб, передаючи різну ідентифіковану інформацію [14].

Отже, часткова "анонімність" не повністю блокує методи ідентифікації користувачів. Хоча вона може бути досить ефективною для вирішення окремих завдань, причому вона практично неефективна в тих випадках, коли необхідна повноцінна система блокування ідентифікації. Розуміючи, що жодна схема не може бути абсолютно надійною, важливо зауважити, що деанонімізація часто виникає через помилки у поведінці самого користувача і технічні методи не завжди можуть забезпечити соціальні аспекти анонімності. Спроби використовувати соціальну інженерію залишаються завжди ефективними. Далі будуть висвітлені поради щодо анонімної поведінки, проте основна увага дослідження спрямована на технічну анонімність - те, що залишається в рамках можливостей програмного забезпечення.

Захист від відстеження обмежений технічними факторами, оскільки його повне блокування не завжди є можливим. З одного боку, багато веб-сайтів використовують елементи, які відстежують користувачів [10], такі як сторонні трекери для реклами, аналітики та інших маркетингових інструментів. На сьогоднішній день існують популярні браузерні розширення для "захисту від

відстеження", які дійсно можуть блокувати більшість таких трекерів. З іншого боку, всі підключення до сервера фіксуються в журналах, тому навіть при наявності анонімності клієнта факт відвідування сайту буде зафіксований.

Наприклад, якщо провайдер в змозі прослуховувати весь трафік, використання VPN не впливає на процес перехоплення, хоча може зробити його менш ефективним. Таким чином, правильніше говорити не про захист від відстеження, а про забезпечення конфіденційності даних в умовах відстеження. Повне усунення відстеження є фактично неможливим.

1.2. Способи ідентифікації та відстеження користувачів в мережі Інтернет

Розглянемо спершу які існують шляхи витоку даних про користувача і які використовуються системами відстеження.

IP-адреса (рис.1.1.), найбільш очевидний ідентифікатор, дозволяє визначити провайдера та країну (нерідко і місто).

Рис.1.1. Засоби відстеження IP адрес

Якщо ж здійснюється цілеспрямований розшук користувача, запит до провайдера дає безліч додаткових даних і в найпростішому випадку встановлює особистість. Будь-який анонімайзер насамперед підміняє IP-адресу. Слід розуміти, що це не впливає на реальний IP хоста, виданий провайдером. Запити так чи інакше перенаправляються на деякий вихідний вузол, адреса якого буде служити «підставним», але головне завдання полягає в тому, щоб зробити визначення

початкового IP максимально скрутним. Також можна проглянути деяку інформацію про користувача можна отримати через адреси поштових серверів які були використані при пересилці електронних повідомлень (рис.1.2).

Рис. 1.2. Заголовки поштових повідомлень

Провайдер DNS. У деяких випадках DNS-запити можуть йти в обхід анонімного каналу. Не всі засоби анонімізації забезпечують захист від витоку DNS.

Атаки профілювання: якщо більша частина трафіку довго виходить в інтернет через один вузол, можна провести так зване профілювання - віднести певну активність до певного псевдоніму, який може бути деанонімізований через інші канали [15].

Прослуховування трафіку на вихідному вузлі, а також MITM – атаки. Особливо важливо за наявності незашифрованого трафіку.

Одночасне підключення до сервера по анонімному та відкритому каналах зв’язку може в деяких ситуаціях створити проблеми, наприклад, при обриві інтернет-з'єднання обидва канали перестануть функціонувати і на сервері потенційно можна буде визначити їх зв’язок, зіставивши час від'єднання користувачів.

Активність в анонімному режимі що спричиняє витік інформації - користування публічними сервісами, особливо тими, на яких вже є інформація про цього користувача.

MAC-адреса зазвичай недоступна кінцевому вузлу, але іноді її підміна має сенс. Є й інші ідентифікатори, що стосуються обладнання та операційної системи, приклади будуть розглянуті далі.

1.3.Ідентифікація і відслідковування користувачів з використанням браузерів

Окрема широка категорія способів ідентифікації, яку слід розглянути докладно. Веб-браузери використовують різноманітні стратегії відстеження користувачів, серед яких варто висвітлити такі ключові методи:

– стандартні HTTP Cookies: Ці файли служать для ідентифікації користувача після першого входу на сайт. Однак їх блокування може призвести до проблем у функціонуванні веб-сайту. З приводу безпеки рекомендується періодично очищати або змінювати cookies;

– сторонні (третя сторона) Cookies: Ці файли встановлюються сторонніми ресурсами і, головним чином, використовуються для таргетування реклами. Блокування їх не негативно впливає на роботу веб-сайту;

– LSO (Local Shared Objects) або Flash Cookies: Ці елементи є загальними для всіх браузерів і залишаються невидаленими стандартними засобами очищення cookies. Зручно вимикати їх зберігання в налаштуваннях Flash Player;

– HSTS SuperCookies: Вони використовують HSTS для збереження ідентифікатора в браузері, але видаляються при очищенні стандартних cookies;

– HTTP Etag: Використовується для перевірки вмісту кешу і може слугувати ідентифікатором, видаляється шляхом очищення кешу;

– Evercookie: Використовує різні механізми зберігання та відновлюється після неповного очищення, включаючи інші методи відстеження;

– HTML5 AppCache: Дозволяє зберігати унікальні дані як ідентифікатор;

– SDCH-словники: Розроблений алгоритм компресії від Google [9], який може використовувати словники для зберігання унікальних ідентифікаторів;

– Ubercookie: Це сучасна версія Evercookie, яка використовує AudioContext API та метод getClientRects для отримання унікальних параметрів браузера. У цьому

випадку використовуються AudioContext API (для отримання набору даних про аудіопідсистему) та метод getClientRects (дає унікальний набір координат). Взагалі, такі способи відстеження можуть використовувати велику різноманітність параметрів, поєднання яких буде унікальним для кожного браузера.

Ці методи викликають значні труднощі в плані анонімізації та захисту конфіденційності користувачів при роботі з веб-сервісами. Важливо бути свідомим і приймати належні заходи для забезпечення особистої безпеки в онлайн-середовищі.

Цифровий відбиток веб-браузера — це унікальний набір параметрів та характеристик, які можуть ідентифікувати конкретного користувача в Інтернеті. Цей відбиток формується на основі різноманітних технічних параметрів, що включають такі аспекти:

–Canvas fingerprinting - відображення прихованого зображення з використанням HTML5 canvas і подальший переведення його в бінарну форму [18]. Причому малюється текст з використанням доступних системі шрифтів і рендерера. Набір шрифтів та методи згладжування трохи різняться на різних машинах. Рендерер залежить від версії браузера, ОС та від GPU. У результаті відмальоване зображення майже унікальне (залишається невелика ймовірність збігу). Існують браузерні доповнення, що дозволяють або блокувати малювання, або замінювати відбиток. При цьому помилкове значення може мати 100% унікальність, але відстежувати по ньому неможливо, оскільки при кожному відвідуванні сторінки генерується новий відбиток.

–WebGL fingerprinting [19] - рендеринг зображення, як і в canvas fingerprinting, але з використанням API WebGL. За наявності WebGL 2 доступний набір даних сильно збільшується. Враховуючи те, що більшість сайтів не використовують WebGL для роботи, відключення WebGL у браузері зазвичай не викликає додаткових проблем, проте це може виглядати підозріло для сучасних антифрод-систем.

–Audio fingerprinting - аналіз обробки звуку аудіопідсистемою, використовує AudioContext API [20]. Вважається дуже ефективним, при поєднанні з відбитком canvas точність ідентифікації практично досягає 100%. Частково змінити відбиток

можна шляхом перемикання частоти дискретизації у системних налаштуваннях динаміків.

–Метод getClientRects дозволяє отримати точний розмір та положення прямокутника у наявному елементі DOM. Дані значення можуть і з часткою ймовірності будуть різнитися на різних комп'ютерах, навіть з однаковою версією браузера. Спочатку було запропоновано для відстеження користувачів Tor Browser [21]. Зміна масштабу сторінки вплине на відбиток.

–Mouse fingerprinting: корисною інформацією є швидкість прокручування колеса миші та руху курсору, доступні для відстеження за допомогою JavaScript. Спосіб відстеження користувачів рухами миші спочатку здавався безглуздим, але, за деякими даними, він успішно використовується на практиці [21]. Таку технологію можна віднести до поведінкового аналізу.

–Заголовки HTTP_Accept містять набір значень, які можуть бути стандартними для багатьох браузерів, але ймовірність їх збігу у двох браузерів становить близько 1:1700.

–Список встановлених плагінів, а також розширень (частково). Від плагінів залежить і список MIME-типів, що підтримуються.

–Набір встановлених шрифтів, окрім впливу на відбиток canvas, може використовуватися і окремо. На їх основі генерується так званий Font fingerprint .

Для оцінки значущості ознак можна використовувати ентропійний підхід. Під ентропією розуміється кількість інформації, що припадає одне елементарне повідомлення джерела, виробляє статистично незалежні повідомлення. Оскільки характеристики на кшталт «майже унікальний» чи «незначний» є точними, дослідники з Electronic Frontier Foundation запропонували кількісну оцінку в бітах ентропії [11]. Так, для Canvas fingerprint ентропія становить близько 15,5 біт, унікальність цього відбитка (якщо не включена заміна) – 1 на 48000.

Навпаки, інформація про те, що в браузері дозволено прийом Cookies, має найнижчу цінність близько 0,2 біт. Існують інші ознаки з відносно низькою ентропією, придатні для відстеження лише у поєднанні з набором інших властивостей: User-Agent. Рядок javascript navigator.userAgent, поля javascript-об'єкта

navigator : appCodeName, appName, appVersion, buildID, oscpu, platform, product, productSub, vendor, vendorSub. Заголовок HTTP Referer і інші.

Представлений перелік параметрів і методів базується на даних, які були зібрані з інтернет-ресурсів, таких як BrowserSpy.dk, panopticlick.eff.org, Whoer.net, browserleaks.com, і не є вичерпним.

Частина визначених властивостей не залежить від конкретного браузера і може використовуватися для ідентифікації користувача незалежно від браузера. Навіть сучасні методи fingerprinting можуть, власне, ігнорувати версію браузера, але все ще надзвичайно точно розпізнавати конкретний комп'ютер завдяки особливостям його апаратної частини та операційної системи [23].

Загалом можна виділити наступні принципи анонімізації браузера: дані з низькою ентропією можуть взагалі не потребувати захисту. Якщо захист необхідний, рекомендується підміняти параметри на максимально поширені значення, уникайте надання їм штучної нестандартності. Проте, важливо періодично змінювати всі або деякі з цих параметрів, оскільки їх комбінація все одно утворює високоентропійний патерн. Щодо даних, таких як canvas-відбиток, які є найціннішими, рекомендується їх змінювати при кожній потребі "змінити особистість".

Ідентифікація та відстеження користувачів може здійснюватися за допомогою особливостей роботи протоколів. Ось кілька прикладів:

Origin Bound Certificates (ChannelID): Самопідписані сертифікати, які ідентифікують клієнта HTTPS-серверу. Кожен новий домен має свій унікальний сертифікат для подальших з'єднань. Можуть використовуватися для трекінгу користувачів без помітних дій з їхнього боку. Криптографічний хеш сертифіката в даному випадку може служити унікальним ідентифікатором.

Session Identifiers та Session Tickets в TLS: Механізми, які дозволяють клієнтам відновлювати перервані HTTPS-з'єднання без повного рукостискання, використовуючи закешовані дані. Ці механізми дозволяють серверам ідентифікувати запити від одного клієнта протягом короткого періоду часу.

Внутрішній DNS-кеш браузера: Такий кеш можна використовуватиме зберігання невеликих обсягів інформації. Наприклад, якщо мати 16 доступних IP-адрес, близько 8–9 закешованих імен буде достатньо, щоб ідентифікувати кожен комп'ютер в Інтернеті. Однак такий підхід обмежений розміром внутрішнього DNS-кешу браузерів і може потенційно призвести до конфліктів у вирішенні імен із DNS-провайдером [10].

1.4.Методи і види атак які використовуються для відстеження і ідентифікації користувачів в мережі Інтернет

Використання різноманітних сервісів та програмно-апаратних засобів не завжди забезпечує безпеку користувачів, оскільки можуть використовуватися наступні засоби ідентифікації та відстеження користувачів.

Отримання реального IP через Flash можливе у випадках, коли анонімізується лише трафік браузера, а не всієї системи. При використанні проксі-сервера можна примусово надіслати через нього Flash-трафік за допомогою програм, таких як Proxifier. Якщо при анонімній роботі не потрібна наявність Flash-плагіну, рекомендується його відключати.

Отримання IP через WebRTC може відбуватися навіть за використання VPN. Зазвичай WebRTC не потрібно для роботи сайту, і його відключення в браузері не викликає проблем, але існують способи підміни IP, що може розкрити користувача.

Отримання реального DNS може призводити до явної невідповідності між IP-адресою та використовуваним DNS-сервером, а також опосередковано розкривати інтернет-провайдера. Використання публічних DNS-серверів (наприклад, Google) не вважається підозрілим. У випадку, якщо VPN-клієнт не забезпечує стабільний захист від такого витоку, доцільно використовувати DNSCrypt, вибравши адресу DNS тієї країни, якій відповідає змінена IP-адреса. Навіть якщо неможливо забезпечити відповідність, це убезпечить від витоку оригінального DNS.

Невідповідність браузерних даних про ОС та характерні особливості TCP для цієї ОС може бути використана для точного визначення ОС та її версії за допомогою

утиліти p0f. Однак при використанні проксі-сервера буде визначена ОС, на якій працює проксі, оскільки він генерує пакети. У результаті розбіжності цих даних з User-agent браузера можна припускати або заміну User-agent, або використання проксі-сервера.

Приналежність IP-адреси до мережі Tor очевидно вказує на використання Tor, оскільки адреси всіх вихідних вузлів відомі. Використання VPN через TOR – один із способів вирішення проблеми.

Розбіжність часового поясу може вказувати на заміну IP. Невідповідність системному часу означає необхідність зміни налаштувань часу.

Заголовки HTTP Proxy, які передають IP-адресу клієнта за проксі, можуть містити реальний IP. Також існує тактика імітації використання проксі, коли в порожній заголовок вставляється випадкова IP-адреса, що створює враження, що основна IP є адресою проксі-сервера. Наприклад, плагін Dolus використовує цей метод.

Відкриті порти є характерними для проксі, веб-проксі та VPN. Зазвичай вони використовують нестандартні порти, часто з авторизацією.

Так званий VPN fingerprint – виявлення використання VPN за характерними значеннями MTU/MSS та іншими ознаками, особливо актуальним для OpenVPN [18].

Підозрювальна назва хоста, що містить слова, такі як "vpn", "hide", "proxy" та інші, може вказувати на використання VPN або проксі-сервера. При налаштуванні власного VPN або проксі-сервера рекомендується уникати "розмовних" імен, але переважно вказувати повну відсутність імені, доступного для зовнішніх зворотних DNS-запитів.

Визначення тунелю за двостороннім пінгом, запущеним до IP клієнта з боку сервера або через XMLHTTPRequest з боку браузера, може вказувати на наявність тунелю, якщо різниця у часі петлі перевищує 30 мс. Спосіб не завжди ефективний.

Мова браузера, яка є нехарактерною для країни, визначеної IP, може вказувати на використання анонімайзера, але можливі винятки. Якщо є лише англійська мова, то цей параметр вважається нейтральним.

Приналежність IP-адреси хостинг-провайдеру: зазвичай вказує на використання VPS.

Також існують атаки підтвердження (Confirmation of Attack) що базуються на можливості зловмисника визначити, який саме мережевий ресурс відвідує користувач через анонімну мережу. Зловмисник використовує припущення щодо цього ресурсу і намагається підтвердити або спростувати свої гіпотези. Для цього він отримує дані трафіку від точки входу користувача до анонімної мережі та від точки виходу з неї до цього ресурсу чи на самому ресурсі.

У мережах з малою затримкою передачі даних виявляться кореляції за кількістю пакетів, часом їх відправлення та іншими параметрами. Це дозволяє злоумиснику обчислити користувача за один сеанс з високою ймовірністю, наприклад, більше 90%, і ймовірність помилки може бути дуже низькою, менше за тисячну частку відсотка.

Якщо злоумисник використовує активні методи, такі як введення затримок в трафік або пошкодження пакетів, то для повного розкриття користувача іноді може бути достатньо одного пакета даних.

Важливо відзначити, що ці атаки можуть бути ускладнені проти прихованих ресурсів, таких як Tor, або замкнутих файлообмінних мереж, наприклад, Freenet, де противнику може бути невідомо, звідки знімати трафік, навіть якщо він знає, до якого ресурсу хоче звернутися користувач. Однак подібні атаки залишаються ефективними в деяких випадках.

Атака перетину, або атака кореляції (англ. "Intersection Attack" або "Traffic Correlation Attack") - це вид атак на анонімні мережі, такі як Tor чи інші системи, які призначені для захисту конфіденційності та анонімності користувачів. Метою атаки перетину є встановлення відповідності між входом і виходом в анонімній мережі, тобто ідентифікація того, хто відправляє певний трафік, який виходить з анонімного сервісу чи вузла.

Основні риси атаки перетину:

–кореляція трафіку: Зловмисник намагається виявити співвідношення між тим, що виходить з анонімної мережі, і тим, що входить в цю мережу;

–статистичні параметри: Атака може використовувати статистичні параметри трафіку, такі як обсяг даних, час передачі, напрямок руху, для встановлення зв'язку між входом і виходом;

–обхід криптографії: Атака перетину спрямована не на обхід криптографії, а на виявлення кореляцій у вже розшифрованому трафіку, який знаходиться поза анонімною мережею;

–деанонімізація користувача: У випадках успішної атаки перетину, зловмисник може деанонімізувати користувача, встановивши зв'язок між його входом і виходом з анонімної мережі;

–протистояння атакам перетину включає в себе розробку технічних заходів, таких як покращення алгоритмів маршрутизації, захист від статистичного аналізу трафіку, а також удосконалення самої концепції анонімних мереж. Заходи включають у себе використання мережевих технологій, що запобігають атакам перетину, і вдосконалення протоколів обміну даними в анонімних мережах.

Висновок до 1 розділу.

Сучасні технології відстеження далеко виходять за рамки традиційних способів на кшталт cookie-файлів, і боротьба з ними стає досить складним завданням. Приховування особистості як таке може здатися відносно простим, але насправді містить багато неочевидних нюансів.

Ідентифікуючі дані необхідно не просто приховувати, а й регулярно змінювати, оскільки статичний «псевдонім» схильний до відстеження не менше, ніж реальна особистість. Найбільшою складністю може бути заміна цифрових відбитків зі збереженням їх повної правдоподібності. Атаки перетину та підтвердження можуть бути ефективними, і деякі заходи захисту визнаються обмеженими, оскільки захист від противника такого рівня є вельми складним завданням.

Тому необхідним є поєднання використання різноманітних систем забезпечують анонімність роботи користувачів в мережі Інтернет.

РОЗДІЛ 2
ЗАСОБИ ПРОТИДІЇ ВІДСТЕЖЕННЮ ТА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ

Проксі-сервери є кілька видів зі своїми особливостями, але зазвичай для анонімізації використовуються SOCKS5. В даний час не можуть вважатися надійними, так як самі по собі не забезпечують шифрування трафіку, а також порівняно легко піддаються деанонімізації навіть при побудові проксі ланцюжка: послідовне вивчення логів на кожному сервері дозволяє визначити реальний IP при будь-якій довжині ланцюжка. Переважно використання у поєднанні з VPN.

VPN-сервіси – також є кілька протоколів, сервіси найчастіше платні, забезпечують високу надійність шифрування каналу. Але, як і у разі проксі-сервера, основною проблемою стає питання довіри до провайдера сервісу. Переважна більшість VPN-провайдерів заявляє про відсутність ведення логів, насправді це неможливо перевірити, найчастіше логування ведеться. Також VPN має такий недолік: при раптовому розриві VPN-підключення весь трафік піде в інтернет безпосередньо, що призводить до розкриття реального IP. Проблема вирішується додатковим настроюванням правил файрвола.

SSH-тунелі спочатку створювалися (і застосовуються досі) для інших цілей, але використовуються і «для анонімності». Частково схожі з VPN щодо шифрування трафіку, але мають інші принципи роботи та потенційно нижчу швидкість. На відміну від VPN, не направляють за умовчанням весь трафік у тунель (хоча для цього існують спеціальні програми), а використовуються на зразок локального проксі-сервера.

Dedicated-сервери – застосовуються як віддалене робоче місце або як платформа для запуску свого VPN-сервера. Нерідко використовують віртуалізацію (VPS), коли на одному фізичному хості розташовується кілька віртуальних серверів, що ускладнює відстеження підключень до конкретного серверу [15].

Анонімна мережа Tor. Деякий час вважалася найбільш надійним засобом забезпечення анонімності в Інтернеті, надалі були випадки деанонімізації

користувачів. Трафік на багатьох вихідних вузлах прослуховується, до того ж вихід у мережу з IP-адреси, що належить Tor, сам по собі розцінюється як підозрілий.

JonDonym, або JAP (Java Anonymous Proxy). Направляє трафік через ланцюжок серверів, користувач може сам вибирати «каскади», що використовуються. Є безкоштовний та преміум-доступ. Браузер JonDoFox в ранніх версіях був збиранням Firefox з набором доповнень, а в даний час це модифікований Tor Browser.

I2P – анонімна, децентралізована мережа, що працює поверх інтернету, яка не використовує IP-адресацію. Перевершує Tor за надійністю шифрування даних, що передаються. Іноді позиціонується як альтернатива Tor, але насправді малопридатна для анонімізації доступу до зовнішнього інтернету (спочатку не була призначена для цього) через нестабільне та повільне підключення, особливо за відсутності публічної IP-адреси.

Віртуальні машини – вирішують низку додаткових завдань безпеки під час анонімної роботи, використовують у комбінації коїться з іншими засобами. Гарантовано направити весь трафік віртуальної машини в VPN або Tor канал зазвичай легше, ніж зробити це з трафіком основної системи. Браузер усередині віртуальної машини не має доступу до даних про апаратне забезпечення фізичного хоста. Рекомендується використовувати в гостьовій системі оформлення, що помітно відрізняється від основної, щоб випадково не переплутати вікна. Особливо важлива візуальна відмінність браузерів. Не допускається встановлення програмного забезпечення з ліцензією, пов'язаною з реальними даними користувача, щоб уникнути витоку цих даних в анонімний канал [27].

Так звані «антидетекти» – складання браузерів із вбудованою заміною різних ідентифікаторів. Часто створюються для нелегальної діяльності (спрямовані на обхід систем антифроду), мають високу вартість і не викладаються у вільний доступ. Зустрічаються і безкоштовні рішення з різним ступенем ефективності. Завдання анонімізації трафіку зазвичай залишається на розсуд користувача. Термін "антидетект" також застосовують до віртуальних машин, модифікованих для правдоподібного маскування під реальний ПК.

Інші засоби анонімізації - слабо популярні, недостатньо перевірені чи не забезпечують надійну анонімність інструменти. Також сюди відносяться програми та браузерні розширення, призначені для захисту від відстеження браузера. Вони доповнюють систему анонімізації у тих аспектах, які забезпечуються засобами, переліченими вище.

Як бачимо з даного короткого огляду є значна кількість засобів, що дозволяють забезпечити захист від відстеження і ідентифікації користувача. Розглянемо більш детально їх принцип роботи з метою виявлення їх сильних і слабких сторін.

2.1.TOR

The Onion Router – найбільш популярний засіб для забезпечення анонімності в Інтернеті. Архітектура мережі наведена на рис. 2.1. Це вільне і відкрите ПЗ, що працює за принципом так званої цибульної маршрутизації: всі дані, що потрапляють в мережу TOR, проходять через три вузли мережі, що вибираються випадковим чином, а перед відправкою послідовно шифруються ключами вибраних вузлів.

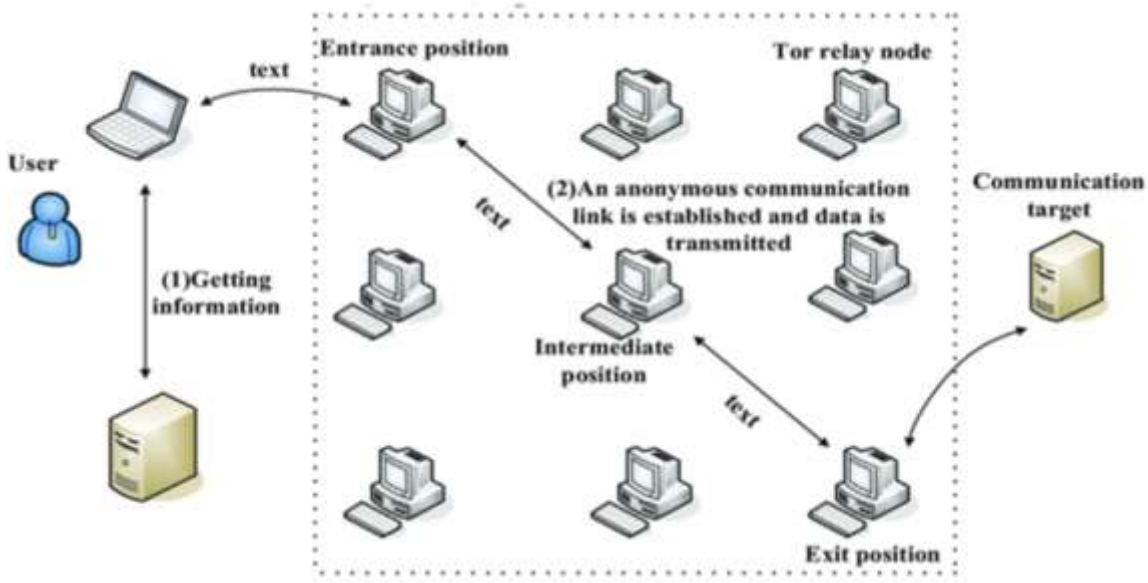

Рис.2.1. Архітектура мережі TOP

Коли перший вузол отримує пакет, він розшифровує верхній шар шифру (звідси аналогія з чищенням цибулини) і дізнається, куди відправити пакет далі. Аналогічно надходять другий та третій сервер (рис.2.2). Найбільш уразливим місцем у такому ланцюжку стають вихідні вузли (exit nodes), на яких трафік остаточно розшифровується та прямує до цільового ресурсу. На вихідних вузлах трафік може прослуховуватися, і це слід пам'ятати у випадках, коли з'єднання з ресурсом відбувається за небезпечним протоколом — наприклад, відвідується сайт, який підтримує HTTPS [28].

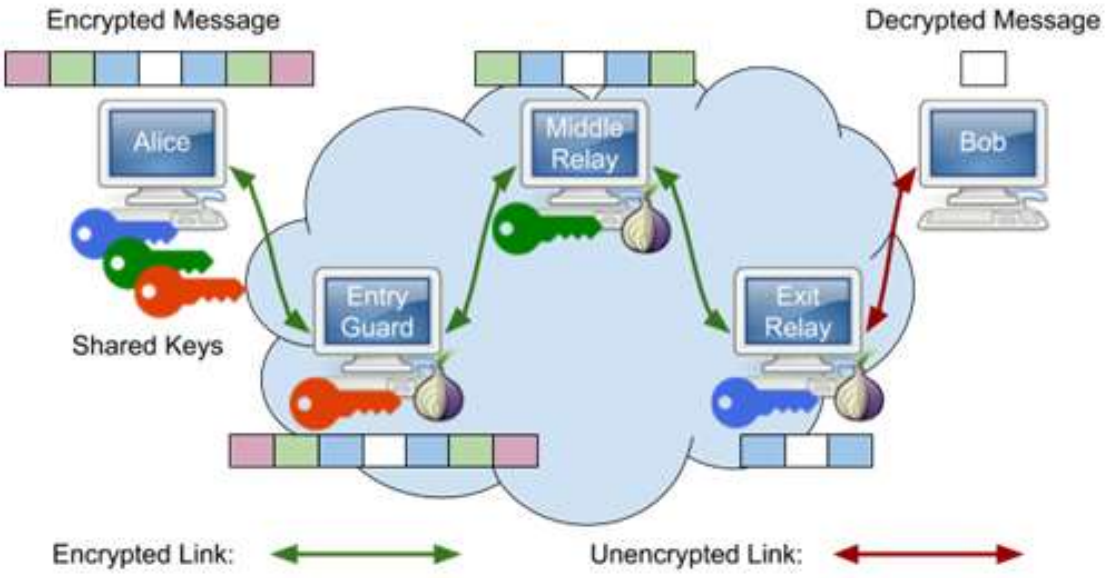

Рис.2.2. Процедура шифрування даних мережею TOR

Фактично, TOR є мережею проксі-серверів, що шифрують, або віртуальних тунелів, що підтримуються переважно добровольцями. На 2017 рік ця мережа має близько 7000 вузлів, з яких 11% є вихідними вузлами [29]. Таким чином, кількість можливих маршрутів є дуже великою, до того ж TOR забезпечує зміну маршруту кожні 10 хвилин.

Вхідні вузли (entry nodes) забезпечують захист від перехоплення та підробки даних на шляху між вхідним вузлом та клієнтом. Крім того, існують мости (bridges) - ретранслятори, адреси яких не публікуються в загальному каталозі, а надаються за запитом клієнта [30]. Мости забезпечують доступ до мережі в тих випадках, коли

інтернет-провайдер блокує відомі вхідні вузли TOR, а також виконують маскування трафіку, що перешкоджає його ідентифікації та блокуванню системами DPI. Розроблено кілька типів мостів, в даний час найбільш ефективним є obfs4.

Ймовірно, для багатьох користувачів знайомство з Tor обмежується роботою Tor Browser. Ця збірка складається з програми Tor та модифікованої версії браузера Firefox. Сучасні версії є порівняно надійним і при цьому доступним інструментом для протидії відстеженню та збереженню анонімності. Багато покращень Tor Browser поступово впроваджуються у звичайний Firefox (проект Tor Uplift). Однак слід чітко розрізняти Tor Browser і Tor, який може бути запущений і без браузера. Раніше широко застосовувався додаток Vidalia - графічний інтерфейс для управління вузлом Tor, але його розробка була припинена. Існує також AdvOR (Advanced Onion Router), що дозволяє примусово спрямовувати трафік додатків через Tor та налаштовувати різні параметри роботи вузла. Взагалі кажучи, звичайний Tor Browser також дозволяє використовувати Tor як проксі-сервер для різних програм. Поки Tor запущено, він надає локальний інтерфейс SOCKS5, параметри якого можна побачити в налаштуваннях проксі-сервера Tor Browser. Для програм, які не підтримують роботу через проксі, можливе використання програми Proxifier або вищезазначеного AdvOR. Важливе обмеження: Tor підтримує лише TCP-трафік, але не UDP. У випадку, коли потрібне функціонування UDP, буде потрібно додаткове тунелювання UDP-трафіку через VPN.

Основний недолік Tor Browser - у тому, що факт його використання легко визначається з боку ресурсу. Перш за все, IP-адреси вихідних вузлів Tor відомі, і деякі сайти обмежують доступ з таких адрес, оскільки Tor нерідко використовується зловмисниками. Також Tor Browser має характерні цифрові відбитки (fingerprints). Механізми боротьби з відстеженням, що використовуються даним браузером, роблять усі екземпляри Tor Browser невідмінними один від одного (або, у всякому разі, прагнуть цього), тому відстежити конкретного користувача дуже складно, проте неважко розпізнати, що він використовує Tor Browser. Зрозуміло, це не стосується внутрішніх сайтів мережі Tor, onion-ресурсів, які безпосередньо призначені для відвідування через Tor.

Мережа Tor вважається надійним засобом анонімізації, але випадки розкриття особи користувачів.

Уразливість Tor до атак, що аналізують трафік, відома давно. Оригінальна проектна документація вказує на вразливість системи перед «глобальним пасивним зловмисником», здатним прослуховувати весь трафік вхідних та вихідних вузлів. Зіставивши обидва потоки трафіку, подібний зловмисник може деанонімізувати кожного користувача. Насправді це можливо в менших масштабах, оскільки жодна організація не здатна контролювати повністю всю мережу Tor, проте наявність навіть двох контрольованих вузлів (вхідного та вихідного) вже дає шанс ідентифікувати деяку, хай і мізерно малу частину користувачів, чий трафік пройде через обидва вузла [34]. Tor спочатку не був спроектований для протистояння масштабним атакам, коли зловмисник має безліч точок присутності в мережі. Тут доречно згадати мережу I2P, створену з урахуванням того, що кожен вузол може прослуховуватись.

Отже, в даний час Tor залишається порівняно ефективним вільним інструментом для забезпечення анонімності та протидії відстеженню (Tor Browser), продовжує активно розроблятися та отримувати нові механізми захисту. Однак його використання пов'язане з деякими незручностями та не є достатнім для надійної анонімізації.

Доцільно розглядати Tor як основу для побудови складніших комбінацій.

2.2. Віртуальна приватна мережа

Технологія Virtual Private Network, призначена для захищеної передачі за допомогою шифрованого тунелю між двома вузлами, на сьогоднішній день стала популярним способом анонімізації і часто сприймається Інтернет-користувачами як альтернатива Tor. Фактично це неправильно – збереження анонімності тут повністю спирається на довіру до VPN-провайдера, за винятком випадків, коли користувач налаштовує власний VPN-сервер. Коректніше стверджувати, що VPN забезпечує приватність даних, наприклад, дає змогу приховати від інтернет-провайдера історію

активності користувача. При цьому швидкість з'єднання у платних VPN зазвичай набагато вища, ніж у Tor.

Існує кілька найпоширеніших протоколів VPN:

– PPTP (рис.2.3). Швидкий, легко настроюється, але порівняно небезпечний і застарілий. Point-to-Point Tunneling Protocol був винайдений Microsoft і тривалий час був стандартним протоколом VPN. Для забезпечення безпеки він спирається різні методи аутентифікації.

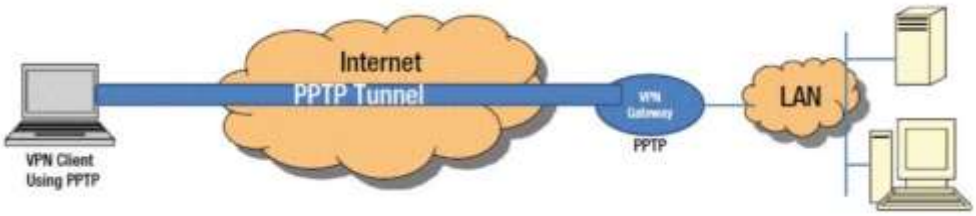

Рис.2.3. Організація тунелю PPTP

Хоча PPTP зазвичай використовується зі 128-бітовим шифруванням, у 1999 році було знайдено низку вразливостей. Найсерйознішою виявилася вразливість протоколу аутентифікації MSCHAP v.2, і з її використанням PPTP було зламано протягом 2 днів. І хоча Microsoft виправила цю помилку за рахунок використання протоколу аутентифікації PEAP замість MSCHAP, вона сама рекомендувала використовувати для VPN протоколи L2TP або SSTP [35].

– L2TP/IPsec (рис.2.4.). Протокол тунелювання рівня 2, на відміну інших протоколів VPN, не шифрує і не захищає дані. Тому зазвичай використовують додаткові протоколи, зокрема IPSec, з допомогою якого дані шифруються ще до передачі. Усі сучасні пристрої та системи, сумісні з VPN, мають вбудований протокол L2TP/IPSec.

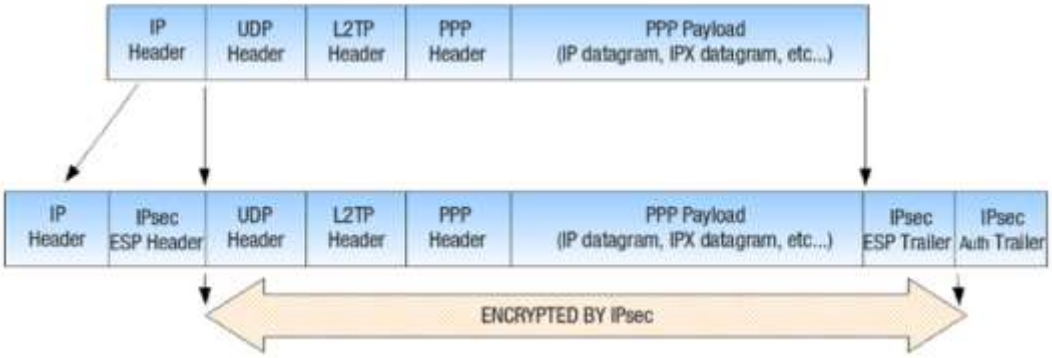

Рис.2.4. Структура пакетів L2TP до та після інкапсуляції IPsec

Встановлення та налаштування здійснюються легко і не займають багато часу, проте може виникнути проблема з використанням порту UDP 500, який блокується файрволами NAT. Отже, якщо протокол використовується з брандмауером, може знадобитися переадресація портів. Не відомо про будь-які великі вразливості IPSec, і при правильному застосуванні він забезпечує надійний захист даних. Однак, двократне інкапсулювання даних робить протокол не таким ефективним, як, наприклад, рішення на основі SSL, і тому він працює повільніше за інші протоколи.

– OpenVPN —технологія що використовує бібліотеку OpenSSL та протоколи SSLv3/TLSv1, а також інші технології для надійного створення віртуальної приватної мережі (VPN). Однією з ключових переваг є його висока гнучкість у налаштуваннях, здатність працювати на різних портах, зокрема на 443 TCP-порту, що дозволяє маскувати трафік, надаючи йому вид звичайного HTTPS і роблячи блокування важким завданням (рис.2.5).

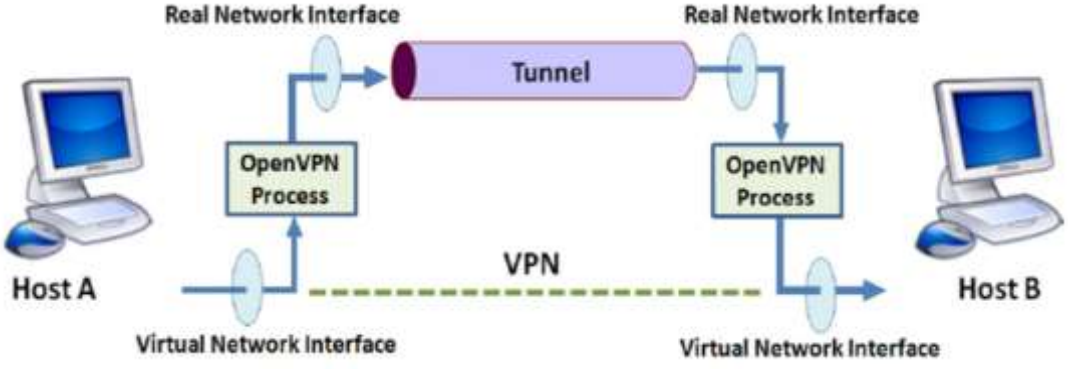

Рис.2.5. Тунель OpenVPN між двома кінцевими точками

Додатковою перевагою є широкий спектр криптографічних алгоритмів, які підтримуються бібліотеками OpenSSL, таких як AES, Blowfish, 3DES, CAST-128, Camelia та інші. Більшість VPN-провайдерів використовують переважно AES та Blowfish.

Щодо швидкості, вона залежить від рівня шифрування, але зазвичай вища, ніж у IPSec. Хоча OpenVPN широко використовується, він не є протоколом за замовчуванням на платформах, проте існують сторонні програми для різних операційних систем, включаючи ПК, Android та iOS.

Недолік гнучкості полягає в тому, що у деяких випадках налаштування може бути складним завданням, особливо в традиційних програмних реалізаціях, де користувачам слід завантажувати та інсталювати клієнт, а також завантажувати конфігураційні файли. Багато провайдерів VPN вирішують цю проблему, надаючи передналаштовані VPN-клієнти. Протокол OpenVPN вважається найбезпечнішим у сучасний момент [35].

– SSTP**.** Протокол безпечного тунелювання сокетів (Secure Socket Tunneling Protocol) був представлений Microsoft у Windows Vista SP1, і, хоча він тепер доступний на Linux, RouterOS та SEIL, він, як і раніше, використовується значною мірою лише Windows-системами.

SSTP використовує SSL v.3 і (рис.2.6.), отже, пропонує аналогічні переваги, що і OpenVPN (наприклад, можливість використовувати TCP-порт 443 для обходу NAT), а оскільки він інтегрований у Windows, він простіше у використанні і більш стабільний, ніж OpenVPN.

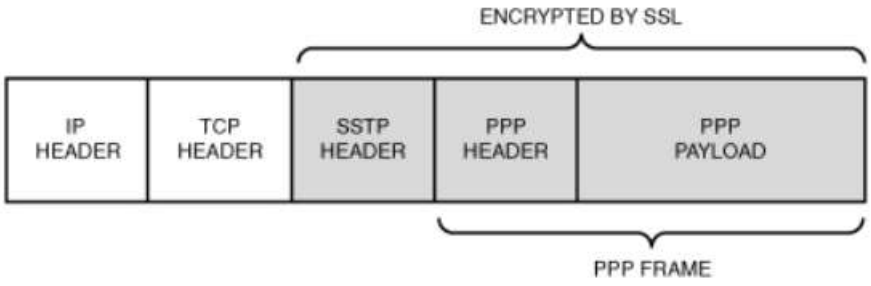

Рис. 2.6. Умовна схема пакету з даними

Підключення відбувається наступним чином (рис. 2.7.):

1)TCP-з'єднання встановлюється від клієнта до сервера;

2)SSL перевіряє сертифікат сервера. Якщо сертифікат дійсний, з’єднання встановлюється, інакше з’єднання відключається;

3)Клієнт надсилає контрольні пакети SSTP у сеансі HTTPS, який встановлює кінцевий автомат SSTP з обох сторін;

4)Передача PPP через SSTP. Клієнт автентифікується на сервері та прив’язує IP-адреси до інтерфейсу SSTP;

5)SSTP-тунель тепер встановлено, і можна починати інкапсуляцію пакетів.

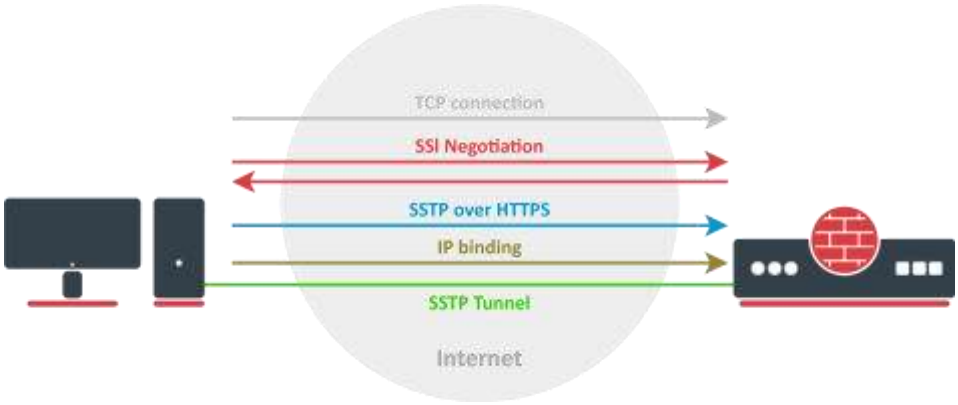

Рис. 2.7. З’єднання по протоколу SSTP

Головний недолік SSTP не має відкритого вихідного коду, тому OpenVPN використовується частіше.

–IKEv2 (протокол обміну ключами, версія 2) розроблений Cisco та Microsoft. Протокол допускає модифікації з відкритим кодом, зокрема для Linux та інших платформ. IKEv2 (Internet Key Exchange version 2) базується на обміні ключами для встановлення безпечного тунелю забезпеченого VPN-з'єднання.

Нижче подано основні етапи його роботи (рис.2.8.):

1)Ініціалізація тунелю: Коли дві сторони вирішують встановити VPN-з'єднання, вони розпочинають процес ініціалізації. Кожна сторона ідентифікується своїм унікальним ідентифікатором.

2)Обмін ідентифікаторами: Сторони обмінюються ідентифікаторами, які можуть включати інформацію про їхній ідентифікатор, сертифікати, або інші дані, що використовуються для аутентифікації.

3)Аутентифікація: Кожна сторона підтверджує свою ідентичність за допомогою обміну аутентифікаційними методами, такими як підписи або перевірка сертифікатів.

4)Створення захищеного каналу: Після успішної аутентифікації сторони використовують обміненими ключами для встановлення безпечного каналу (тунелю) для обміну даними.

5)Обмін ключами для шифрування: Здійснюється обмін ключами, які використовуються для шифрування і розшифрування даних, що передаються через VPN-з'єднання.

6)Обмін даними: Після встановлення захищеного каналу відбувається обмін даними між сторонами через безпечний тунель.

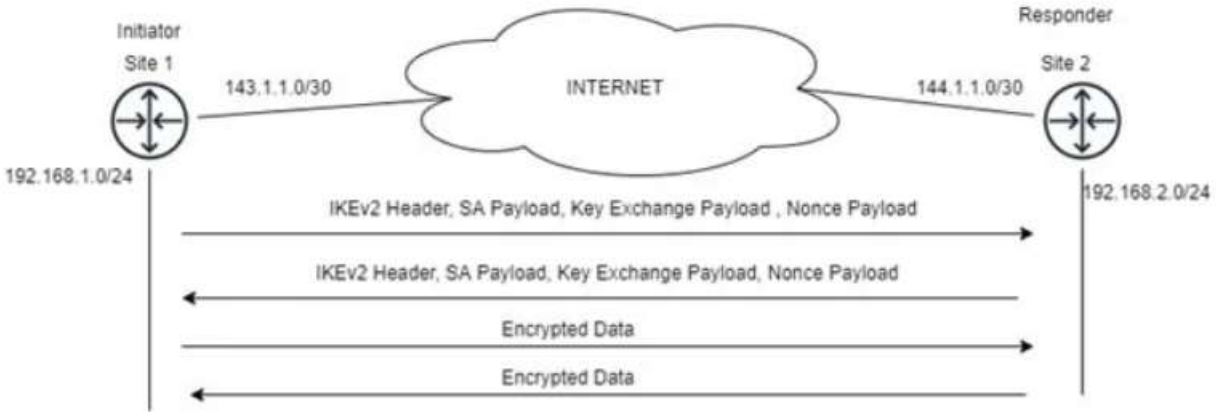

Рис.2.8. Процедура з’єднання по протоколу IKEv2

Протокол IKEv2 володіє вбудованою підтримкою для переустановки з'єднання у випадку його розриву, що робить його особливо ефективним для мобільних пристроїв, які можуть часто змінювати типи мереж і втрачати з'єднання.. Недолік – закритий вихідний код.

– SoftEther VPN — мультипротокольний VPN-сервер під ліцензією GPLv2, розробляється з 2013 року, має широкий спектр можливостей (рис.2.9). Має власний

протокол SSL-VPN, який не відрізняється від звичайного HTTPS-трафіку. Заявлена підтримка L2TP/IPsec, MS-SSTP, OpenVPN, L2TPv3 та EtherIP, причому для L2TP вказана сувора сумісність із вбудованими клієнтами в iOS та Android.

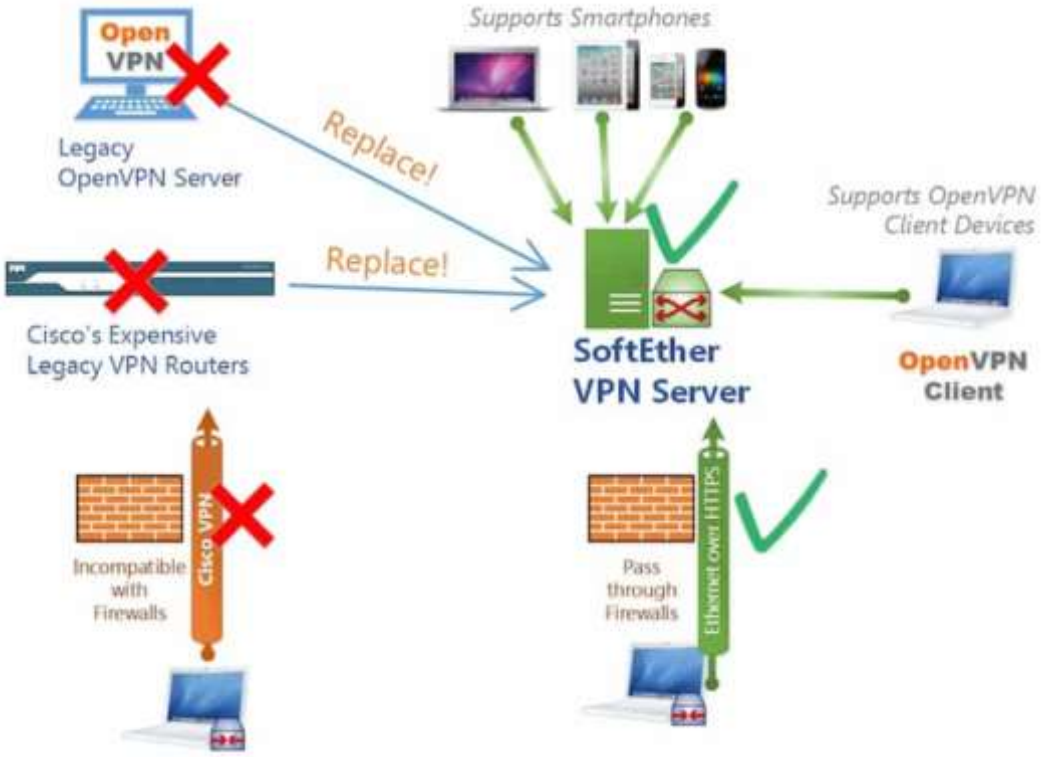

Рис.2.9. Характеристики SoftEther VPN

Сам сервер має версії під Windows, Linux, OS X, FreeBSD та Solaris. Працює швидше, ніж OpenVPN, не потребує наявності TUN/TAP, має вбудований NAT та DHCP. Протокол SSL-VPN може працювати через TCP, причому підтримуються численні сесії TCP, UDP і навіть ICMP [36].

2.3. Використання VPS

Віртуальний приватний сервер (VPS), може використовуватися для налаштування власного VPN, SSH або проксі-сервера, а іноді навіть вузла Tor, якщо це дозволяє VPS-хостинг. Вартість оренди VPS може бути нижчою, ніж придбання VPN, забезпечуючи при цьому адміністративний доступ для повного контролю та налаштування.

Адміністративний доступ дозволяє повністю відключити ведення логів і налаштувати VPN-сервер під власні потреби, якщо ви маєте відповідні навички. Однак слід зазначити, що недоліком такого підходу є те, що на одному VPS може бути лише один користувач, і його взаємодія може бути легше відстежити, ніж у випадку використання великих платних чи безкоштовних VPN.

Незважаючи на це, віртуальні сервери на одному фізичному сервері можуть забезпечувати певний рівень анонімності, оскільки зовнішньому спостерігачу буде складно ідентифікувати конкретного користувача серед усіх віртуальних ізольованих екземплярів.

При виборі VPS важливо звертати увагу на ліміти трафіку, пропускну здатність та конфігурацію ресурсів, таких як обсяг оперативної пам'яті. Також важливо враховувати підтримку TUN/TAP для розгортання VPN-сервера та налаштування правил файрвола для забезпечення безпеки.

Доступ до сервера зазвичай здійснюється через SSH з використанням сертифікатів для захисту від несанкціонованого доступу. Крім того, можуть бути використані різні техніки, такі як port knocking, для додаткового захисту послуг та унеможливлення виявлення зловмисниками.

2.4. Операційні системи для анонімної роботи

Для анонімної роботи в Інтернеті і забезпечення приватності користувачів існують спеціальні операційні системи, які призначені для максимального захисту від слідування та збереження конфіденційності. Ось кілька таких операційних систем:

–Tails (The Amnesic Incognito Live System): Tails — це live-система, яка може запускатися з USB-накопичувача або DVD і не залишає слідів на системі, на якій вона використовується. Вона автоматично маршрутизує весь інтернет-трафік через Tor, надаючи анонімність та конфіденційність.

–Whonix: Whonix — це операційна система, розроблена для використання в кількошаровому оточенні. Вона складається з двох частин: одна частина працює в

середовищі, ізольованому від Інтернету, інша частина використовує Tor для всіх мережевих з'єднань.

–Qubes OS: Qubes OS — це операційна система, яка використовує кількошаровий підхід до ізоляції завдань. Вона дозволяє створювати віртуальні машини для різних завдань та ізолює їх одна від одної. Це допомагає уникнути перехоплення даних та забезпечити конфіденційність.

–Subgraph OS: Subgraph OS базується на Debian і розроблено з основною метою забезпечити безпеку та анонімність. Вона включає в себе інтегровані інструменти для шифрування, захисту від атак та інші заходи для забезпечення приватності.

Ці операційні системи призначені для використання в анонімних і безпечних умовах та надають ряд технічних заходів для захисту конфіденційності користувачів в Інтернеті.

Розглянемо докладніше два перші пункти цього списку.

2.4.1.Whonix

ОС Whonix - система для анонімної роботи, заснована на Debian і що складається з двох віртуальних машин, одна з яких є шлюзом, що відправляє весь трафік в мережу Tor, а інша - ізольованою робочою станцією, що підключається лише до шлюзу. Існує також варіант фізичного поділу шлюзу та робочої станції. Whonix реалізує механізм так званого ізолюючого проксі-сервера. Робоча станція не отримує зовнішню IP-адресу в Інтернеті, і це дозволяє нейтралізувати безліч вразливостей, наприклад, навіть якщо шкідливе програмне забезпечення отримає root-доступ до робочої станції, у нього не буде можливості дізнатися реальну IP-адресу [40].

Whonix, як стверджують розробники, успішно пройшла безліч тестів на витоку. Навіть такі програми, як Skype, BitTorrent, Flash, Java, відомі своїми особливостями виходити у відкритий Інтернет в обхід Tor, були успішно протестовані щодо відсутності витоку компрометуючих даних. ОС Whonix реалізує такі механізми анонімізації:

– весь трафік будь-яких програм йде через мережу Tor;

– для захисту від профілювання трафіку Whonix реалізує концепцію ізоляції потоків. Попередньо встановлені в Whonix програми налаштовані на використання окремого Socks-порту, а оскільки кожен Socks-порт використовує окремий ланцюжок вузлів у мережі Tor, то профільування неможливо;

– забезпечується безпечний хостинг сервісів Tor Hidden Services. Навіть якщо зловмисник зламає web-сервер, він не зможе вкрасти закритий ключ Hidden-сервісу, оскільки ключ зберігається на Whonix-шлюзі;

– Whonix захищений від DNS-витік, оскільки у своїй архітектурі використовує принцип ізольованого проксі. Усі DNS-запити перенаправляються на DnsPort Tor;

– Whonix підтримує obfuscated bridges - мости Tor;

– застосовуються технології "Protocol Leak Protection and Fingerprinting Protection", що знижують ризик ідентифікації цифрового відбитка браузера або системи шляхом використання найбільш загальних значень, наприклад, ім'я користувача - user, тимчасова зона - UTC і т.д.;

– є можливість тунелювати інші анонімні мережі: Freenet, I2P, JAP, Retroshare через Tor, або працювати з кожною такою мережею безпосередньо;

– важливо зазначити, що у Whonix протестовані, документовані та успішно працюють усі схеми комбінування VPN/SSH/Proxy з Tor [41].

2.4.2.TAILS

The Amnesic Incognito Live System здобула популярність як «система, яку використовував Едвард Сноуден» та «найанонімніша ОС». Насправді важко сказати, що Tails краще (або гірше), ніж Whonix, оскільки їх концепції суттєво різняться. Tails є Live-дистрибутивом для завантаження з Flash-накопичувача та не залишає слідів на комп'ютері, де використовувалась. Як і Whonix, Tails заснована на Debian. Усі вихідні з'єднання здійснюються через мережу Tor, а спроби неанонімних з'єднань блокуються [43]. Tor Browser працює у захищеному режимі (AppArmor). У той же час, Tails має «Небезпечний браузер» (звичайний Firefox), що дозволяє

відвідувати сайти безпосередньо, без Tor. Загалом Tails може здатися менш безпечною, ніж Whonix, оскільки має доступ до фізичної системи, MAC-адреси, реальної IP, у той час як Whonix-Workstation ізольований у віртуальній машині. З іншого боку, у разі Whonix можливі уразливості як у двох її компонентах, так і в VirtualBox та в операційній системі хоста. В принципі, запуск Tails у віртуальній машині також можливий, але потрібно використовувати пакет virt-manager в Debian.

Використання VPN у Tails не рекомендоване розробниками, тому така можливість за замовчуванням відсутня, і налаштування VPN вимагає втручання у правила iptables. Вважається, що ланцюжок VPN через Tor шкодить анонімності, про це сказано в офіційній документації Tor. Справа в тому, що важливою перевагою Tor є часта зміна маршрутів трафіку, а при підключенні до VPN-сервера через Tor фактично створюється постійний маршрут, фіксоване місце призначення. Тим не менш, реалізувати такий ланцюжок дозволяє Whonix. Для Tails можлива схема Tor через VPN, якщо використовувати роутер з прошивкою dd-wrt і підключитися до VPN з роутера.

При необхідності більш надійного приховування шифрованих даних доцільно використовувати TrueCrypt (або VeraCrypt). В даний час творці Tails рекомендують використовувати cryptsetup, що базується на LUKS. Ця програма дозволяє створювати приховані розділи, однак такий розділ прихований не до кінця. Існує можливість виявити заголовок прихованого розділу, що дозволяє встановити його наявність. Заголовок ж прихованого розділу TrueCrypt не відрізняється від випадкових даних, і, наскільки відомо, виявити його неможливо [44].

При запуску Tails синхронізує системний годинник. Якщо при цьому виявляється суттєва розбіжність часу, Tor Browser припиняє роботу та перезапускається. З погляду зовнішнього спостерігача, така поведінка може бути використана виявлення користувачів Tails, головним чином тому, що синхронізація відбувається при кожному запуску системи.

Нижче представлені деякі з відмінностей розглянутих систем (табл. 2. 1)

Таблиця 2.1

Порівняння дистрибутивів

	Whonix	Tails
Тип системи	Образи віртуальних машин або встановлення на ПК чи USB-диск	Live-дистрибутив для завантаження з DVD або USB-носія
Запуск у VirtualBox	Так	Допускається
Захист від витоків IP	Повна, крім випадку злому Whonix-Gateway	Витік можливий при помилках системного ПЗ або зараженні вірусом
Захист від атаки «холодного завантаження»	Ні	Так
Підтримка VPN	Так, документовано	Не передбачена
Приховування MAC-адреси хоста в локальній мережі	Ні	Так
Може служити шлюзом у мережу Tor для будь-якої ОС	Так	Ні
Можливість відвідувати сайти безпосередньо, без Tor	Ні, але можна через браузер основної ОС	Через окремий браузер (Firefox)

Висновки до другого розділу:

Проведений аналіз показав значну кількість програмно-апаратних засобів, спрямованих на блокування відстеження та ідентифікації користувачів в Інтернеті. Сучасні технології дозволяють досягти високого рівня безпеки, але, як завжди, людський фактор залишається важливим чинником. Tor та анонімні операційні системи, побудовані на його основі, представляють собою потужні інструменти для забезпечення анонімності в мережі.

VPN-сервіси, зокрема, є зручними використанням, але менш безпечними порівняно з Tor.

Перспективним варіантом може бути використання підключення до VPN через Tor, яке комбінує переваги обох технологій. Проте і ця конфігурація має свої переваги та недоліки.

РОЗДІЛ 3
АПРОБАЦІЯ МЕТОДІВ ПРОТИДІЇ ВІДСТЕЖЕННЮ І ВІДСЛІДКОВУВАННЯ КОРИСТУВАЧІВ

В якості вихідних даних припускаємо, що система призначена для широкого кола користувачів, вихідна система не анонімна: інтернет-провайдеру відома особистість користувача, ПК використовується для повсякденної роботи, ОС Windows. Буде задіяно надійний VPN-сервіс або попередньо налаштований VPS.

3.1. Вибір ПЗ та необхідної конфігурації системи

Передбачається, що буде реалізований ланцюжок «VPN через Tor», при якому на виході є IP-адреса VPN-сервера, що не викликає підозр, на відміну від адрес Tor. Домогтися цього в Tor Browser складно - він спрямовує трафік виключно в Tor і не приймає альтернативних налаштувань проксі-сервера. У той же час, як згадувалося вище, Tor Browser має характерні цифрові відбитки. Отже, у нашому випадку необхідно використовувати звичайний Firefox, але для цього потрібно змінити конфігурацію. Варіанти з Chromium-браузерами не розглядаються, тому що для анонімної роботи практично завжди рекомендується Firefox - цьому сприяє і репутація Mozilla, яка активно виступає за збереження приватності, і гнучкість налаштувань браузера.

У додатку Б наведено деякі параметри, які доступні через службову сторінку about:config (деякі відсутні за замовчуванням, але працюють, якщо їх створити) [47]. Крім них, існує ще безліч параметрів, однак придатних для посилення захисту. Основна мета такої настройки - запобігання витоку різних другорядних даних, з урахуванням того, що всі основні функції браузера повинні працювати як завжди. Наприклад, відключення різних опцій телеметрії – лише спосіб підвищити конфіденційність, проте відключення WebRTC – характерний ознака боротьби з витоком реального IP під час використання деяких засобів анонімізації, а подібних ознак слід уникати.

У звичайному меню налаштувань Firefox активуємо пункт «Завжди працювати в режимі приватного перегляду». Хоча режим інкогніто не забезпечує анонімність, він є найпростішим і найефективнішим засобом боротьби з Evercookie, оскільки будь-які збережені ідентифікатори будуть видалені після закриття вікна браузера незалежно від способу їх зберігання. Теоретично, можна вимкнути використання кешу та локального сховища, проте на практиці це може спричинити деякі проблеми. На вкладці «Приватність» рекомендується заборонити прийом cookies зі сторонніх сайтів. У додаткових налаштуваннях повністю відключити відправлення телеметрії.

В даний час Firefox містить деякі опції протидії "фінгерпринтінгу", запозичені з Tor Browser. Відповідний режим активується опцією privacy.resistfingerprinting. Однак цей режим ми не будемо використовувати, оскільки деякі цифрові відбитки в ньому ідентичні відбиткам Tor Browser, наприклад, Canvas fingerprint. Також він підміняє часовий пояс на UTC без можливості вибору, а в нашому випадку часовий пояс повинен відповідати геолокації IP-адреси, що використовується.

Крім зміни налаштувань Firefox, потрібно використовувати деякі браузерні доповнення для заміни відбитків та блокування відстеження.

– CanvasBlocker – заміняє відбиток Canvas fingerprint. Має опцію повного блокування запиту canvas readout та різні режими заміни, а також підтримує білий та чорний списки. Відбиток генерується випадково при кожному оновленні сторінки, що виключає можливість відстеження користувача за цим відбитком.

– NoScript – це розширення, яке дозволяє блокувати виконання JavaScript, Java, Flash та інших потенційно небезпечних компонентів HTML-сторінок. Також надає захист від XSS-атак.

– uBlock Origin – розширення для фільтрації вмісту. Дозволяє блокувати не тільки рекламу, а й різні елементи, що відстежують (списки фільтрів у категорії «Приватність» слід активувати). У деяких випадках захищає навіть від фінгерпринтінгу: наприклад, якщо сайт використовує стандартний скрипт fingerprint2.js, завантаження скрипта буде блоковано, оскільки він входить до списку

фільтрації. Має опцію запобігання витоку локального IP через WebRTC. Також стане заміною Safe Browsing завдяки спискам шкідливих доменів.

– Decentraleyes – захищає від відстеження з боку великих CDN (мереж доставки контенту) шляхом надання локальних ресурсів та блокування мережевих запитів до CDN. Може розглядатися як додаток до фільтрів. Не викликає проблем із функціональністю сайтів.

– Privacy Badger – засіб блокування відстежувальних елементів, створений Фондом електронних рубежів (EFF), здатний до самонавчання.

– HTTPS Everywhere – ще один додаток від EFF, що примусово використовує https-з'єднання для сайтів, які це підтримують.

– Smart Referer - підміняє http referer, дозволяє відправляти referer тільки в межах одного сайту (рекомендований режим) або видаляти referer взагалі (можливі проблеми). Підтримує додавання винятків.

– AudioContext Fingerprint Defender – спотворює відбитки AudioContext шляхом додавання випадкового шуму.

– ScriptSafe містить безліч функцій анти-відстеження, частково повторює функціонал NoScript, uBlock та інших доповнень, але має й деякі унікальні опції: запобігання маніпуляціям з буфером обміну, додавання випадкових малих затримок між натисканнями клавіш.

– User-agent Switcher – заміна User-agent, у тому числі через JavaScript.

3.2.Архітектура системи

Для надійного захисту від можливих витоків та для ізоляції браузера від основної системи було вирішено використати віртуальну машину. Оскільки концепція Whonix - дві ВМ, одна з яких є інтернет-шлюзом, з'єднаною внутрішньою мережею - працює дуже ефективно, вона і буде застосована в даному випадку. Whonix дозволяє підключати до свого шлюзу не лише оригінальну Whonix-Workstation, а й будь-яку іншу ВМ. Незважаючи на те, що для анонімної роботи традиційно використовується Linux, вибір зроблено на користь Windows - така

машина буде виглядати набагато більш "звичайною", оскільки переважна більшість ПК працює під Windows. Спроби маскувати Linux-версію браузера під Windows-версію потенційно ненадійні і тому небажані. Зазначимо, що сучасна Windows 10 містить велику кількість функцій, спрямованих на збирання та відсилання даних про користувача та явно непридатних для анонімної роботи. Навіть застосовуючи всі можливі рекомендації та програми для відключення «збору телеметрії», неможливо гарантувати надійне забезпечення приватності. Тому буде встановлена Windows 7, з якої також потрібно видалити кілька оновлень з функціоналом надсилання телеметрії. На сьогоднішній день дана система все ще широко використовується, і її наявність не буде підозрілою.

Шлюз Whonix-Gateway забезпечить анонімізацію трафіку засобами мережі Tor, але необхідно приховати факт використання Tor як від сайтів, так і від інтернет-провайдера (якщо в цьому є необхідність). IP-адреса не повинна бути адресою вузла Tor, тому додатково використовується VPN. Можливі два варіанти – персональний VPN-сервер, запущений на VPS, або використання будь-якого VPN-сервісу. Перший варіант дозволяє налаштувати VPN для максимальної захищеності (відсутність ведення логів, застосування надійних криптографічних алгоритмів, різні заходи для приховання факту використання VPN), проте має дуже істотний недолік - сервер лише один, і можливість багаторазово змінювати IP-адресу відсутня. Будь-який комерційний VPN-сервіс надає на вибір цілу низку серверів, часто вони розташовані в різних країнах, і користувач може перемикатися між ними в будь-який момент. З іншого боку, далеко не всі провайдери VPN налаштовують свої сервери так, щоб сайти не могли розпізнати наявність VPN.

У практичній частині цієї роботи буде продемонстровано приклад запуску VPN-сервера і наведено його конфігурацію.

При налаштуванні VPN-сервера передбачено наступне: використовується протокол TCP та порт 443 (інший варіант – нестандартний порт, нехарактерний для VPN та проксі-серверів). Всі запити DNS надсилаються через VPN. Адреси DNS взяті зі списку OpenNIC і належать до тієї країни, де розташований обраний VPS. Сервер блокує зовнішні ICMP-запити, тому метод двостороннього пінгу для

визначення тунелю не працює. Значення MTU примусово встановлюється в 1500, стиснення трафіку (характерна ознака OpenVPN) вимкнено. Задіяно опцію шифрування керуючого каналу у поєднанні з HMAC-автентифікацією (tls-crypt) OpenVPN.

Для маскування трафіку Tor буде задіяний obfs4 – додатковий компонент Tor, спеціально призначений для протидії аналізу трафіку DPI-системами. Крім того, доцільно виключити з використання вузли Tor, які перебувають у країні перебування користувача, у нашому випадку це українські вузли. Ця можливість вбудована у додаток Tor і легко налаштовується. Усі зміни конфігурації Tor потрібно виконати на Whonix-Gateway. За винятком цих дій, втручатися в налаштування на шлюзі не рекомендується.

Цифрові відбитки Firefox підмінюються за допомогою вищезгаданих браузерних доповнень, деяких можливостей Firefox, а також зміною параметрів віртуальної машини. Окремі параметри можна підмінити і за допомогою JavaScript, підключаючи скрипти користувача через доповнення Tampermonkey, але це спрацьовує не у всіх випадках. Наприклад, роздільну здатність екрана краще змінювати для самої ВМ через налаштування VirtualBox. User-agent залишаємо без змін або підмінюємо лише версію браузера. Мова браузера – англійська за замовчуванням, допускається встановити іншу локалізацію інтерфейсу, але при цьому видалити українську зі списку мов, якими запитуються веб-сторінки (це впливає на заголовок HTTP Accept-Language). Flash-плагін встановлювати небажано. Часовий пояс змінюється в системі і повинен відповідати геолокації VPN-сервера, що використовується (враховуючи також літній/зимовий час).

Додаток CanvasBlocker замінює відбиток Canvas та частково WebGL. Браузер Firefox дозволяє перевизначити значення рядків Renderer і Vendor для API WebGL, проте відбиток WebGL залишається найбільш складним. Імовірна заміна всіх параметрів для WebGL 2 може бути реалізована тільки при повноцінній емуляції відеокарти у віртуальній машині. У звичайному VirtualBox функціональність WebGL залежатиме від того, чи включено 3D-прискорення графіки у віртуальній машині та чи встановлені «доповнення гостьової ОС». І нарешті, заміна відбитка

AudioContext виконується за допомогою AudioContext Fingerprint Defender, також можна перемикати частоту дискретизації в налаштуваннях динаміків.

Підсумкова схема реалізації має вигляд (рис.3.1).

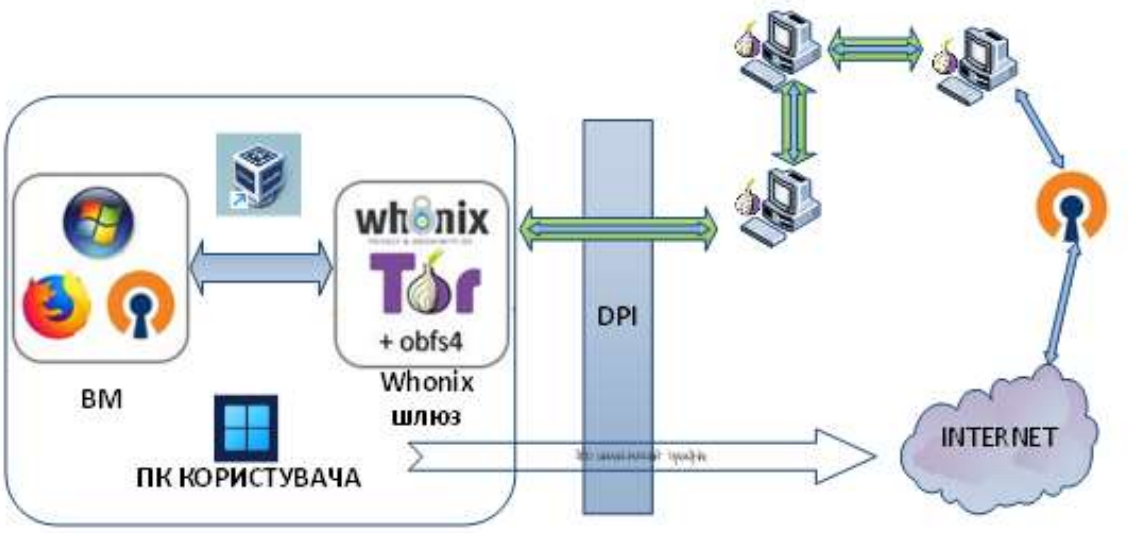

Рис. 3.1. Компоненти системи протидії відстеження і ідентифікації користувачів

Під позначенням DPI тут мається на увазі будь-яке обладнання аналізу та запису трафіку (у тому числі системи СОРМ-3), встановлене у інтернет-провайдера. Схема не виключає можливості одночасного відвідування будь-якого сайту з віртуальної машини та з основної системи, але навіть у цьому випадку з боку сайту було б дуже складно розпізнати, що відвідувач один і той самий. Зауважимо, що при даній схемі немає необхідності маскувати трафік OpenVPN, оскільки він знаходиться усередині каналу Tor з обфускацією.

У той же час, VPN забезпечить захист трафіку від можливого прослуховування на вихідних вузлах мережі Tor.

3.3.Налаштування сервера

Для тестового запуску VPN використано віртуальний сервер у VPS-провайдера HostSailor. Операційна система – Debian x64, гіпервізор – Xen, сервер

розташований у Нідерландах. Для віддаленого доступу до сервера протоколу SSH використовувався клієнт PuTTY, а також програма WinSCP для зручної роботи з файлами на сервері.

Перш ніж приступати до установки VPN, слід убезпечити сервер від можливого несанкціонованого доступу. Спершу необхідно налаштувати вхід за сертифікатом Ed25519. Ed25519 – це схема сигнатур еліптичної кривої, яка забезпечує кращий захист, ніж ECDSA та RSA, та гарну продуктивність через невелику довжину ключа. У PuTTYgen генерується пара ключів і задається пароль для закритого ключа, потім публічний ключ копіюється на сервер і додається до списку авторизованих ключів.

3.3.1.Встановлення та налаштування OpenVPN та Easy-RSA

Переконаємося, що підтримка TUN/TAP на VPS увімкнена, для цього в консолі введемо команду:

```
cat /dev/net/tun
```

Відповідь "File descriptor in bad state" є нормальною. Якщо ж отримаємо No such file or directory, то адаптер TUN/TAP не включений [38]. Залежно від провайдера, потрібно включити цю функцію через панель керування сервером на сайті, або зробити запит на техпідтримку. На Xen VPS у Hostsailor адаптер був включений спочатку.

Для встановлення пакету OpenVPN у Debian виконуємо команди:

```
apt update
apt install openvpn
```

Створимо папку для ключів і перейдемо до неї:

```
mkdir /etc/openvpn/keys
cd /etc/openvpn/keys
```

Всі операції зі створення ключів та сертифікатів можна виконати за допомогою утиліти openssl, але простіше скористатися спеціально створеною для цього програмою Easy-RSA, яка використовує openssl для виконання дій із ключами та сертифікатами. Створюємо файл налаштувань:

```
wget https://github.com/OpenVPN/easy-rsa/archive/master.zip unzip master.zip
cd /etc/openvpn/keys/easy-rsa-master/easyrsa3 cp vars.example vars
```

Тепер у WinSCP також заходимо в папку /etc/openvpn/keys/easy-rsa-master/easyrsa3 і відкриваємо файл vars. Знаходимо наступні рядки:

```
#set_var EASYRSA_REQ_COUNTRY « US»
#set_var EASYRSA_REQ_PROVINCE «California»
#set_var EASYRSA_REQ_CITY « San Francisco»
#set_var EASYRSA_REQ_ORG « Copyleft Certificate Co»
#set_var EASYRSA_REQ_EMAIL « me@example.net»
#set_var EASYRSA_REQ_OU " My Organizational Unit"
```

Це параметри, наявність яких є обов'язковою для генерації ключа. Значення в лапках можна замінити на будь-які на свій розсуд, вони в даному випадку ні на що не впливають. Потім ці рядки необхідно розкоментувати (прибрати символ # на початку рядків). Також розкоментуємо параметри, що задають довжину ключа:

```
#set_var EASYRSA_KEY_SIZE 2048
#set_var EASYRSA_DIGEST « sha256»
```

Щоб підвищити стійкість шифрування RSA, збільшимо довжину ключів до найбільшої – замінимо 2048 на 4096, а sha256 sha512. Однак замість RSA можна використовувати більш сучасну криптографію на еліптичних кривих [49], що дасть експоненційне зростання криптостійкості при меншій довжині ключа. Наприклад, популярним сьогодні ключам RSA з довжиною 1024-2048 біт відповідає лише 160-

224 бітний ключ ECC. Крім високої надійності шифрування, це підвищує продуктивність. Також у цьому випадку не потрібно генерувати файл ключа Діффі-Хеллмана. Вибір між RSA та еліптичними кривими необхідно зробити до початку роботи з EasyRSA для створення ключів. У файлі конфігурації vars нам потрібно вказати такі параметри:

```
set_var EASYRSA_ALGO ec
set_var EASYRSA_CURVE secp521r1
```

Список кривих, що підтримуються, досить великий, і серед них складно вибрати найбільш надійну. У 2013 році окремі висловлювання представників АНБ викликали побоювання, що деякі, а можливо, і всі види криптографії на основі еліптичних кривих, які використовуються органами зі стандартизації в США, були навмисно ослаблені, щоб спростити для АНБ завдання їхнього злому. Доказів, що це можливо для кривих, які використовуються для підписання та обміну ключами, немає, і деякі фахівці вважають це малоймовірним. У ході роботи спочатку було обрано менш поширену криву secp256k1, яку, зокрема, використовує система Bitcoin і яка була згенерована канадською компанією Certicom, а не Національним інститутом стандартів та технології США (як інші криві). Передбачається, що ця крива надає менше можливостей приховати «бекдор» [50]. На жаль, починаючи з версії 2.4.5, OpenVPN не працює з цією кривою (точніше, вона не підтримується оновленою бібліотекою OpenSSL 1.1), тому довелося зупинитися на secp521r1.

3.3.2.Генерування сертифікатів

Ми повинні створити так звану PKI – інфраструктуру публічних ключів. В цілому, PKI ґрунтується на використанні криптосистеми з відкритим ключем та наявності центру, що засвідчує. Ключі створюються парами – закритий та відкритий. Для обміну з будь-ким захищеною інформацією ми обмінюємося відкритими ключами. У цьому випадку сервер матиме свій закритий ключ та відкриті ключі клієнтів. У клієнтів є свої закриті ключі та відкритий ключ сервера. А засвідчувати справжність ключів буде центр, який ми також створимо самостійно, і

у всіх учасників обміну кореневий буде його кореневий сертифікат. Порядок дій для створення PKI наступний:

- ініціалізувати PKI;
- створити центр, що засвідчує – Certificate Authority;
- згенерувати сертифікати сервера;
- згенерувати сертифікати клієнта;
- створити файл параметрів Діффі-Хеллмана;
- створити список відгуків сертифікатів(опційно);
- (Посилення безпеки) Створити ключ автентифікації TLS.

Виконуємо команду ініціалізації:

```
./ easyrsa init-pki
```

Отже, створимо свій центр, що засвідчує (CA). Насправді, з міркувань безпеки, це слід робити на іншому комп'ютері, ізольованому від мережі, щоб унеможливити компрометації ключа [51]. Зараз для спрощення процедури ми створюємо CA на нашому VPN-сервері, для цього достатньо ввести команду:

```
./ easyrsa build-ca
```

Як і при генерації ключів SSH, необхідно захистити ключ надійним паролем. Також буде запрошено Common Name, можна просто натиснути Enter. Отримуємо файли: ca.crt (кореневий сертифікат, відкритий, буде передаватися клієнтам) та ca.key (закритий ключ, який не повинен бути скомпрометований).

Тепер створимо пару ключів для VPN-сервера. Закритий ключ сервера ми не захищатимемо паролем, тому що вводити цей пароль довелося б при кожному перезавантаженні сервера. Створюємо запит на сертифікат:

```
./ easyrsa gen-req server nopass
```

Буде створено два файли: server.key – закритий ключ сервера, server.req – файл-запит посвідчувального центру на підписання сертифіката. Підписуємо його:

```
./ easyrsa sign-req server server
```

Підтверджуємо операцію та вводимо пароль закритого ключа УЦ. Отримаємо підписаний відкритий ключ сервера - server.crt. Повний шлях до нього вийде: `/etc/openvpn/keys/easyrsa3/pki/issued/server.crt .`

Далі, у разі вибору алгоритму RSA, слід згенерувати файл параметрів Діффі-Хеллмана. Це забезпечить використання надійної схеми шифрування, коли навіть компрометація секретного ключа не дозволить розшифрувати записаний трафік з попередніх сесій. Процес займе деякий час:

```
./ easyrsa gen-dh
```

На виході одержуємо файл dh.pem. У цьому випадку був обраний алгоритм еліптичної криптографії, який вимагає створення цього файла. Також можна створити список відкликаних сертифікатів у разі втрати будь-якого пристрою з OpenVPN-клієнтом. Процедура відкликання зробить загублений ключ недійсним. Зараз просто створюємо сам список:

```
./ easyrsa gen-crl
```

Нарешті, скопіюємо ключі до папки OpenVPN і перейдемо до цієї папки:

```
cp pki/ca.crt /etc/openvpn/
cp pki/dh.pem /etc/openvpn/
cp pki/crl.pem /etc/openvpn/
cp pki/issued/server.crt /etc/openvpn/
cp pki/private/server.key /etc/openvpn/
cd /etc/openvpn
```

Додатково ми використовуємо механізм HMAC (hash-based message authentication code), який служить для перевірки цілісності даних, що передаються, щоб виключити можливість «атаки посередника». Для включення HMAC потрібно згенерувати спеціальний ключ і додати до конфігураційного файлу сервера директиву tls-auth, що вказує на цей ключ. Тоді сервер додаватиме підпис HMAC до всіх пакетів рукостискання SSL/TLS. Будь-який UDP-пакет, який не має правильного підпису, може бути відкинутий без подальшої обробки. HMAC-підпис, що встановлюється директивою tls-auth, забезпечує підвищений рівень безпеки на додаток до механізмів протоколу SSL/TLS. Це може захистити від:

– DoS-атак чи флуда на UDP-порт OpenVPN.

– Сканування портів для визначення прослуховуваних сервером UDP-портів.

– Вразливості, пов'язані з переповненням буфера в реалізації SSL/TLS.

– Спроб ініціації SSL/TLS-рукостискання від несанкціонованої машини (хоча, зрештою, такі рукостискання не пройдуть аутентифікацію, tls-auth може відсікнути їх на більш ранній стадії).

Згенеруємо ключ:

```
openvpn --genkey --secret ta.key
```

Цей ключ також буде переданий клієнту. Однак сучасні версії OpenVPN мають досконаліший механізм захисту, який активується опцією tls-crypt. Це включає не тільки функціонал tls-auth, але і шифрування всіх пакетів керуючого каналу, що ускладнює впізнання трафіку OpenVPN. Ключ використовується той самий, тому налаштування зводиться до заміни директиви tls-auth на tls-crypt у файлах конфігурації.

Тепер за допомогою WinSCP змінимо права доступу у файлів: ca.crt, crl.pem, dh.pem, server.crt – виставляємо для всіх 0644. На файлах server.key та ta.key мають бути права 0600. На даному етапі сервер уже готовий до роботи, але потрібно створити ключі клієнтів і правильні файли конфігурації. Переходимо знову до папки EasyRSA, створюємо та підписуємо ключ:

```
cd /etc/openvpn/keys/easy-rsa-master/easyrsa 3. /easyrsa gen-req client_name nopass ./easyrsa sign-req client_name
```

Параметр nopass застосовується на розсуд користувача. Якщо захистити ключ паролем, це підвищить безпеку, але доведеться вводити пароль під час кожного підключення до VPN. У цьому випадку для підключення достатньо мати закритий ключ. Ім'я client_name – довільне, наприклад home_pc. Тепер, коли всі ключі створені, конфігуруємо та запускаємо сервер. У папці /etc/openvpn створюємо файл server.conf (або замінюємо існуючий). Вміст використаного файлу наведено у додатку В.

Додаткове налаштування та запуск сервера

Оскільки сервер служить одночасно і DNS-резолвером, потрібно встановити DNSMasq (команда apt install dnsmasq). У файл конфігурації /etc/ dnsmasq.conf додаємо рядки:

```
server=185.208.208.141
server=146.185.176.36
interface=tun0
```

В даному випадку тут вказані адреси використаних DNS від OpenNIC, а також мережний інтерфейс TUN, запити з якого оброблятиме DNSmasq. У системному файлі /etc/resolv.conf слід також вказати аналогічні адреси DNS і видалити звідти адреси Google DNS, якщо вони були за промовчанням. Для перенаправлення трафіку з мережі VPN до зовнішнього інтернету зазвичай використовуються механізми NAT та IP forwarding. У файл /etc/sysctl.conf додаємо (або розкоментуємо вже наявні) рядки:

```
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding=1
```

Для застосування налаштувань виконуємо команду sysctl -p /etc/sysctl.conf. Тепер додаємо правила файрволу iptables:

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 185.141.27.70 iptables -A INPUT -i eth0 -p icmp -j DROP
```

Тут 10.8.0.0/24 – підмережа, що використовується для VPN, а 185.141.27.70 – публічна статична адреса даного VPS. Друге правило блокує ICMP із зовнішньої мережі, як згадувалося – це міра боротьби з розпізнаванням тунелю.

Перезапуск DNSMasq, запуск та перевірка працездатності OpenVPN:

```
systemctl restart dnsmasq
systemctl start openvpn@server
systemctl status openvpn@server
```

Етап налаштування VPN-сервера завершено, але для підключення до VPN потрібно створити файл конфігурації клієнта.

3.4. Налаштування клієнтської частини

На клієнтський ПК встановлюється VirtualBox, образи двох віртуальних машин Whonix завантажуються з офіційного сайту та імпортуються у VirtualBox. У схемі, що описується, використовується тільки Whonix-Gateway, але доцільно завантажити і Whonix-Workstation для тих випадків, коли більш важлива підвищена захищеність, ніж зручність і непомітність. Створюється ще одна віртуальна машина, в якій встановлюється Windows 7.

Застосовується програма Destroy Windows Spying для видалення засобів збору телеметрії. У налаштуваннях віртуальної машини вказується внутрішня мережа Whonix. Також рекомендується виставити число ядер процесора більше одного, цей параметр доступний через браузер (властивість navigator.hardwareConcurrency), а

одне ядро надто явно вказує на наявність ВМ. У мережних налаштуваннях самої системи слід встановити параметри для підключення до Whonix-Gateway:

IP-адреса – 10.152.152.50

Маска підмережі – 255.255.192.0

Шлюз - 10.152.152.10

DNS – 10.152.152.10

На Whonix-Gateway редагується файл налаштувань Tor для включення obfs4 та заборони використання українських вузлів. Вміст файлу:

```
DisableNetwork 0
UseBridges 1
ClientTransportPlugin obfs2, obfs3, obfs4 exec
/usr/bin/obfs4proxy bridge obfs4 <адреса моста>
# 2-3 адреси, кожен в окремому рядку
ExcludeNodes { ukr }, {??}
# ?? – вузли з невідомою геолокацією
```

У ході тестування було використано такі адреси мостів:

```
bridge obfs4 194.135.88.138:443
9F0BC3AA3CC72F17DC7789D7ABC7A763038F82CB
cert=lINVQVt8EQS5q9DWz3S+RHLosgiRVXueHlMfY3q iat-mode=0 bridge obfs4
185.79.93.126:59815 1594A9B832D4E0BD946A5988B364F1687814EC5D
cert=3DlWyDr4IwpZlxQbDX+7obB/EZ E3ftp4ILYK/G+OQ iat-mode=0 bridge
obfs4 144.76.182.167: 43981 77644CB35D66304974B84855A580155053365935
cert=yI120MhitxPLUcJFhDgspTy+sHOm4VlSAXLegRjYsu9qEd2yR59YNq3tv
```

У систему встановлюється OpenVPN-клієнт та браузер Firefox. Файл конфігурації для клієнта наведено у програмі В (деякі параметри OpenVPN для сервера та клієнта запозичені у сервісу RootVPN). При відключеному VPN весь трафік йде через Tor, що дозволяє відвідувати onion-сайти Firefox (спочатку необхідно в about:config відключити параметр network.dns.blockDotOnion). Важливо: не слід встановлювати Tor Browser в даній машині, оскільки це призведе

до ланцюжка Tor через Tor - вбудований Tor-клієнт браузера буде працювати через Tor-шлюз. Це не тільки знижує швидкодію, але й потенційно небезпечно через можливу появу маршрута, що самоперетинається, і скорочення ефективної довжини ланцюжка до одного-двох вузлів. Якщо потрібно використовувати Tor Browser, можна запустити його в системі або всередині Whonix-Workstation.

У Firefox встановлюється набір додатків, згаданих раніше та застосовуються необхідні налаштування. Повний перелік можливих параметрів конфігурації досить великий і немає єдиного правильного варіанта. "Білий список шрифтів" застосовується таким чином: на одному з сайтів (наприклад, BrowserLeaks) виявляємо список шрифтів, що розпізнаються в поточній конфігурації. Створюємо рядковий параметр font.system.whitelist на сторінці about:config у Firefox. Вміст параметра заповнюємо отриманим списком шрифтів. Тепер «відбиток шрифтів» змінюватиметься, коли видаляються деякі шрифти зі списку. Зазначимо, що різні сайти перевіряють наявність різного набору шрифтів, тому видалення (або додавання до системи) деякого шрифту не гарантує зміну отриманого списку на конкретному сайті.

Параметр WebGL Renderer під VirtualBox містить слова Software Adapter, це видає наявність віртуалізації, тому потрібно підмінити рядок значенням, взятим із будь-якого реального ПК. Підміну User-agent зручно виконувати за допомогою User-agent Switcher, проте невідповідність ОС або движка браузера може бути виявлена за непрямими ознаками, тому бажано замінювати лише версію браузера.

На додаток CanvasBlocker рекомендується вибрати режим fake at input, оскільки він більш складний для виявлення. Системний годинник слід періодично синхронізувати. Крім того, у Firefox 60 точність таймера знижена до 2 мс за замовчуванням і до 100 мс у режимі ResistFingerprinting.

Очищення даних (cookies, Local Storage та ін.) відбувається при перезапуску Firefox, а також при використанні функції «Забути» або видалення даних для конкретного сайту (у Firefox 63 розробники планують спростити цю процедуру). Крім того, додаток Firefox Multi-Account Containers дозволяє відкрити один і той же

сайт у декількох ізольованих вкладках, кожна з яких не має доступу до інших вкладок.

3.5. Тестування запропонованої системи блокування відстеження і ідентифікації

Спершу необхідно переконатися, що заміна всіх цифрових відбитків надійно працює, а сайти, що відвідуються, не розпізнають наявність засобів анонімізації. У віртуальній машині з Windows було виконано підключення до налаштованого VPN через Whonix-Gateway, використано Firefox. Під час роботи не було помічено проблем із підключенням OpenVPN за протоколом TCP через ланцюжок Tor та obfs4. Часовий пояс у системі було змінено до запуску браузера.

Для перевірки VPN використовувалися Інтернет-ресурси наведені в додатку :

Спершу отримаємо дані про основну систему без анонімізації (рис.3.2).

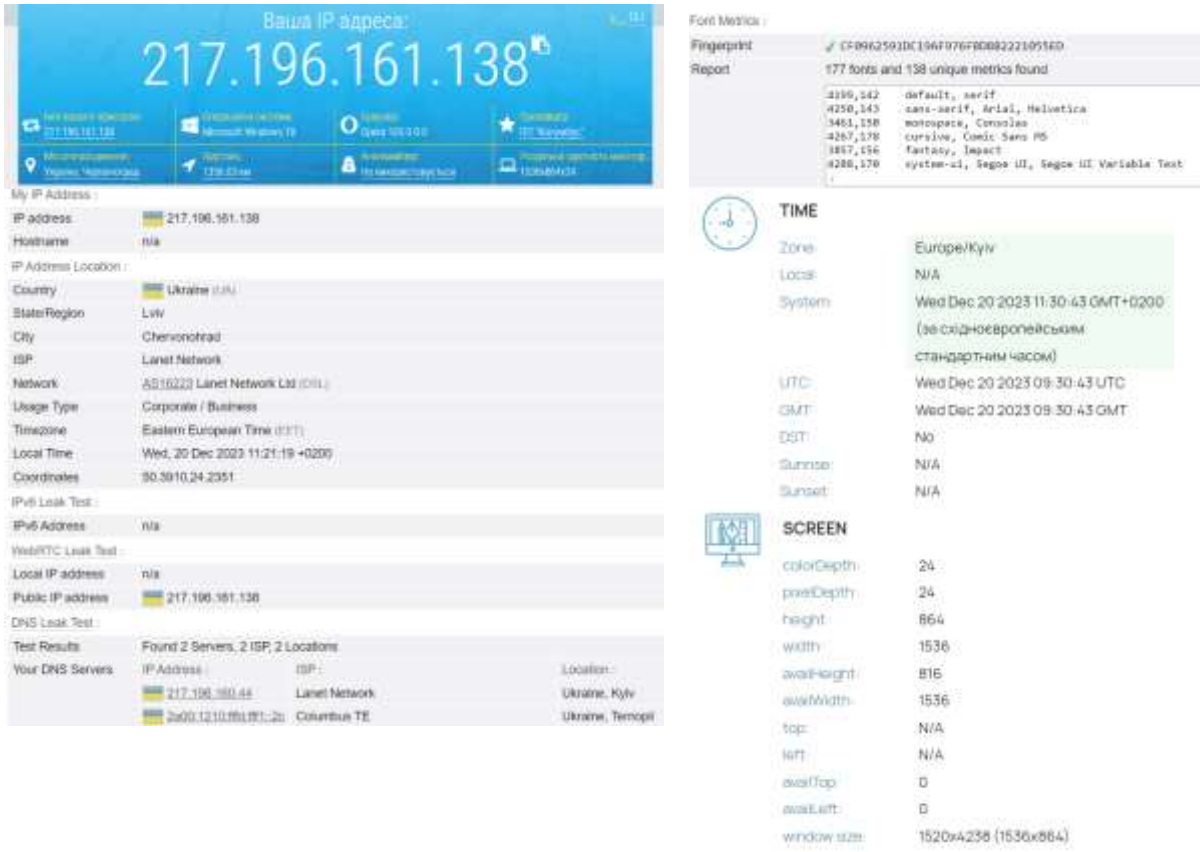

Рис.3.2. Інформація з браузера, встановленого на ПК

Цифрові відбитки Canvas, WebGL, AudioContext з основної системи не мають значення, оскільки у віртуальній машині вони будуть іншими навіть без застосування додаткових засобів для їх заміни. Завдання – переконатися у наявності можливості міняти їх багаторазово.

Перевірки на виявлення засобів анонімізації показали практично ідеальні результати (рис.3.3.), проте слід розуміти, що деякі сайти можуть використовувати повніші бази IP-адрес хостингів і VPN-провайдерів.

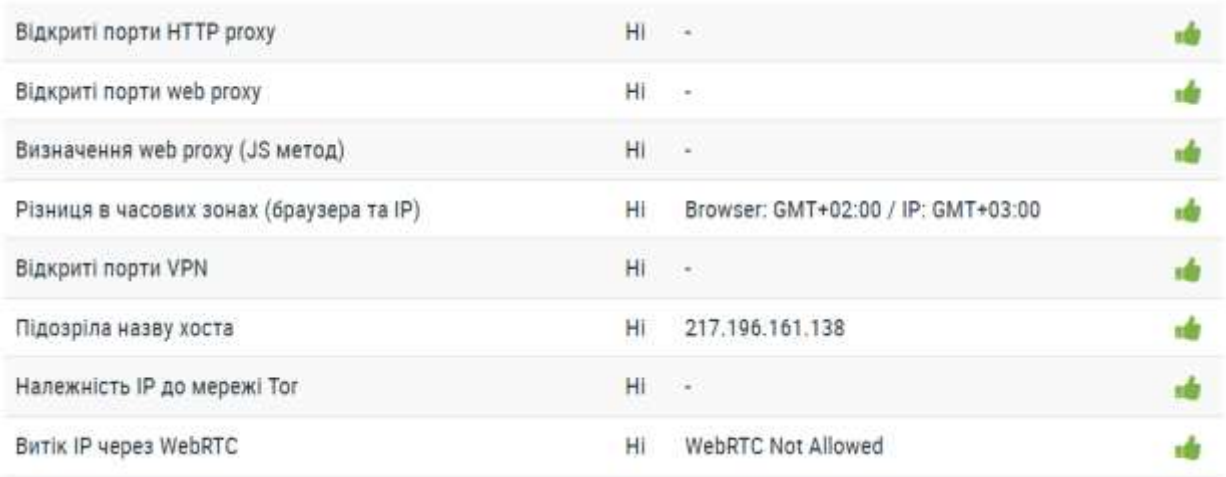

Рис. 3.3. Перевірка на сайті 2ip.ua

Важливо відзначити, що цей ресурс не зміг визначити DNS-адреси та факт приналежності IP до хостинг-провайдера HostSailor. Це є недоліком сайту, а не перевагою VPN-сервера.

Для наочного порівняння наведемо результат цієї перевірки для VPN-провайдера ProtonVPN (рис.3.4)(в режимі безкоштовного доступу):

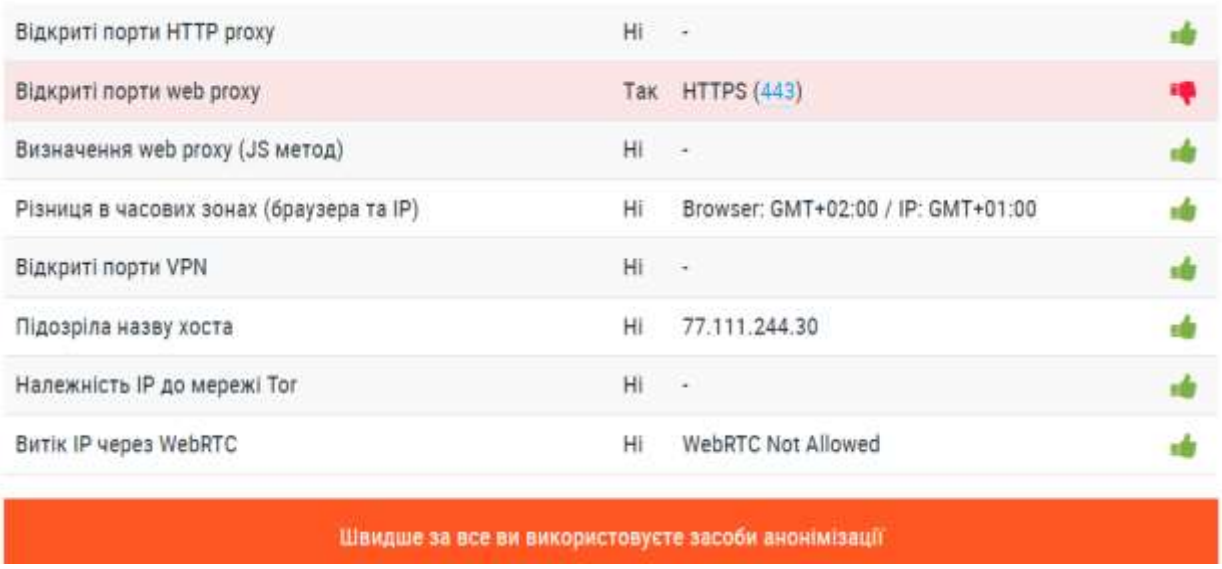

Рис. 3.4. Приклад незадовільного результату

Очевидно, що тут не було виставлено відповідного часового поясу, проте решта трьох параметрів залежить саме від налаштувань сервера.

Тестування на сайті Whoer показало, що витік реального IP через WebRTC не відбувається, але є витік внутрішньомережевої адреси (10.8.0.2), яка побічно свідчить про наявність VPN. Після включення в uBlock відповідної опції (Prevent WebRTC from leaking local IP addresses) цей витік блокується (рис. 3.5). Альтернативний спосіб: встановити параметр media.peerconnection.ice.proxy_only=true у конфігурації Firefox. Результат аналогічний до дії uBlock. Після цього даний сайт не виявляє жодних ознак використання анонімайзера:

Рис. 3.5. Тест на сайті Whoer.net

Перевірка MTU показує нейтральне значення 1500 і, відповідно, не виявляє присутності VPN:

```
First seen    = 2023/12/20 12:31:10
Last update   = 2023/12/20 12:31:10
Total flows   = 2
Detected OS   = Windows NT kernel [generic]
HTTP software = Chrome 60.x or newer (ID seems legit)
MTU           = 1500
Network link  = Ethernet or modem
Language      = Ukrainian
Distance      = 8

PTR test      = Probably home user
Fingerprint and OS match. No proxy detected (this test does not include headers detection).
No OpenVPN detected.
```

Рис. 3.6. Перевірка MTU

Витоків сторонніх адрес DNS виявлено не було, визначаються тільки ті адреси, які використовуються сервером і відносяться до Нідерландів.

Your IP	Provider	Country
*...	*...	*...
173.194.170.10	Google	The Netherlands
172.253.7.197	Google	The Netherlands
173.194.170.12	Google	The Netherlands
74.125.181.204	Google	The Netherlands
74.125.114.208	Google Servers	The Netherlands
172.253.11.206	Google	The Netherlands
172.217.41.11	Google	The Netherlands
173.194.169.99	Google	The Netherlands
172.253.11.196	Google	The Netherlands
173.194.170.9	Google	The Netherlands
74.125.114.193	Google Servers	The Netherlands
172.217.40.71	Google	The Netherlands

Рис. 3.7. Перевірка адрес DNS

Один із варіантів цифрового відбитка браузера наведено нижче.

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	0.39	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	20.65	1645312.0	c2c4645b2004347687b0ee050fafbbcc
Screen Size and Color Depth	17.48	182812.44	1280x680x24
Browser Plugin Details	1.23	2.35	undefined
Time Zone	2.56	5.91	-120
DNT Header Enabled?	0.78	1.72	True
HTTP_ACCEPT Headers	2.01	4.02	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	19.65	822656.0	593985985e588db7b927e4e70057819f
Language	0.92	1.89	en-US
System Fonts	19.65	822656.0	Arial, Arial Black, Calibri, Cambria, Cambria Math, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Console, Lucida Sans Unicode, Microsoft Sans Serif, MS Gothic, MS PGothic, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.04	8.24	Win64
User Agent	8.13	279.39	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Touch Support	0.59	1.51	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.22	1.16	Yes

Рис. 3.8.Цифровий відбиток браузера з Panopticlick.eff.org

Відбиток Canvas на сайті BrowserLeaks має такий формат:

Signature	✓ E2BAD04C
Uniqueness	100% (0 of 258561 user agents have the same signature)
Image File Details :	BrowserLeaks.com <canvas> 1.0
File Size	3849 bytes
Number of Colors	259
PNG Hash	C93AB3EAB4750C3D6523AE4EF07DA53E

Рис. 3.9. Випадковий Canvas Fingerprint з CanvasBlocker

Порівняємо це з оригінальним відбитком та з заміною через вбудовану функцію Firefox ResistFingerprinting:

Рис. 3.10. Відбитки HTML5 Canvas

1 – Відбиток без використання заміни

2 – Випадковий відбиток при увімкненому CanvasBlocker

3 – Статична підміна з опцією ResistFingerprinting

Даний сайт не виявляє присутності CanvasBlocker в режимі fake at input, як і інших підозрілих ознак, крім uBlock:

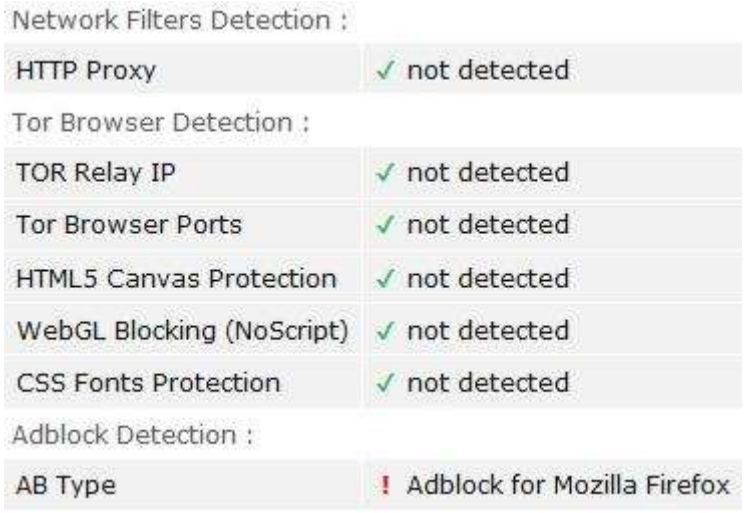

Рис. 3.11. Перевірка на сайті BrowserLeaks

Аналогічно розглянемо відбитки WebGL. Помічено, що у віртуальній машині доступна лише обмежена функціональність WebGL 1.0, незважаючи на увімкнене 3D-прискорення графіки в налаштуваннях цієї ВМ.

Debug Renderer Info :	
Unmasked Vendor	! Google Inc.
Unmasked Renderer	! ANGLE (Software Adapter Direct3D11 vs_5_0 ps_5_0)
WebGL Fingerprint :	
WebGL Report Hash	C6FCC26C0E17D793BC09415795D74264
WebGL Image Hash	42F3ECF80B0132497576DC52941323D9

Рис. 3.11. Вихідний відбиток WebGL у VirtualBox

Debug Renderer Info :	
Unmasked Vendor	! Google Inc.
Unmasked Renderer	! ANGLE (Intel(R) HD Graphics 620 Direct3D11 vs_5_0 ps_5_0)
WebGL Fingerprint :	
WebGL Report Hash	D77B1800B2862B40C1B1DF5E71F4E53F
WebGL Image Hash	550CE9AC46F5293812F64F779CDE4ED2

Рис. 3.12. Відбиток після заміни

Тепер встановимо параметр webgl.enable-debug-renderer-info= false :

Debug Renderer Info :	
Unmasked Vendor	n/a
Unmasked Renderer	n/a
WebGL Fingerprint :	
WebGL Report Hash	FD2F31E5AC14E11D570EB122A99F666E
WebGL Image Hash	F429E49DA8C387231B91D42248DA37BE

Рис. 3.13. Заміна відбитка та приховування даних

CanvasBlocker впливає лише значення Image Hash, змінюючи його випадковим чином. Report Hash залежить від вмісту рядків Vendor та Renderer, які перевизначаються через параметри Firefox (webgl.renderer-string-override).

Відбитки шрифтів (рис.3.14-3.15) отримані до і після заміни:

Рис.3.14. Відбиток шрифтів до заміни

Рис. 3.15. Відбиток шрифтів після заміни

Приклади Audio Fingerprint.

Рис. 3.16. Початкові відбитки AudioContext

Рис. 3.17. Випадкові відбитки AudioContext

У Під час тестування було підтверджено можливість зміни цифрових відбитків необмежену кількість разів (Canvas, WebGl Image, Audio Fingerprint) або, як мінімум, неодноразової заміни (шрифти, User-agent, роздільна здатність екрану, WebGL Render, ClientRects та ін).

Висновок: запропонована конфігурація ПЗ забезпечує ефективну протидію різним сучасним методам відстеження, надійну ізоляцію анонімного браузера від неанонімної системи, захист від розкриття реальних даних про систему, не порушуючи при цьому функціональність браузера. Успішно перевірено також правильність налаштування OpenVPN щодо його маскування.

У той же час необхідно враховувати, що підключення VPN через Tor є менш надійним з точки зору анонімності, ніж використання тільки Tor, так само як і Windows зазвичай не рекомендується для анонімної роботи, на відміну від спеціальних Linux-дистрибутивів.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Для забезпечення безпеки та охорони праці користувачів комп'ютерів при проведенні наукових досліджень слід враховувати особливості робочих місць, де використовуються електронні обчислювальні засоби. Виконання кваліфікаційної роботи магістра пов'язане із роботою за ЕОМ, тому забезпечення відповідності вимогам охорони праці робочих місць є важливим питанням Основними вимогами щодо охорони праці в цьому контексті є:

–організація робочих приміщень;

–забезпечення захисту від шкідливих чинників;

–ергономіка робочих місць;

–навчання користувачів.

Розглянемо деякі з цих вимог більш детально. Розміщення робочих місць, оснащених ЕОМ виконується в приміщеннях з однобічним розміщенням вікон, що обов'язково мають бути оснащені сонцезахисним засобами: шторами та жалюзями. При розміщенні робочих місць у приміщеннях з джерелами шкідливих та небезпечних виробничих чинників, вони зобов’язані розміщатись в повністю ізольованих кабінетах з природним освітленням та організованою вентиляцією. Площа, на якій розташовується одне робоче місце для обслуговуючого персоналу, має складати не менше 6,0 м^2, об'єм – не менше ніж 20 м^3, а висота – не менше 3,2 м.

Робочі місця з відеодисплейним терміналом зобов’язані розміщатися на віддалі не менше як 1,5 м від стіни з віконними прорізами, від інших стін – на відстані 1 м, одне від одного на відстані не менше ніж 1,5 м. У випадку розміщення робочих місць необхідно виключити можливість прямого засвічування екрану джерелом природного освітлення. Робоче місце раціонально розташовувати так, щоб природне світло падало на нього збоку, переважно з лівого.

Розташовувати відеодисплейний термінал на робочому місці необхідно так, щоб поверхня екрана повинна знаходитись на віддалі 400-700 мм від органів зору користувача. Висота робочої поверхні столу при виконанні роботи сидячи повинна налаштовуватись в межах 680-800 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною не менше як 500 мм, глибиною на рівні колін не менше 450 мм та на рівні витягнутої ноги не менше як 650 мм.

Поверхня підлоги повинна бути гладкою, без вибоїн, не слизькою, мати антистатичні властивості, зручною для вологого прибирання. Не дозволяється використовувати для оздоблення інтер'єру полімерні матеріали, що виділяють у повітря шкідливі хімічні речовини.

В середині приміщення, де здійснюється робота з дослідження методів підвищення пропускної здатності мобільних мереж, особливу увагу потрібно приділити запобіганню загрози ураження електричним струмом. Дане приміщення відноситься до приміщень з підвищеною небезпекою ураження електричним струмом в наслідок наявності високої (більше 75 %) вологості. Тому безпека експлуатації електрообладнання має забезпечуватись рядом заходів, що включають використання ізоляції струмоведучих частин, захисних блокувань, захисного заземлення тощо.

Величина напруженості електромагнітного поля на робочих місцях з персональними ЕОМ мають не перевищувати гранично допустимі, які складають 20 кВ/м. Експозиційна доза рентгенівського випромінювання на відстані 0,05 м від екрана до корпуса монітора при будь-яких положеннях регулювальних пристроїв не повинні перевищувати 7,74·10-12 Кл/кг, що відповідає потужності еквівалентної дози 0,1 мБер/год (100 мкР/год). З метою забезпечення захисту і досягнення нормативних рівнів випромінювань необхідно використовувати екранування робочого місця і скорочення часу опромінення за рахунок перерв на відпочинок.

Зважаючи на те, що під час експлуатації пристроїв крім усього іншого обладнання використовується устаткування, робота якого генерує завади, потрібно передбачити захист від завад. Визначено, що приміщення, де проводиться робота з дослідження може мати робочі місця із шумом, що спричиняється вентиляторами

блоку живлення ЕОМ і кулерами мікропроцесора та відеокарти. З метою попередження травмування від дії шуму він підлягає нормуванню. Основним документом стосовно виробничого шуму, що діє в нашій країні, Допустимі рівні звукового тиску, рівні звуку і еквівалентні рівні шуму на робочих місцях у виробничих приміщеннях не мають бути більшими ніж значення, що приведені в таблиці 4.1.

Таблиця 4.1

Нормовані рівні звукового тиску і еквівалентні рівні звуку

Рівні звукового тиску в дБ в октавних полосах із середньо-геометричними частотами, Гц									Рівні звуку і еквівалентні рівні звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

Для встановлення нормованих показників шуму в приміщенні передбачено такі заходи:

1) оздоблення стін спеціальними перфорованими плитами, панелями з метою шумопоглинання;

2) контроль рівня шуму не менше 1 разу на рік.

Отже в даному підрозділі розглянуто вплив середовища на працездатність та здоров’я користувачів комп’ютерів. Як висновок можна сказати, що робоче місце яке використовувалось для написання даного наукового дослідження відповідає вимогам з охорони праці.

Однак необхідно не забувати що надмірна робота з ПК може привезти до порушення роботи організму користувача. Тому необхідно дотримуватись вимог щодо планування робочого часу за ЕОМ.

Як висновок можна сказати, що мета охорони праці при виконанні наукової роботи полягає в створенні комфортного та безпечного робочого середовища для користувачів комп'ютерів, а також забезпечення високого рівня безпеки відповідно до вимог та ефективності при виконанні наукових завдань.

4.2.Безпека в надзвичайних ситуаціях

4.2.1.Фактори, що впливають на функціональний стан користувачів комп’ютерів

Комп’ютерна техніка широко використовується в усіх галузях людської діяльності. Людина, яка працює з комп’ютером, постійно перебуває під впливом небезпечних і шкідливих виробничих факторів: електромагнітних полів, інфрачервоного та іонізуючого випромінювань, шуму й вібрації, статистичної електрики. Крім цього, оператор піддається значному розумовому і психоемоційному навантаженню, високій напрузі зорової та м’язової діяльності.

Незадовільний функціональний стан користувачів комп'ютерів може викликати небажані наслідки (професійні та професійно зумовлені захворювання), що також пов'язано зі значними соціальними та економічними втратами враховуючи стрімке зростання кількості комп'ютеризованих робочих місць.

На рисунку 4.1 зображено фактори, що впливають на функціональний стан користувача комп’ютером, зокрема, виробниче середовище, трудовий процес, внутрішні та зовнішні засоби діяльності, а також соціально- психологічні фактори.

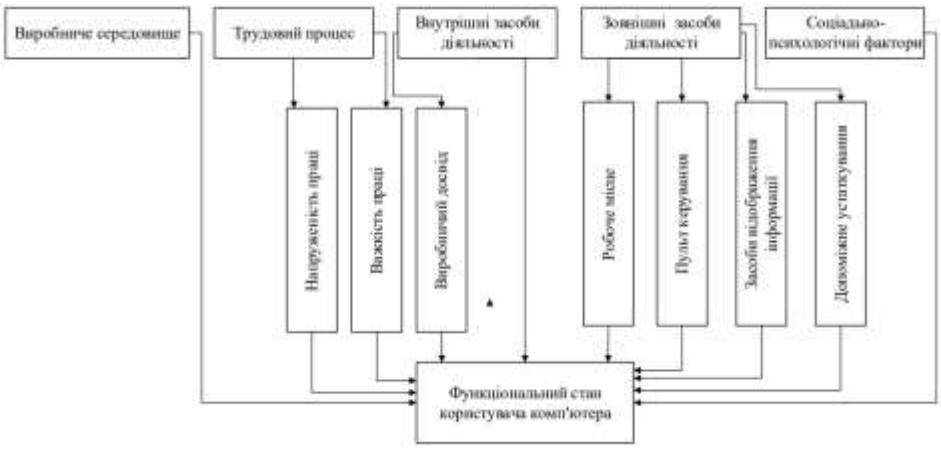

Рис. 4.1 Фактори, що впливають на функціональний стан користувача комп’ютера

Тому для зменшення ризику захворювань необхідно проводити комплекс медико-гігієнічних, адміністративно-технічних й ергономічних заходів. До цих передовсім повинні входити:

–контроль за конструкцією, добрим станом і функціонуванням комп’ютера;

–відповідність місця праці рекомендаціям ергономіки та гігієни;

–створення оптимальних умов для праці у виробничому приміщенні;

–раціональний режим праці;

–диспансерне медико-гігієнічне обслуговування з цілеспрямованим проведенням оздоровчих (наприклад корекція зору) і профілактичних заходів;

–особиста участь працівника у догляді за своїм здоров’ям.

Трудова діяльність користувачів комп’ютерів відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі – фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників.

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп’ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп’ютерів відзначається значними інформаційними навантаженнями.

Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях.

Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів.

4.2.2.Негативний вплив радіоактивного забруднення місцевості після ядерного вибуху на виробничу діяльність промислового підприємства та організації

Радіоактивне забруднення є четвертим фактором, на який припадає близько 10 % енергії ядерного вибуху. Під час ядерного вибуху утворюється велика кількість радіоактивних речовин, які, осідаючи з димової хмари на поверхню землі, забруднюють повітря, місцевість, воду, а також всі предмети, що знаходяться на ній, споруди, лісові насадження, сільськогосподарські культури, урожай, незахищених людей і тварин.

Джерелами радіоактивного забруднення є радіоактивні продукти ядерного заряду, частина ядерного палива, яка не вступила в ланцюгову реакцію, і штучні радіоактивні ізотопи. [12]

Радіоактивні речовини, які випадають зі хмари ядерного вибуху на землю, утворюють радіоактивний слід. З рухом радіоактивної хмари і випаданням з неї радіоактивних речовин розмір забрудненої території поступово збільшується. Слід у плані має, як правило, форму еліпса, велику вісь якого називають віссю еліпса. Розміри сліду радіоактивної хмари залежать від характеру вибуху і швидкості вітру, який є середнім за швидкістю і напрямком для всіх шарів атмосфери від поверхні землі до верхньої межі радіоактивної хмари. Слід може мати сотні й навіть тисячі кілометрів у довжину і кілька десятків кілометрів у ширину. Радіоактивне забруднення місцевості в межах сліду нерівномірне. Найбільше радіоактивних речовин випадає на осі сліду, від якої ступінь забруднення зменшується у напрямку до бокових меж, а також від центру вибуху до кінця хмари.

Основним джерелом забруднення місцевості є радіоактивні продукти поділу. Це суміш багатьох ізотопів різних хімічних елементів, які утворюються в процесі поділу ядерного заряду і радіоактивного розпаду цих ізотопів. При поділі ядер урану-235 і плутонію-239 утворюється майже 200 ізотопів 70 хімічних елементів. Більшість радіоізотопів належить до короткоживучих – йод-131, ксенон-133, лантан-140, церій-141 та ін. з періодом напіврозпаду від кількох секунд до кількох днів. Стронцій-90, цезій-137, рубідій-10, криптон-8, сурма-125 та інші мають напіврозпаду від одного до кількох років. Радіоізотопи цезій-135, рубідій-B7,

самарій-147, неодим-144 характеризуються надзвичайно повільним розпадом, який триває тисячі років.

Непрореагована частина ядерного палива, яка випадає на землю, – це ядра атомів урану і плутонію, що розділилися і є альфа-випромінювачами.

Великий вплив на ступінь і характер забруднення місцевості мають метеорологічні умови. Вітер у верхніх шарах атмосфери сприяє розсіванню радіоактивного пилу на великі території і цим самим знижує ступінь забруднення місцевості. Сильний вітер у приземному шарі атмосфери частину радіоактивного пилу, який випав на поверхню землі, може підняти в повітря і перенести на іншу територію, що призведе до зменшення ступеня забруднення в даному районі, але збільшення території, забрудненої радіоактивними речовинами. [13]

Під час дощу, снігу, туману ступінь забруднення в районі випадання опадів вищий, ніж у суху погоду. За таких умов протягом одного і того ж часу з дощем або снігом на поверхню землі осідає значно більше радіоактивних речовин. Але сніг ослаблює іонізуючі випромінювання (внаслідок екранізуючої дії) і рівень радіації зменшується. Випадання дощу сприяє перенесенню радіоактивних речовин у ґрунт, а на місцевості також знижується рівень радіації.

ВИСНОВКИ

Основні результати роботи полягають у наступному:

1)Було проведено масштабний пошук різної інформації про сучасні методи ідентифікації користувачів та відстеження їхньої активності в Інтернеті.

2)Проведений аналіз показав значну кількість програмно-апаратних засобів, спрямованих на блокування відстеження та ідентифікації користувачів в Інтернеті. Tor та анонімні операційні системи, побудовані на його основі, представляють собою потужні інструменти для забезпечення анонімності в мережі. VPN-сервіси, зокрема, є зручними використанням, але менш безпечними порівняно з Tor.

3)Перспективним варіантом запропоновано використання підключення до VPN через Tor, яке комбінує переваги обох технологій. В результаті було отримано конфігурацію програмного комплекту, що поєднує ряд позитивних якостей різних технологій.

4)Значною мірою було підтверджено початкову гіпотезу про те, що високий рівень захисту досягається без шкоди функціональності браузера.

5)Запропонована конфігурація ПЗ забезпечує ефективну протидію різним сучасним методам відстеження, надійну ізоляцію анонімного браузера від неанонімної системи, захист від розкриття реальних даних про систему, не порушуючи при цьому функціональність браузера.

6)Використовуваний ланцюжок «VPN через Tor», за всіх її переваг, може бути визнаний анонімним лише за умови, що клієнту вдалося зберегти анонімність при реєстрації і особливо при оплаті сервісів необхідних для роботи розробленої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nikiforakis, Nick; Joosen, Wouter; Livshits, Benjamin. Privaricator: Deceiving fingerprinters with little white lies. In: *Proceedings of the 24th International Conference on World Wide Web*. 2015. p. 820-830.

2. Cao, Yinzhi, Song Li, and Erik Wijmans. "(Cross-) browser fingerprinting via OS and hardware level features." *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, 2017.

3. Nunes, Vítor, et al. "Enhancing the Unlinkability of Circuit-Based Anonymous Communications with k-Funnels." *Proceedings of the ACM on Networking* 1.CoNEXT3 (2023): 1-26.

4. Sendner, Christoph, et al. TorMult: Introducing a Novel Tor Bandwidth Inflation Attack. *arXiv preprint arXiv:2307.08550*, 2023.

5. Von Arx, Theo; Tran, Muoi; Vanbever, Laurent. Revelio: A Network-Level Privacy Attack in the Lightning Network. In: *8th IEEE European Symposium on Security and Privacy (EuroS&P 2023)*. 2023.

6. Perino, Diego; Varvello, Matteo; Soriente, Claudio. Long-term measurement and analysis of the free proxy ecosystem. *ACM Transactions on the Web (TWEB)*, 2019, 13.4: p. 1-22.

7. Steven Englehardt and Arvind Narayanan. Online Tracking: A 1-million-site Measurement and Analysis. In Proceedings of the 2016 *ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Association for Computing Machinery, New York, NY, USA, 2016. p.1388–1401.

8. Чим небезпечне "шпигунство" Google URL: https://www.epravda.com.ua /publications/2019/07/31/650137/ (дата звернення: 8.12.2023).

9. Wollmer, Benjamin; Wingerath, Wolfram; RITTER, Norbert. Context-Aware Encoding and Delivery in the Web. In: *International Conference on Web Engineering*. Cham: Springer International Publishing, 2020. p. 525-530.

10. Vastel, Antoine, et al. Fp-stalker: Tracking browser fingerprint evolutions. In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018. p. 728-741.

11. Artur, Mickiewicz. Technologies and methods of user tracking on the Internet. *Редакційна колегія*, 2021, 77.

12. Желібо П,, Заверуха Н. М., Запарний В. В. Безпека життєдіяльності: Навч. посіб. / За ред, Є. П. Желібо. 6-е вид. - К.: Каравела, 2008. 344 с.

13. Депутат О. П., Коваленко І. В. "Цивільна оборона. Підручник/За ред. Полковника ВС Франчука.–2-ге вид., доп." Львів, Афіша, 2001.

14. Карабан Д., Жаровський Р. Аналіз проблем забезпечення анонімності користувачів при використанні мережі Інтернет. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 456.

15. Карабан Д., Жаровський Р. Методи забезпечення анонімності в Інтернеті. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С.237

16. What is Tor and how does it work? URL: https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/ (дата звернення: 5.12.2023).

17. Configure (Private) (Obfuscated) Tor Bridges URL:https://www.whonix.org/wiki/Bridges (дата звернення: 5.12.2023)

18. VPN протоколи URL: https://www.vpnunlimited.com/ua/help/vpn-protocols (дата звернення: 8.12.2023).

19. Що таке IKE та IKEv2 VPN протоколи? URL: https://www.vpnunlimited.com/ua/help/vpn-protocols/ikev2-protocol (дата звернення: 8.12.2023)

20. Чайковський, А. В., Жаровський Р. О., Лещишин Ю. З. "Конспект лекцій з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для студентів спеціальності 123–Комп'ютерна інженерія." 2021. 343с.

21. Жаровський, Руслан Олегович. "Конспект лекцій з дисципліни Захист інформації у комп'ютерних системах." 2019 268 с.

22. Лупенко С.А., Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. 2021. 34 с.

Додаток А.

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедиміната (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів
6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ
55. **В. В. Яцишин, О. О. Горбач** **440**
ПРОЦЕСИ РОЗРОБКИ ТА МОДЕЛІ ЖИТТЄВОГО ЦИКЛУ КОМП'ЮТЕРНИХ СИСТЕМ
56. **А. М. Луцків, Ю. Б. Мельничук** **441**
ПРИНЦИПИ ОРГАНІЗАЦІЇ ОНЛАЙН АУКЦІОНІВ З ІНТЕГРАЦІЄЮ ЕЛЕМЕНТІВ БЛОКЧЕЙН ТЕХНОЛОГІЇ І ТЕОРІЇ ІГОР
57. **Т. А. Озарків, Р. О. Жаровський** **442**
ОПТИМІЗАЦІЯ РОБОТИ ПРОТОКОЛУ EIGRP В УМОВАХ ВЕЛИКИХ МЕРЕЖ ЗІ СКЛАДНОЮ ТОПОЛОГІЄЮ
58. **М. Р. Лещук, Б. М. Зозуляк, В. М. Кравчук, Р. І. Королюк** **443**
МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ КОНТРОЛЮ НАТЯГУ ПРИ ПРОКАТУВАННІ АЛЮМІНІЮ
59. **Ю. І. Микитів, І. Я. Харів, М. Б. Горват, Р. З. Золотий** **445**
АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМФОРТУ ТА ЕНЕРГОЕФЕКТИВНОСТІ БУДІВЕЛЬ
60. **М. С. Дзюмак, С. З. Кульчицький, І. М. Поливаний, О.С. Голотенко** **447**
ДОСЛІДЖЕННЯ СИСТЕМИ ПЛАНУВАННЯ МАРШРУТУ НА ОСНОВІ ІНТЕРВАЛЬНИХ ОБЧИСЛЕНЬ
61. **А. О. Мацюк, В. В. Дрогомирецький, Ю. О. Зеленко, А. А. Станько** **448**
РОЗРОБКА СИСТЕМИ КЕРУВАННЯ ПРОЦЕСОМ ПАКУВАННЯ КОНСЕРВНИХ ВИРОБІВ
62. **Т. В. Чомко, В. В. Панчук, В. П. Пинило, В. В. Карташов** **450**
РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА УПРАВЛІННЯ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ КЕРУВАННЯ ПІДЙОМНИМ МЕХАНІЗМОМ
63. **А. М. Луцків, А. Я. Островський** **452**
ХАРАКТЕРИСТИКИ ТА СФЕРА ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ
64. **Н. М. Ковтун, Р. О. Жаровський** **453**
АНАЛІЗ ЗАСОБІВ ПРОТИДІЇ ВТОРГНЕННЯМ І АТАКАМ НА КОМП'ЮТЕРНІ СИСТЕМИ
65. **А. М. Луцків, В. В. Гладій** **455**
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ТА КЛАСИФІКАЦІЇ РОЗПОДІЛЕНИХ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ
66. **Д. Р. Карабан, Р. О. Жаровський** **456**
АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧІВ ПРИ ВИКОРИСТАННІ МЕРЕЖІ ІНТЕРНЕТ
67. **А. В. Ремез, Й. Р. Кравець, І. В. Карп, Д. П. Стухляк** **457**
ДОСЛІДЖЕННЯ РУЙНІВНОГО НАПРУЖЕННЯ ПРИ ЗГИНАННІ НАПОВНЕНИХ ЕПОКСИКОМПОЗИТІВ
68. **Р. О. Іванов, Е. С. Рожко, А. В. Антонишин, І. В. Чихіра** **459**
РОЗРОБКА СИСТЕМИ АВТОМАТИЗАЦІЇ СКЛАДСЬКОГО УПРАВЛІННЯ НА БАЗІ ПЛК
69. **В. В. Яцишин, О. В.Пасіка, С. О. Куліков** **461**
КОНЦЕПТУАЛЬНА АРХІТЕКТУРА КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ ПРИВАТНИМИ РЕСТОРАНАМИ

УДК 004.45

Д. Р. Карабан; Р. О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧІВ ПРИ ВИКОРИСТАННІ МЕРЕЖІ ІНТЕРНЕТ

D. R. Karaban; R. O. Zharovskyi, Ph.D.

ANALYSIS OF PROBLEMS ENSURING ANONYMITY OF INTERNET USERS

Тема дослідження спрямована на вивчення проблем, пов'язаних з розробкою та використанням програмних засобів для забезпечення анонімності та захисту від відстеження в Інтернеті. На сьогоднішній день існує значна кількість подібних інструментів, таких як VPN-сервіси та анонімайзери, але багато з них стикаються з низкою технічних і етичних викликів [1].

В першу чергу, досягнення максимальної анонімності в Інтернеті виявляється складним завданням через множину факторів, які необхідно враховувати. Багато сервісів пропонують лише частковий захист, а ідентифікація користувачів в мережі TOR [2], яка позиціонується як найбільш безпечна, не є рідкістю. Деякі VPN-провайдери також можуть володіти можливістю відстеження та збереження історії користувачів, що порушує приватність.

По-друге, використання анонімізації часто призводить до зниження зручності користувача через обмежену швидкість з'єднання та обмеження функціональності браузера. Рекомендації щодо підвищення безпеки можуть включати вимкнення потенційно небезпечних функцій, але це може призвести до недоцільності для нормальної роботи деяких веб-сайтів, які використовують JavaScript та Cookies [3].

По-третє, сам факт використання анонімізації може стати помітним та привернути увагу, що ускладнює використання деяких ресурсів та обмежує доступ до них. Багато сайтів блокують доступ з IP-адрес TOR, а існують інші фактори, які дозволяють зовнішнім спостерігачам виявити користувача, що приховує свою особистість.

Основною метою даного дослідження є оцінка та вивчення можливості створення засобу анонімізації, який має максимально ефективно поєднувати всі якості, розглянуті вище: надійність, зручність, непомітність використання, простота налаштування. Дані якості найчастіше вважаються несумісними (посилення безпеки знижує комфортність тощо), тому необхідно визначити граничні можливості їх поєднання та доступні шляхи реалізації цього. У результаті спроектувати програмний продукт з перспективою його практичної реалізації та впровадження.

Література

1. Dutta, Nitul, et al. Being Hidden and Anonymous. Cyber Security: Issues and Current Trends, 2022, 17-36.

2. Fassl, Matthias, et al. Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. Proceedings of the ACM on Human-Computer Interaction, 2023, 7.CSCW2: 1-26.

3. Madhusudhan, R.; Surashe, Saurabh V. Privacy and Security Comparison of Web Browsers: A Review. In: International Conference on Advanced Information Networking and Applications. Cham: Springer International Publishing, 2022. p. 459-470.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

Д.Р. Карабин; Р.О. Жаровський
МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В ІНТЕРНЕТІ
D.R. Karaban; R.O. Zharovskyi
METHODS OF PROVIDING ANONYMITY IN THE INTERNET 237

Корнєв О., Пастух О.
РОЗРОБКА МУЛЬТИАГЕНТНОЇ ПРОГРАМНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ КУРСУ КРИПТОВАЛЮТ НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ
Korniev O., Pastukh O.
DEVELOPMENT OF A MULTI-AGENT SOFTWARE SYSTEM FOR FORECASTING THE CRYPTOCURRENCY COURSE BASED ON NEURAL NETWORK TECHNOLOGIES 238

Р. Войтович, М. Петрик
ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИРІШЕННЯ ЗАДАЧ КЛАСИФІКАЦІЇ БІООБ'ЄКТІВ НА ЗОБРАЖЕННЯХ
R. Voytovych, M. Petryk
APPLICATION OF NEURAL NETWORKS TO SOLVE THE PROBLEMS OF CLASSIFICATION OF BIOOBJECTS IN IMAGES 239

О.Р. Оробчук, Р. В. Гарматій
АКТУАЛЬНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ВЕБДОДАТКАХ
O.R. Orobchuk, R. V. Harmatii
INFORMATION SYSTEM FOR AUTOMATED VULNORABILITY DETECTION IN WEB APPLICATION 240

Олег Пастух, Назар Гушпіт
ГЛОБАЛЬНА СИСТЕМА ВЗАЄМОПОВ'ЯЗАНИХ КОМП'ЮТЕРНИХ МЕРЕЖ INTERNET COMPUTER
Oleh Pastukh, Nazarii Hushpit
GLOBAL SYSTEM OF INTERCONNECTED COMPUTER NETWORKS INTERNET COMPUTER 241

Лисенко М.О.
ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНТРОЛЮ ВІДВІДУВАНОСТІ ТА СЕАНСІВ КІНОТЕАТРУ З ВИКОРИСТАННЯМ СХОВИЩА ДАНИХ
Lysenko M.
DESIGN OF THE INFORMATION SYSTEM FOR MONITORING ATTENDANCE AND CINEMA SESSIONS USING A DATA WAREHOUSE 242

А.В. Мельник
СИСТЕМА АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ SELENIUM І JENKINS ТА СЕРЕДОВИЩА INTELLIJ IDEA
A.V. Melnyk
AUTOMATED TESTING SYSTEM USING SELENIUM AND JENKINS TOOLS AND INTELLIJ IDEA ENVIRONMENT 243

Олег Пастух, Юрій Олексійко
РОЗРОБКА ПРОГРАМНОЇ СИСТЕМИ КЕРУВАННЯ ГУЧНІСТЮ ЗВУКУ НА ОСНОВІ ВІДЕО ПОТОКУ ЖЕСТІВ РУКИ
Oleh Pastukh, Yuri Oleksiiko
DEVELOPMENT OF A SOFTWARE SYSTEM FOR CONTROLLING SOUND VOLUME BASED ON A VIDEO STREAM OF HAND GESTURES 244

Орлов Володимир
РОЗРОБКА ВЕБ-СЕРВІСУ ВЗАЄМОДІЇ З БЛОКЧЕЙНОМ ETHEREUM ДЛЯ ФІНАНСОВОЇ ПЛАТФОРМИ МОВОЮ PYTHON
Orlov Volodymyr
DEVELOPMENT OF A WEB SERVICE FOR INTERACTION WITH THE ETHEREUM BLOCKCHAIN FOR A FINANCIAL PLATFORM IN PYTHON 245

УДК 004.45

Д.Р. Карабан; Р.О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В ІНТЕРНЕТІ

D.R. Karaban; R.O. Zharovskyi, Ph.D.

METHODS OF PROVIDING ANONYMITY IN THE INTERNET

Існує широкий спектр методів для забезпечення анонімності користувачів в Інтернеті. Проксі-сервери мають кілька видів із своїми особливостями, проте найчастіше для анонімізації використовуються SOCKS5. Зараз їх надійність вважається обмеженою, оскільки вони самі по собі не забезпечують шифрування трафіку і можуть легко піддаватися деанонімізації, навіть при використанні проксі-ланцюга. Цю проблему часто вирішують шляхом комбінування їх з VPN.

VPN-сервіси також використовуються для анонімізації, проте основною проблемою залишається питання довіри до постачальника послуг. Більшість VPN-провайдерів стверджують, що не ведуть логів, але це важко перевірити, і часто логування все ж здійснюється. Крім того, при раптовому відключенні VPN-підключення весь трафік може потрапити в Інтернет безпосередньо, розкриваючи реальний IP. Ця проблема розв'язується налаштуванням правил файрвола.

SSH-тунелі спочатку були створені для інших цілей, але зараз використовуються і для анонімізації. Їхня шифрувальна техніка схожа на VPN, але принципи роботи та швидкість можуть бути іншими. На відміну від VPN, вони не направляють за умовчанням весь трафік через тунель і можуть використовуватися як локальні проксі-сервери.

Dedicated-сервери використовуються як віддалені робочі станції або платформа для власного VPN-сервера. Їх використання часто включає в себе віртуалізацію, коли на одному фізичному хості розташовано кілька віртуальних серверів, що ускладнює відстеження конкретного сервера.

Анонімна мережа Tor, яка раніше вважалася однією з найбільш надійних, тепер має випадки деанонімізації користувачів. Трафік на виході може бути прослуховований, і вихідна IP-адреса, що належить Tor, може викликати підозри.

JonDonym або JAP (Java Anonymous Proxy) направляє трафік через ланцюг серверів, і користувач може вибирати використовувані "каскади". Він має безкоштовні та платні варіанти. Браузер JonDoFox, спочатку збиралися як змішаний Firefox з додатковими розширеннями, зараз модифікований Tor Browser.

I2P - це анонімна децентралізована мережа, яка працює поверх інтернету і не використовує IP-адресацію. Вона перевершує Tor у надійності шифрування передаваних даних, але не завжди підходить для анонімізації доступу до зовнішнього інтернету через нестабільне та повільне підключення.

Віртуальні машини допомагають вирішити додаткові завдання безпеки під час анонімної роботи, а їх використання у поєднанні з іншими засобами є досить ефективним. "Антидетект" використовують складання браузерів із вбудованими заміною різних ідентифікаторів, але їх використання зачасту є обмеженим і часто пов'язане з нелегальною діяльністю.

Інші методи анонімізації можуть бути менш популярними, менше перевіреними або не гарантувати надійну анонімність. До них відносяться програми та браузерні розширення, спрямовані на захист від відстеження браузера, і вони часто доповнюють систему анонімізації.

Додаток Б.

Установки конфігурації браузера Firefox

privacy.resistFingerprinting = true – активувати деякі можливості протидії відстеженню, запозичені з Tor Browser (у цій роботі це було небажано, оскільки деякі відбитки в такому режимі ідентичні відбиткам Tor Browser, наприклад, Canvas fingerprint).

privacy.firstparty.isolate = true – політика First Party Isolation також запозичена з Tor, це блокування стороннього контенту, у тому числі Cookies, які не відносяться безпосередньо до сторінки, що викликається. Може спричинити проблеми з деякими сайтами.

browser.safebrowsing.enabled = false

browser.safebrowsing.downloads.enabled = false

browser.safebrowsing.malware.enabled = false – відключення Safe browsing, що в теорії збільшує ризик зараження, але перш за все відключає відправку інформації про всі відвідувані сайти та завантажені файли на ресурси Google та Mozilla.

browser.search.suggest.enabled = false – відключає передачу тексту, що набирається у вікні пошуку, пошуковій системі без явного підтвердження запиту з боку користувача.

dom.enable_performance = false – вимкнути передачу браузером інформації про час початку та закінчення завантаження сторінки.

network.dns.disablePrefetch = true – заборонити попередню роздільну здатність імен для всіх посилань на веб-сторінці.

dom.battery.enabled = false – не відстежувати рівень заряду батареї. dom.network.enabled = false – не визначати параметри з'єднання з мережею (при цьому передається тип з'єднання).

media.peerconnection.enabled = false – заборонити підтримку WebRTC для захисту від витоку IP-адреси. Альтернатива: опція «Запобігти витоку локальної IP-адреси через WebRTC» у розширенні uBlock.

geo.enabled = false - відключення геолокації.

media.navigator.enabled = false

media.navigator.video.enabled = false — вимкнення взаємодії з мікрофоном та камерою.

media.navigator.streams.fake = true – режим генерування тестового аудіо та відеосигналу, що підміняють реальний сигнал від камери та мікрофона.

webgl.disable-extensions = true

webgl.min_capability_mode = true – обмеження функцій WebGL, що забороняє передачу сайтам докладної інформації про графічні можливості системи. Можна вимкнути WebGL і повністю (webgl.disabled = true) або блокувати його за допомогою NoScript, дозволяючи за необхідності.

privacy.trackingprotection.enabled = true – активувати захист від відстеження. В даний час ця функція доступна у звичайних налаштуваннях, або можна використовувати для цього uBlock з додатковими фільтрами (EasyPrivacy, Merged Ultimate List).

general.useragent.override = <рядок> – підміна User-agent вручну (але для цього зручніше використовувати розширення).

dom.webaudio.enabled = false – відключення AudioContext API (наразі вже існують доповнення для боротьби з Audio fingerprinting).

layout.css.visited_links_enabled = false – не виділяти відвідувані посилання.

Додаток В.

Конфігураційні файли

Вміст конфігураційного файлу сервера OpenVPN

```
port 443
proto tcp
dev tun
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
topology subnet
max-clients 200
ca ca.crt
cert server.crt
key server.key
dh none
tls-crypt tc.key
crl-verify crl.pem
mssfix 0
client-to-client
push "dhcp-option DNS 10.8.0.1"
ping 10
ping-restart 120
push "ping 10"
push "ping-restart 120"
persist-tun
cipher AES-256-GCM
tls-version-min 1.2
ncp-ciphers AES-256- GCM: AES -256-CBC
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA 256:TLS -
ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
remote-cert-tls client
tls-server
status-version 2
script-security 2
sndbuf 393216
rcvbuf 393216
reneg-sec 2592000
hash-size 1024 1024
verb 3
mute 3
replay-window 128
compress
log /dev/null
```

Вміст конфігураційного файлу клієнта OpenVPN

```
client
dev tun
dev-type tun
remote 192.168.10.10 443 tcp
nobind
persist-tun
cipher AES-256-GCM
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA 256:TLS -
ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
verb 4
mute 10
mssfix 0
ping 10
ping-restart 120
hand-window 70
server-poll-timeout 4
reneg-sec 2592000
sndbuf 393216
rcvbuf 393216
remote-cert-tls server
tls-client
compress
block-outside-dns
script-security 2
auth-nocache
<ca>
#-----CERTIFICATE-----
</ca> <tls-crypt>
#OpenVPN static key </tls-crypt>
<cert>
#-----CERTIFICATE-----
</cert>
<key>
#-----PRIVATE KEY-----
</key>
```

Додаток Д.

Онлайн засоби для тестування системи протидії відстеженню і ідентифікації

https://2ip.ua/privacy - Визначає наявність VPN або проксі-сервера за характерними особливостями. Слід зазначити, що за повної відсутності засобів анонімізації цей сайт також видасть «добрий» результат.

https://whoer.net - також перевіряє ознаки наявності анонімайзера, але деякі параметри відрізняються від 2ip.ua: відмінність мови браузера, неповна заміна User-agent, присутність IP у «чорних списках». Додатково відображає різні дані про браузер та виводить деякі рекомендації щодо підвищення безпеки.

https://www.perfect-privacy.com/dns-leaktest/ — найбільш надійний сервіс для визначення DNS-серверів, що використовуються, дозволяє перевірити відсутність витоків (бажано повторити тест кілька разів).

Основні сайти для визначення цифрових відбитків:

https://browserleaks.com/ - дозволяє отримати відбитки Canvas, WebGL 2.0, шрифтів (Font fingerprinting), прямокутних блоків (метод getClientRects), показує різну інформацію, доступну через JavaScript, перевіряє функції WebRTC. Визначає ступінь «унікальності» відбитка Canvas та його відповідність відомим браузерам.

https://audiofingerprint.openwpm.com/ - Відбиток AudioContext API. https://browserprint.info - Комплексний відбиток по ряду параметрів, включаючи шрифти, Canvas, AudioContext, розмір екрану та інші.

https://panopticlick.eff.org/ — один із перших сайтів, які демонстрували технологію цифрового відбитка браузера має схожість з BrowserPrint, але набір параметрів трохи менше.