МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Метод протидії відстеження та ідентифікації користувачів мережі Інтернет».

Виконавець: _____ Артем ЛИСЯНИЙ
(підпис)

Керівник: _____ Ірина КОЗЛЮК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Лисяного Артема Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Метод протидії відстеження та ідентифікації користувачів мережі Інтернет»

затверджена наказом ректора від «28» вересня 2023 р. №1965/ст

2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.

3. Вихідні дані до роботи: існуючі методи анонімізації в мережі інтернет

4. Зміст пояснювальної записки:.проблематика збереження анонімності та приватності; методи забезпечення анонімності в інтернеті; проєктування програмного комплекту; запуск та тестування

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft Power Point Office 365, лістинг файлу налаштувань параметрів анонімності.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	02.10.2023-04.10.2023	Виконано
2	Вступ	05.10.2023-08.10.2023	Виконано
3	Проблематика збереження анонімності та приватності	09.10.2023-22.10.2023	Виконано
4	Методи забезпечення анонімності в інтернеті	23.10.2023-05.11.2023	Виконано
5	Проєктування програмного комплекту	06.11.2023-14.11.2023	Виконано
6	Запуск та тестування	15.11.2023-30.11.2023	Виконано
7	Охорона праці	01.12.2023-06.12.2023	Виконано
8	Охорона навколишнього середовища	07.12.2023-17.12.2023	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	18.12.2023-31.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професор Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “22" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Ірина КОЗЛЮК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Артем ЛИСЯНИЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Метод протидії відстеження та ідентифікації користувачів мережі Інтернет» містить 116 сторінок, 19 рисунків, 5 таблиць, 74 використаних джерела.

ПРИВАТНІСТЬ В ІНТЕРНЕТІ, АНОНІМНІСТЬ ОНЛАЙН, ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ, ШИФРУВАННЯ ДАНИХ, VPN ТА КОНФІДЕНЦІЙНІСТЬ, АНОНІМІЗАЦІЯ IP-АДРЕС, БЛОКУВАННЯ ВІДСТЕЖЕННЯ, АНОНІМНІСТЬ ТА БЕЗПЕКА БРАУЗЕРІВ, ТЕХНОЛОГІЇ ЗАХИСТУ ОСОБИСТОЇ ІНФОРМАЦІЇ, КОНФІДЕНЦІЙНІСТЬ МЕРЕЖЕВОГО З'ЄДНАННЯ, БРАУЗЕРНІ КУКІ ТА ЇХ ВПЛИВ НА КОНФІДЕНЦІЙНІСТЬ, ПРОКСІ-СЕРВЕРИ ТА ЇХ РОЛЬ У КОНФІДЕНЦІЙНОСТІ, ЗАХИСТ ВІД ОНЛАЙН-ШПИГУНСТВА, КОНТРОЛЬ ЗА ВІДСТЕЖЕННЯМ АКТИВНОСТІ, КОНФІДЕНЦІЙНІСТЬ МОБІЛЬНИХ ПРИСТРОЇВ, ІНФОРМАЦІЙНА БЕЗПЕКА ТА АНТИВІРУСИ, СИСТЕМИ ЗАПОБІГАННЯ ВИТОКУ ДАНИХ, СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЗАХИСТ ВІД НЕЇ, ГЛОБАЛЬНІ СТАНДАРТИ ЗАХИСТУ ДАНИХ (GDPR, CCPA ТОЩО), ЕФЕКТИВНІСТЬ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ В ІНТЕРНЕТІ.

Об’єкт дослідження – методи та технології, спрямовані на забезпечення конфіденційності, анонімності та захисту особистих даних користувачів в мережі Інтернет. Основна увага при цьому приділяється розробці та вдосконаленню інструментів для протидії відстеженню, ідентифікації та моніторингу користувачів в онлайн середовищі.

Предмет дослідження – процеси, методи та технології, спрямовані на вивчення та забезпечення конфіденційності, анонімності, безпеки та захисту особистих даних користувачів у мережі Інтернет.

Мета кваліфікаційної роботи – оцінка та вивчення можливості створення засобу анонімізації, який має максимально ефективно поєднувати всі якості, розглянуті вище: надійність, зручність, непомітність використання, простота налаштування.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

VPN: Віртуальна приватна мережа (Virtual Private Network).

IP: Інтернет-протокол (Internet Protocol).

ISP: Постачальник послуг Інтернету (Internet Service Provider).

DNS: Система доменних імен (Domain Name System).

TOR: The Onion Router (анонімна мережа для забезпечення конфіденційності).

SSL/TLS: Secure Sockets Layer / Transport Layer Security (протоколи шифрування та аутентифікації).

Cookies: Куки (інформація, яку веб-сайт зберігає на пристрої користувача).

OSINT: Відкрите джерело інформації (Open Source Intelligence).

MAC-адреса: Медіа-адреса керуючого (Media Access Control address).

2FA: Двоетапна перевірка особи (Two-Factor Authentication).

HTTPS: Захищений протокол передачі гіпертексту (HyperText Transfer Protocol Secure).

AI: Штучний інтелект (Artificial Intelligence).

GDPR: Загальний регламент з питань захисту даних (General Data Protection Regulation).

DPI: Глибоке аналізування пакетів (Deep Packet Inspection).

P2P: Рівень до рівня (Peer-to-Peer).

IoT: Інтернет речей (Internet of Things).

IMSI: Міжнародний ідентифікатор мобільного абонента (International Mobile Subscriber Identity).

NGFW: Наступне покоління брандмауер (Next-Generation Firewall).

MAC-фільтрація: Фільтрація за MAC-адресою (Media Access Control Filtering).

Cryptography: Криптографія (техніка забезпечення конфіденційності та безпеки даних).

ВСТУП

Актуальність теми. Дана кваліфікаційна робота розглядає проблему розробки та використання ефективних програмних засобів, що забезпечують анонімність і протидію відстеженню під час роботи в Інтернеті. Нині існує велика кількість подібних інструментів, а VPN-сервіси та різні "анонімайзери" набувають дедалі більшої популярності. Однак практично всі вони мають ті чи інші недоліки.

По-перше, максимально надійне забезпечення анонімності є складним комплексним завданням, що включає безліч різних факторів, і багато сервісів вирішують це завдання лише частково. Відома низка випадків ідентифікації користувачів навіть у мережі TOR, яка часто позиціонується як найбезпечніша. Крім того, багато VPN-провайдерів можуть навмисно відстежувати і зберігати історію дій користувача, а потім надавати її за запитом державних служб.

По-друге, під час використання подібних інструментів часто знижується зручність роботи через невисоку швидкість з'єднання, а також обмеження функціональності браузера. Для надійного захисту часто пропонується відключати деякі потенційно небезпечні функції, які можуть призвести до витоку даних і розкриття особистості анонімного користувача, але є необхідними для нормальної роботи багатьох інтернет-сайтів. Насамперед сюди належить вимкнення JavaScript і заборона приймання Cookies.

По-третє, сам факт використання анонімізації часто виявляють за різними ознаками, що може привертати увагу до користувача. Також це може ускладнювати роботу: наприклад, деякі сайти обмежують доступ з IP-адрес, що належать вузлам TOR. Існує безліч чинників, які дають змогу зовнішньому спостерігачеві визначити, що користувач намагається приховати свою особистість. Таким чином, непомітність, скритність є ще одним важливим параметром надійного засобу анонімізації, але більшість наявних рішень не забезпечують цього.

Нарешті, не всі інструменти і схеми забезпечення мережевої анонімності можна назвати простими в налаштуванні та використанні, якщо враховувати, що вони повинні бути зрозумілі будь-якому інтернет-користувачеві, а не тільки "просунутому". Надійність роботи особливо складних схем буде сильно залежати від рівня знань і навичок користувача, вимагати чіткого розуміння принципів і деталей налаштування. Однак надійна мережева анонімність у сучасних реаліях може знадобитися найрізноманітнішим категоріям користувачів. Природно, необхідний рівень безпеки залежить від конкретного сценарію використання.

Додатковою проблемою є брак актуальних наукових публікацій, особливо україномовних, у цій галузі. Значна частина корисної інформації міститься на різних Інтернет-ресурсах, форумах, зокрема всередині анонімних мереж, але не в тих джерелах, які вважалися б авторитетними. Крім того, останнім часом подібна інформація починає піддаватися цензурі, однак це лише підтверджує поточну актуальність проблеми анонімності в Інтернеті [1-60].

Основною метою кваліфікаційної роботи є оцінка та вивчення можливості створення засобу анонімізації, який має максимально ефективно поєднувати всі якості, розглянуті вище: надійність, зручність, непомітність використання, простота налаштування. Ці якості найчастіше вважаються несумісними (посилення безпеки знижує комфортність тощо), тому необхідно визначити граничні можливості їхнього поєднання та доступні шляхи реалізації цього. У підсумку - спроєктувати програмний продукт із перспективою його практичної реалізації та впровадження.

Під час дослідження вирішуються такі **наукові завдання:**

- Збирання та аналіз інформації про всілякі засоби і методи забезпечення анонімності в Інтернеті, актуальні на цей час;
- Конкретизація та розгляд чинників, за якими можливе відстеження користувача під час роботи в мережі;
- Аналіз різних шляхів витоку даних, що призводить до порушення анонімності;
- З'ясування можливості забезпечення тих чи інших аспектів захисту без шкоди зручності роботи з сайтами;

- Вивчення всіх ознак, за якими сам факт використання засобу анонімізації може бути помічений Інтернет-ресурсом або іншим спостерігачем;
- Виявлення нетехнічних чинників втрати анонімності, тобто помилок поведінки анонімного користувача в Інтернеті;
- Складання рекомендацій щодо технічної анонімізації та правил поведінки для різних моделей загроз.

Об'єктом дослідження – є методи та технології, спрямовані на забезпечення конфіденційності, анонімності та захисту особистих даних користувачів в мережі Інтернет. Основна увага при цьому приділяється розробці та вдосконаленню інструментів для протидії відстеженню, ідентифікації та моніторингу користувачів в онлайн середовищі.

Предметом дослідження – є процеси, методи та технології, спрямовані на вивчення та забезпечення конфіденційності, анонімності, безпеки та захисту особистих даних користувачів у мережі Інтернет.

Методи дослідження зазначеної теми включають різні підходи та техніки для вивчення та аналізу проблем конфіденційності та безпеки в Інтернеті:

- **Літературний аналіз:** систематичний аналіз наявної наукової літератури, публікацій, статей та досліджень, що стосуються методів протидії відстеженню та ідентифікації користувачів мережі Інтернет.
- **Емпіричні дослідження:** проведення специфічних експериментів, опитувань або аналізу даних для оцінки ефективності конкретних методів протидії відстеженню та ідентифікації користувачів.
- **Кейс-стаді:** дослідження конкретних випадків використання методів протидії відстеженню для аналізу їхньої ефективності та проблем, що виникають у реальних сценаріях.
- **Технічне моделювання та симуляції:** створення моделей та симуляцій для аналізу різних аспектів методів протидії відстеженню та оцінки їхньої ефективності.

- **Аналіз законодавства та політик:** вивчення та аналіз правових аспектів та політик, пов'язаних із захистом конфіденційності та протидією відстеженню в Інтернеті.
- **Системний аналіз:** аналіз системи як цілісності, включаючи взаємодію різних складових та елементів методів протидії відстеженню.

Наукова новизна та практичне значення отриманих результатів.

Наукова новизна включає розробку та вдосконалення технологій, методів та стратегій, які реалізуються з метою забезпечення приватності, конфіденційності та безпеки користувачів у цифровому середовищі:

- Вдосконалення технологій обробки та аналізу даних для забезпечення конфіденційності та захисту особистої інформації.
- Подальший розвиток ефективних методів анонімізації, які забезпечують високий рівень безпеки та конфіденційності.

Практичне значення отриманих результатів: ця робота робить внесок у наукове дослідження проблеми анонімної роботи в Інтернеті, протидії цензурі Інтернету та сучасним системам відстеження.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ПРОБЛЕМАТИКА ЗБЕРЕЖЕННЯ АНОНІМНОСТІ ТА ПРИВАТНОСТІ

1.1. Літературний пошук за темою кваліфікаційної роботи

На перший погляд, ця тема здебільшого обговорюється на неофіційних інтернет-ресурсах, однак насправді існує безліч наукових публікацій, присвячених потенційним вразливостям анонімних мереж, методикам ідентифікації пристроїв, розробленню нових засобів для захисту від найсучасніших технік відстеження тощо.

Публікація "PriVaricator: Deceiving Fingerprinters with Little White Lies", що з'явилася 2014 року на сайті Microsoft Research, описувала інструмент для випадкової підміни деяких даних про браузер, доступних через JavaScript, для боротьби з його ідентифікацією. У 2017 році група дослідників зі США опублікувала статтю "Cross-Browser Fingerprinting via OS and Hardware Level Features", в якій описується техніка розпізнавання комп'ютерів із високою точністю незалежно від використовуваного браузера, причому автори радять використовувати Tor Browser для протидії таким методам ідентифікації. Стаття дає гарне уявлення про сучасні способи так званого "фінгерпринтингу". Значна частина параметрів пов'язана з обробленням тривимірної графіки WebGL.

Одразу три статті за темою використання мережі Tor було опубліковано у 2015 році групою авторів з Нідерландського політехнічного університету. Наведено потенційні слабкості Tor, згадано деякі альтернативи та випробувано можливість роботи відеоконференц-зв’язку через Tor.

Робота "Online Tracking: A 1-million-site Measurement and Analysis" - дослідження методів відстеження, що трапляються нині, опубліковане Прінстонським університетом 2016 року.

Інтернет-ресурс The Free Haven містить велику добірку статей [1] на різні теми, що стосуються анонімності та шифрування, починаючи з 1977 року до теперішнього часу. Наприклад, стаття 2018 року "Inside Job: Applying Traffic

Analysis to Measure Tor from Within", опублікована Військово-морською дослідницькою лабораторією США, присвячена аналізу трафіку Tor через проміжні вузли і відстеженню використання onion-сервісів. Інший інтернет-проєкт [2], що належить американській правозахисній організації "Фонд електронних рубежів", є початковим посібником зі збереження конфіденційності та захисту від стеження в Інтернеті. Схожі матеріали та курси по безпеці в мережі публікувало Міністерство цифрової трансформації України.

М. Райтман у книжці "Мистецтво легального, анонімного та безпечного доступу до ресурсів Інтернету" (2017) висвітлює безліч тем: шифрування файлів та їхнє надійне видалення, використання менеджерів паролів, захист від вірусів, безпечне спілкування за допомогою наскрізного шифрування, анонімні мережі та інше. Детально описано роботу з системою Tails та інструментами PGP. Книжка Д. Колісніченка "Анонімність і безпека в Інтернеті" (2012) на більш простому рівні описує використання Tor і I2P, шифрування файлів та електронної пошти, а також загальні принципи поведінки.

1.2. Потреба в анонімності та захисті від відстеження

Проблема забезпечення анонімності в Інтернеті існувала від самого моменту виникнення Всесвітньої павутини, але особливо актуальною в усьому світі вона стала у 2013 році, коли Едвард Сноуден розкрив правду про програми глобального стеження - американську систему PRISM та інші комплекси негласного масового збору даних. Уже тоді це було названо безпрецедентним вторгненням у приватне життя громадян.

Спочатку ж Інтернет був саме "територією свободи". Але зараз прагнення держави і деяких комерційних структур "знати все" про кожного інтернет-користувача призвело до необхідності справжньої боротьби за недоторканність особистих даних. Сам факт наявності стеження просто дратує, навіть незалежно від того, яку саме активність у Мережі веде користувач - незаконну або абсолютно легальну [6]. Право на

приватність є одним із фундаментальних прав будь-якої сучасної людини, зокрема й в Інтернеті.

Насамперед розглянемо поняття анонімності. Під час роботи в Інтернеті анонімність - це неможливість пов'язати активність користувача з його реальною особою і місцем розташування. Але формально слід позначити відмінність між повною анонімністю і "псевдонімом" (у деяких англомовних публікаціях використовуються терміни anonymity і pseudonymity). Анонімне підключення до сервера означає, що сервер не здатний з'ясувати його початкове походження (справжній IP клієнта), а також пов'язати його з будь-яким ідентифікатором. Якщо ж є будь-який ідентифікатор (Cookie-файл, унікальний відбиток браузера тощо), за яким сервер може визначити, що цей клієнт підключався до нього раніше, то йдеться вже про "псевдонімності" [7]. Фактично, у багатьох випадках цього достатньо, немає необхідності прагнути зробити кожне підключення повністю унікальним. Проте чим довше використовується один і той самий "псевдонім", тим більше накопичується профілюючої інформації про його активність. Тому він повинен періодично змінюватися, інакше анонімність користувача може бути врешті-решт втрачена.

Помилково можна припустити, що анонімність означає повну відсутність даних про користувача. У низці випадків це або неможливо, або недоцільно. Приклад - власне IP-адреса. Під час відвідування сайту користувач може приховати свій справжній IP, але технічно неможливо зробити це так, щоб сервер не визначив узагалі ніякого IP (і водночас відправив контент за призначенням). Тобто IP-адреса зрештою не може бути повністю відсутньою, її можна тільки замаскувати. Другий приклад - User-agent браузера. Замінити його на порожній рядок можна, але категорично небажано. Такий браузер буде різко виділятися серед безлічі інших і набуде не анонімності, а особливої унікальності. До того ж багато сайтів у ньому працюватимуть некоректно. Тут слід зазначити, що User-agent сам по собі не унікальний і належить до тих параметрів, за якими неможливо однозначно ідентифікувати та відстежувати користувача - однак поєднання великої кількості "неунікальних" даних часто формує унікальний цифровий відбиток.

У травні 2015 року Рада з прав людини ООН представила звіт засідання, присвяченого анонімності та шифруванню в інтернеті [8]. Головний висновок документа: можливість анонімного користування інтернетом і використання шифрування особистих даних і засобів комунікації є необхідними і мають розцінюватися як частина прав людини. Незважаючи на те, що засоби анонімізації нерідко застосовуються зловмисниками, сама можливість бути анонімним в Інтернеті - лише засіб, що може бути використаний у найрізноманітніших цілях і з різних мотивів. Але досі часто трапляється думка, що "звичайному законослухняному користувачеві" анонімність просто не потрібна: йому нема чого приховувати від держави, і його діяльність в Інтернеті нікому не цікава [9]. Тут насамперед потрібно згадати, що самого факту збору даних це не скасовує. А відстеженням користувачів займаються не лише спецслужби, а й багато інтернет-компаній (Google, Apple, Meta - лише найяскравіший приклад), і взагалі більшість веб-сайтів [10]. Тим часом, історія дій користувача в Мережі належить до особистих даних і не призначена для сторонніх очей, як і особисте листування. Позиція "мені нема чого приховувати" фактично означає "мене не хвилює недоторканність мого приватного життя". Розробники TOR дотримуються принципу "можливо, це і не секрет, але це просто не ваша справа". Але найбільш вдало з цього приводу висловився американський юрист Гленн Грінвальд 2014 року: "Останні 16 місяців, що я обговорював цю тему в усьому світі, щоразу хтось говорив мені: "Я не особливо хвилююся з приводу вторгнення в особисте життя, тому що мені нема чого приховувати". Я завжди відповідаю їм однаково. Я дістаю ручку, пишу адресу своєї електронної пошти і кажу: "Ось моя пошта. Я хочу, щоб ви, прийшовши додому, надіслали мені паролі до всіх ваших облікових записів, не тільки до банальної, пристойної робочої пошти, а й до всіх, тому що я б хотів мати можливість покопатися в тому, що ви робите онлайн, почитати, що захочу, опублікувати те, що здасться мені цікавим. Зрештою, якщо ви не погана людина, якщо ви не робите нічого поганого, то вам не потрібно нічого приховувати". Жодна людина не прийняла моєї пропозиції. Я щоразу сумлінно перевіряю свою пошту, але вона порожня. І тому є причина, яка полягає в тому, що ми, будучи людьми, навіть ті з нас, хто на словах заперечує важливість власного приватного життя, інстинктивно розуміємо його надзвичайну важливість" [11].

Нарешті, деяким людям анонімність необхідна через специфіку їхньої роботи. Тут показова інформація про використання Tor у легальних цілях. Корпорації використовують його як безпечний спосіб проведення аналізу на конкурентному ринку, а також як доповнення до VPN. Журналісти можуть користуватися Tor для безпечного спілкування з інформаторами та дисидентами, соціальні працівники - під час спілкування з урахуванням тонкої соціальної специфіки в чатах і веб-форумах для біженців, жертв насильства. Неурядові організації використовують Tor для підключення своїх співробітників до потрібних сайтів у закордонних відрядженнях, якщо є сенс не афішувати їхню роботу. Деякі громадські організації рекомендують Tor для забезпечення безпеки своїх членів. Спецслужби використовують Tor для забезпечення секретності під час виконання особливих завдань. Громадські активісти з EFF (Фонд електронних рубежів) підтримують розробку Tor, оскільки вбачають у ньому механізм для захисту базових громадянських прав і свобод в Інтернеті [12].

1.3. Можливість збереження анонімності

Отже, в умовах сучасного світу надійна інтернет-анонімність може знадобитися практично будь-якій людині. Однак необхідний і достатній рівень безпеки для різних категорій користувачів буде різним: наприклад, одній людині життєво необхідно ховатися від упізнання, а іншій потрібен "анонімайзер" просто для доступу до заблокованих веб-сайтів. Відповідно, вибір методу забезпечення анонімності починається з чіткого розуміння, для чого саме потрібна ця анонімність. Загальна схема моделювання загроз під час захисту персональних даних включає 5 основних питань (за версією EFF):

1. Що саме ви хочете захистити?
2. Від кого ви збираєтеся це захищати?
3. Наскільки висока ймовірність того, що вам доведеться це захищати?
4. Які можуть бути наслідки, якщо ви зазнаєте невдачі?
5. Які ресурси ви готові витратити на запобігання цим наслідкам? [13]

Очевидно, що ідеальна безпека неможлива, будь-яке рішення містить певний компроміс. Нині нерідко можна зустріти висловлювання, що анонімності в Інтернеті вже не існує. Проте, забезпечити анонімну роботу в Інтернеті в разі потреби - як і раніше можливо. Необхідно пам'ятати таке:

1. Адекватно оцінювати потенційного "противника". Інтернет-провайдер або власник точки доступу Wi-Fi часто мають можливість прослухати більшу частину трафіку, але, як правило, не зацікавлені в активному відстеженні та деанонімізації користувача. Що ж стосується власників використовуваних ресурсів (веб-сайтів, проксі/VPN-серверів), то у них у розпорядженні безліч засобів для відстеження (витік DNS, Flash-плагіни, банерні мережі, різні "відбитки браузера", кілька різних видів Cookies) і серйозний комерційний інтерес до того, щоб надійно відстежувати користувача (для таргетування реклами, продажу даних тощо). А уряд і спецслужби можуть отримати доступ і до даних, зібраних веб-сайтами, і до даних, які зберігаються у провайдера. Таким чином, ті, хто мають можливість і бажання відстежувати користувача - мають доступ до більшості можливих каналів витоку.

2. Каналів витоку інформації дуже багато, і вони дуже різноманітні (раптове вимкнення VPN, отримання реального IP через WebRTC або Flash-плагіни браузера, надсилання серійного номера якимось додатком під час спроби оновлення). При цьому регулярно виявляються (і створюються) нові шляхи витоку. Тому спроба блокувати кожен із них в індивідуальному порядку, унікальними для кожного методами, може просто не мати сенсу, однаково щось виявиться упущено.

3. Під час "роботи в інтернеті" використовується не тільки браузер - у багатьох користувачів буде також запущено якийсь месенджер, поштовий клієнт, торрент-клієнт, що-небудь ще. При цьому інформація, що передається їхніми каналами, часто перетинається і дає змогу зв'язати їх між собою (.torrent-файл, викачаний із сайту, завантажується в торрент-клієнт, посилання, яке прийшло в листі/повідомленні, відкривається в браузері тощо). Додамо до цього те, що сама ОС і багато застосунків регулярно з'єднуються з мережею для пошуку оновлень і з інших причин, передаючи різну інформацію, яка також може виявитися ідентифікуючою [14].

Таким чином, часткова "анонімність" фактично не є анонімністю. Вона може бути достатньою для деяких завдань, але майже марна в тих випадках, коли існує потреба в дійсно повноцінній анонімності. Зрозуміло, жодна схема не може бути абсолютно надійною, до того ж деанонімізація нерідко відбувається через помилки в поведінці самого користувача - аспекти соціальної анонімності не можна забезпечити технічними методами. Соціальна інженерія ніколи не втрачає своєї ефективності. Рекомендації щодо анонімної поведінки також будуть розглянуті далі, але основною темою дослідження є технічна анонімність - те, що залишається в межах можливостей програмного забезпечення.

Захист від відстеження має деякі технічні обмеження, оскільки його блокування можливе не у всіх випадках. З одного боку, багато веб-сайтів використовують відстежувальні елементи [10], сторонні трекери для реклами, аналітики та інших маркетингових інструментів, і наразі популярні браузерні розширення для "захисту від відстеження" - більшість таких трекерів справді можна заблокувати. З іншого боку, всі підключення до сервера записуються в лог, тому факт відвідування сайту буде зафіксовано незалежно від рівня анонімності клієнта. Також, наприклад, якщо провайдер може прослуховувати весь трафік, то використання VPN не впливає на сам процес перехоплення, хоча й робить його малоефективним. Таким чином, правильніше говорити не про захист від відстеження, а про захист конфіденційності даних в умовах відстеження. Виключити відстеження повністю - неможливо.

1.4. Способи ідентифікації та відстеження

Основні шляхи витоку даних.

1) IP-адреса, найочевидніший ідентифікатор, дає змогу визначити провайдера і країну (нерідко і місто). Якщо ж проводиться цілеспрямований розшук користувача, запит до провайдера дає безліч додаткових даних і в найпростішому випадку встановлює особу. Будь-який анонімайзер насамперед підміняє IP-адресу. Слід розуміти, що це ніяк не впливає на реальний IP хоста, виданий провайдером. Запити так чи інакше перенаправляються на деякий вихідний вузол, адреса якого слугуватиме

"підставним", але головне завдання полягає в тому, щоб зробити визначення первісного IP максимально складним.

2) DNS провайдера. У деяких випадках DNS-запити можуть іти в обхід анонімного каналу. Не всі засоби анонімізації забезпечують захист від витоку DNS.

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

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

5) Одночасне підключення до сервера анонімним і відкритим каналами може в деяких ситуаціях створити проблеми, наприклад, у разі обриву інтернет-з'єднання обидва канали перестануть функціонувати, і на сервері потенційно можна буде визначити їхню пов'язаність, зіставивши час від'єднання користувачів.

6) Активність, що деанонімізує, в анонімному сеансі - користування публічними сервісами, особливо тими, на яких уже є інформація про цього користувача.

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

8) Інформація з браузерів. Окрема велика категорія способів ідентифікації, яку слід розглянути дуже докладно.

Відстеження через веб-браузер.

- **Стандартні HTTP Cookies.** Під час першого входу на сайт не призводять до жодних витоків даних, але надалі слугують ідентифікатором користувача. Водночас повне блокування прийому Cookies може бути неприйнятним, оскільки заважає нормальній роботі з сайтом. Протидією зазвичай служить регулярне очищення cookies, а іноді їх модифікування.

- **Сторонні (третьої сторони, 3rd party) cookies** встановлюються сторонніми ресурсами, підключеними до сайту, що відвідується. Головним чином пов'язані з таргетуванням реклами, заборона їхнього прийому зазвичай не порушує роботу сайту.
- **LSO (Local Shared Objects)** або **Flash Cookies** є загальними для всіх браузерів і не видаляються під час стандартного очищення cookies. Налаштування Flash Player дають змогу вимкнути можливість зберігання LSO.
- **HSTS SuperCookies** використовує прапори HSTS, що зберігаються в браузері, для встановлення двійкового ідентифікатора. Вони видаляються під час очищення звичайних cookies.
- **HTTP Etag** призначений для перевірки вмісту кешу, але може бути використаний як ідентифікатор. Було описано подібне застосування і для заголовка Last-Modified, він може зберігати довільний рядок замість дати. Збережені Etag видаляються шляхом очищення кешу.
- **Evercookie** [16], "невидаляємі куки" використовують набір механізмів зберігання і відновлюються з резервних копій після неповного очищення. Включають у себе всі згадані вище методи, а також: зберігання ідентифікатора у властивості window.name, використання сховищ HTML5 localStorage, sessionStorage, indexedDB, ізольованого сховища Silverlight і деякі інші способи залежно від їхньої доступності. Через здатність відновлення (якщо хоча б в одному зі сховищ залишилася копія, будуть відновлені всі інші копії) також відомі як zombie cookie.
- **HTML5 AppCache** також дає змогу зберігати унікальні дані як ідентифікатор. Займає проміжне значення між механізмами зберігання даних у HTML5 і звичайним кешем браузера.
- **SDCH-словники** - розроблений Google алгоритм компресії, заснований на використанні наданих сервером словників. Ці словники можна використовувати і для зберігання унікальних ідентифікаторів, які можна помістити як в ID словників, так і безпосередньо в сам контент [17].
- **Ubercookie** описувалися як "сучасна версія Evercookie", але фактично це не різновид Cookie, а один зі способів отримання цифрового відбитка (browser

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

Цифровий відбиток веб-браузера.

- **Canvas fingerprinting** - відтворення прихованого зображення з використанням HTML5 canvas і подальше переведення його в бінарну форму [18]. Причому малюється текст, з використанням доступних системі шрифтів і рендерера. Набір шрифтів і методи згладжування трохи відрізняється на різних машинах. Рендерер залежить від версії браузера, ОС і від GPU. У підсумку відмальоване зображення майже унікальне (залишається невелика ймовірність збігу). Існують браузерні доповнення, що дають змогу або блокувати відтворення, або підміняти відбиток. При цьому помилкове значення може мати 100% унікальність, але відстежувати за ним неможливо, оскільки під час кожного відвідування сторінки генерується новий відбиток.
- **WebGL fingerprinting** [19] - рендеринг зображення, як і в canvas fingerprint, але з використанням API WebGL. За наявності підтримки WebGL 2 доступний набір даних сильно збільшується. З урахуванням того, що більшість сайтів не використовують WebGL для роботи, вимкнення WebGL у браузері зазвичай не спричиняє додаткових проблем, однак 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 в системних налаштуваннях динаміків.
- **Метод getClientRects** дає змогу отримати точний розмір і положення прямокутника в наявному елементі DOM. Ці значення можуть і з високою часткою ймо-

вірності будуть відрізнятися на різних комп'ютерах, навіть з однаковою версією браузера. Спочатку був запропонований для відстеження користувачів Tor Browser [21]. Зміна масштабу сторінки вплине на відбиток.

- **Mouse fingerprinting:** корисною інформацією є швидкість прокрутки колеса миші та рухи курсору, доступні для відстеження за допомогою JavaScript. Спосіб відстеження користувачів за рухами миші спочатку здавався безглуздим, але, за деякими даними, він успішно використовується на практиці [21]. Таку технологію можна віднести вже до поведінкового аналізу.
- **Заголовки HTTP_Accept** містять набір значень, які можуть здатися стандартними для багатьох браузерів, але ймовірність їхнього збігу у двох браузерів становить близько 1:1700.
- Список встановлених плагінів, а також розширень (частково). Від плагінів залежить і список підтримуваних MIME-типів.
- Набір встановлених шрифтів, крім впливу на відбиток canvas, може використовуватися й окремо. На їхній основі генерується так званий Font fingerprint.
- **Хід годинника.** Якщо система не синхронізує свій годинник зі стороннім сервером часу, то він почне відставати або поспішати, що створить унікальну різницю між реальним і системним часом, яку можна виміряти з точністю до мікросекунди за допомогою JavaScript. Але навіть при синхронізації з NTP-сервером будуть невеликі відхилення, які також можна буде виміряти [17].

Для оцінювання значущості ознак може бути використано ентропійний підхід. Під ентропією розуміють кількість інформації, що припадає на одне елементарне повідомлення джерела, яке виробляє статистично незалежні повідомлення. Оскільки характеристики на кшталт "майже унікальний" або "малозначущий" не є точними, дослідники з Electronic Frontier Foundation запропонували кількісну оцінку в бітах ентропії [22]. Так, для Canvas fingerprint ентропія становить близько 15,5 біт, унікальність цього відбитка (якщо не ввімкнено підміну) - 1 на 48000.

Навпаки, інформація про те, що в браузері дозволено прийом Cookies, має найнижчу цінність - близько 0,2 біт. Далі наведено ознаки з відносно низькою ентропією, придатні для відстеження тільки в поєднанні з набором інших властивостей.

- Роздільна здатність монітора і розмір вікна браузера (включно з параметрами другого монітора в разі мультимоніторної системи), а також глибина кольору. Окремо визначається "доступна область" (availWidth і availHeight), часто відрізняється від основної. Може бути отримано не тільки через JavaScript, а й без нього за допомогою медіа-запитів CSS.
- **User-Agent.** Показує версію браузера та ОС. Може бути легко змінений, але це не завжди має сенс, оскільки є й інші шляхи визначення платформи.
- Рядок javascript navigator.userAgent, а також поля javascript-об'єкта navigator: appCodeName, appName, appVersion, buildID, oscpu, platform, product, productSub, vendor, vendorSub. Розширення для підміни User-Agent зачіпають і navigator.userAgent, але решту параметрів нерідко ігнорують і легко видають невідповідність. Функціонал для їхньої підміни помічений у розширенні "User-agent Switcher".
- **Заголовок HTTP Referer** дає змогу серверу визначити, що користувач перейшов на цю сторінку з іншого сайту, що допомагає відстежувати переміщення. Часто буває необхідний для нормального функціонування сайту.
- Мова браузера (JavaScript navigator.language) і бажана мова відображення сторінок (HTTP Accept-Language).
- Часовий пояс.
- Значення заголовка DNT (Do not track).
- Довжина історії вкладок - значення атрибута history.length.
- Наявність сенсорного екрана і підтримувана кількість торкань.
- Рівень заряду батареї (за наявності) через Battery Status API.
- Доступна інформація про CPU і GPU.
- Результат обчислення деяких математичних функцій. Приклад із сайту browserprint.info: функція Math.tan(-1e300) у Windows і в 64-бітному Linux повертає абсолютно різний результат.

Наведений список параметрів і методів складено на основі даних, що надаються інтернет-ресурсами BrowserSpy.dk, panopticlick.eff.org, Whoer.net, browserleaks.com, і він не є вичерпним.

Деякі сучасні технології відстеження, теоретично, призначені для антифрод-систем і не повинні зустрічатися на сайтах, не пов'язаних з електронними платежами. Але фактично це неможливо гарантувати. Значення має сам факт того, що деяка технологія існує і застосовується на практиці. Частина перелічених вище властивостей не залежать від браузера і можуть бути використані для крос-браузерної ідентифікації. Як уже згадувалося, сучасні fingerprinting-методи можуть навіть не враховувати версію браузера, але однаково розпізнавати конкретний ПК із високою точністю завдяки особливостям його апаратного забезпечення та операційної системи [23].

Загалом можна виокремити такі принципи анонімізації браузера: дані з низькою ентропією можуть узагалі не потребувати захисту, а якщо захист здійснюється, слід підміняти параметр на максимально поширене значення, не надаючи йому штучної нестандартності. Але слід періодично змінювати всі або деякі з цих параметрів, оскільки в сукупності вони все одно утворюють патерн із високою ентропією. Що ж стосується даних на кшталт canvas-відбитку, які мають найбільшу цінність, то їх слід змінювати щоразу, коли потрібно "змінити особистість".

Особливості деяких протоколів.

1. **Origin Bound Certificates (ChannelID)** - самопідписані сертифікати, що ідентифікують клієнта HTTPS-серверу. Для кожного нового домену створюється окремий сертифікат, який використовується для з'єднань, ініційованих надалі. Сайти можуть використовувати OBC для трекінгу користувачів, не роблячи при цьому будь-яких дій, які будуть помітні клієнту. Як унікальний ідентифікатор можна використовувати криптографічний хеш сертифіката, що надається клієнтом як частина легітимного SSL-рукостискання.

2. Подібним чином і в TLS є два механізми - session identifiers і session tickets, які дають змогу клієнтам відновлювати перервані HTTPS-з'єднання без виконання повного рукостискання. Досягається це за рахунок використання закешованих даних. Два ці механізми протягом невеликого проміжку часу дають змогу серверам ідентифікувати запити, які надходять від одного клієнта.

3. Практично всі сучасні браузери реалізують свій власний внутрішній DNS-кеш, щоб прискорити процес вирішення імен (і в деяких випадках знизити ризик DNS rebinding атак). Такий кеш можна використовувати для 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 провайдера [17].

Виявлення присутності засобів анонімізації.

1) Витік реального IP через Flash. Актуально в тих випадках, коли анонімізується тільки трафік браузера, а не всієї системи. У разі використання проксі-сервера можна примусово направити через нього трафік Flash за допомогою Proxifier або іншої аналогічної програми. Якщо під час анонімної роботи не потрібна наявність Flash-плагіна, рекомендується його відключати [24].

2) Витік IP через WebRTC може відбуватися навіть під час використання VPN. Найчастіше WebRTC не потрібен для роботи сайту, і його вимкнення в браузері не спричиняє проблем, але є і способи підміни IP, що розкривається.

3) Витік DNS призводить до явної невідповідності IP-адреси і використовуваного DNS-сервера, а також побічно розкриває найменування інтернет-провайдера. Використання публічних DNS-серверів (наприклад, Google) не вважається підозрілим. У разі, якщо VPN-клієнт не забезпечує стабільний захист від такого витоку, доцільно використовувати DNSCrypt, за можливості вибравши адресу DNS тієї країни, якій відповідає підмінна IP-адреса. Навіть якщо неможливо забезпечити відповідність, це вбереже від витоку оригінального DNS.

4) Невідповідність браузерних даних про ОС і характерних особливостей TCP для цієї ОС. Різні системи по-різному формують TCP-пакети, утиліта p0f дає змогу точно визначити ОС і приблизно її версію. Однак під час використання проксі-сервера буде визначено ОС, на якій працює проксі, оскільки саме він генерує пакети. У підсумку розбіжність цих даних із User-agent браузера означає або підміну User-agent, або використання проксі-сервера [25].

5) Належність IP-адреси до мережі Tor очевидно вказує на використання Tor, оскільки адреси всіх вихідних вузлів відомі. Використання VPN через TOR - один зі шляхів вирішення проблеми.

6) Розбіжність часового поясу: IP-адреса має певну геолокацію, що дає змогу співвідносити її з часовим поясом. Невідповідність системному часу означає підміну IP. Практично всі анонімайзери не підміняють часовий пояс у браузері, за винятком деяких браузерних розширень. Зазвичай потрібно змінювати системні налаштування часу.

7) Заголовки HTTP Proxy. Проксі-сервери, що не належать до анонімних, передають IP-адресу клієнта за проксі. X_FORWARDED_FOR, FORWARDED_FOR, X_FORWARDED, HTTP_FORWARDED, HTTP_CLIENT_IP, HTTP_FORWARDED_FOR_IP, HTTP_VIA, FORWARDED_FOR_IP, HTTP_PROXY_CONNECTION - можуть містити реальний IP. З іншого боку, існує тактика навмисної імітації використання проксі, коли в порожній заголовок підставляється випадковий IP- адресу. Це створює враження, що основний IP є адресою проксі-сервера. Так працює, наприклад, плагін Dolus.

8) Відкриті порти, характерні для проксі, веб-проксі, VPN. Переважно використання нестандартних портів, за можливості - з авторизацією.

9) Так званий VPN fingerprint - виявлення використання VPN за характерними значеннями MTU/MSS і деякими іншими ознаками, особливо актуально для OpenVPN [25].

10) Підозріла назва хоста: якщо за кінцевим IP дозволяється ім'я хоста, воно не повинно містити слова на кшталт vpn, hide, proxy тощо. Під час налаштування власного VPN або проксі-сервера слід уникати "промовистих" імен, але переважною є повна відсутність імені, доступного для зовнішніх зворотних DNS-запитів.

11) Визначення тунелю за двостороннім пінгом. Запустивши пінг до клієнтського IP з боку сервера, можна дізнатися приблизну довжину маршруту. Те ж саме можна зробити з боку браузера через XMLHTTPRequest. Отриману різницю в петлі понад 30 мс можна інтерпретувати як тунель. Спосіб спрацьовує не у всіх випадках [24].

12) Мова браузера, нехарактерна для країни, що визначається за IP. Може вказувати на використання анонімайзера, але можливі винятки. Якщо присутня тільки англійська мова, то параметр вважається нейтральним.

13) Належність IP хостинг-провайдеру: зазвичай вказує на використання VPS.

Атаки перетину і підтвердження в анонімних мережах.

Атаки підтвердження (окремий випадок атак перетину) ґрунтуються на тому, що у супротивника є припущення, який мережевий ресурс відвідує цей користувач через анонімну мережу. Йому потрібно лише підтвердити або відкинути цю гіпотезу. Для цього противнику потрібно зняти дані трафіку з точки входу користувача в анонімну мережу і точки виходу з неї до цього ресурсу (або на самому ресурсі). У мережах із малою затримкою передавання даних спостерігатимуться явні кореляції за числом пакетів, за часом їхнього відправлення та іншими параметрами, що дасть змогу обчислити користувача за один сеанс з імовірністю понад 90%, тоді як імовірність помилки може бути меншою за тисячні частки відсотка. Якщо противник застосує активні методи - наприклад, сам буде вносити затримки в трафік або пошкоджувати пакети, то для повного розкриття користувача іноді достатньо одного пакета даних.

Ці атаки дещо ускладнені проти прихованих ресурсів Tor і замкнутих файлообмінних мереж на кшталт Freenet, оскільки противнику невідомо, звідки знімати трафік, навіть якщо він знає, до якого ресурсу хоче звернутися користувач. Проте, схожі атаки такого роду бувають досить ефективні і в цих випадках.

Інший варіант атак перетину (коли також заздалегідь невідома принаймні одна з двох точок, звідки потрібно знімати трафік) - супротивнику невідомий ресурс, до якого хоче звернутися користувач, але він контролює деяку кількість вузлів анонімної мережі. Якщо трафік користувача випадково пройде через ці вузли в початковій і кінцевій точці, достатньо кореляції статистичних параметрів трафіку (тобто без необхідності його розшифровки) між вхідним вузлом (або між точкою входу в анонімну мережу в провайдера користувача та кінцевим вузлом ланцюжка), щоб провести атаку перетину й подивитися, до якого ресурсу звертається користувач з останнього вузла

ланцюжка. При цьому кількість вузлів між першим і останнім вузлом ланцюжка не відіграє особливої ролі проти більшості такого роду атак і є аргументом щодо марності збільшення довжини ланцюжків більше трьох вузлів. Такий варіант атак істотно обмежує анонімність користувача в мережах типу Tor.

Варто пам'ятати, що анонімні мережі або захищають від аналізу трафіку (Tor), або забезпечують цензурозахищеність інформації (Freenet), але всі такого роду мережі погано захищені проти атак підтвердження отримання інформації, заздалегідь відомої супротивнику, або іншої можливості статистичних атак перетину. Побудова мереж із дотриманням умов такого роду - складне теоретичне завдання. У дизайні наявних анонімних мереж атаками перетину і підтвердження здебільшого нехтують або обмежуються мінімальними заходами захисту, тому що захист від супротивника такого рівня надто складний, хоча і меншою мірою, ніж від умовного "глобального спостерігача". Різного роду атаки на знаходження кореляцій практично на 100% ефективні та тривіально прості проти поодиноких проксі, що шифрують, і VPN, які іноді використовують для отримання невисокого рівня "анонімності" [26].

ВИСНОВКИ ДО РОЗДІЛУ 1

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 в реальності містить багато неочевидних нюансів. Ідентифікаційні дані необхідно не просто приховувати, а й регулярно змінювати, оскільки статичний "псевдонім" схильний до відстеження не менше, ніж реальна особистість. Найбільшу складність може становити підміна цифрових відбитків зі збереженням їхньої повної правдоподібності.

РОЗДІЛ 2
МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В ІНТЕРНЕТІ

2.1. Основні категорії засобів анонімізації

1) Проксі-сервери - є кілька видів зі своїми особливостями, але зазвичай для анонімізації використовують SOCKS5. Наразі не можуть вважатися надійними, оскільки самі по собі не забезпечують шифрування трафіку, а також порівняно легко піддаються деанонімізації навіть під час побудови ланцюжка проксі: послідовне вивчення логів на кожному сервері дає змогу визначити реальний IP за будь-якої довжини ланцюжка. Переважно використання в поєднанні з VPN.

2) VPN-сервіси - також існує кілька протоколів, сервіси найчастіше є платними, забезпечують високу надійність шифрування каналу. Але, як і у випадку з проксі-сервером, основною проблемою стає питання довіри до провайдера сервісу. Переважна більшість VPN-провайдерів заявляють про відсутність ведення логів, насправді це неможливо перевірити, найчастіше логгування ведеться. Також VPN має такий недолік: у разі раптового розриву VPN-підключення весь трафік піде в інтернет безпосередньо, що призводить до розкриття реального IP. Проблема вирішується додатковим налаштуванням правил файрволу.

3) 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 і потенційно нижчу швидкість. На відміну від VPN, не спрямовують за замовчуванням увесь трафік у тунель (хоча для цього існують спеціальні програми), а використовуються на кшталт локального проксі-сервера.

4) Dedicated-сервери - використовуються як віддалене робоче місце або як платформа для запуску власного VPN-сервера. Нерідко використовують віртуалізацію (VPS), за якої на одному фізичному хості розташовується кілька віртуальних серверів, що ускладнює відстеження підключень до конкретного сервера [15].

5) Анонімна мережа Tor. Деякий час вважалася найнадійнішим засобом забезпечення анонімності в Інтернеті, надалі мали місце випадки деанонімізації користувачів. Трафік на багатьох вихідних вузлах прослуховується, до того ж вихід у мережу з IP-адреси, яка належить Tor, сам по собі розцінюється як підозрілий.

6) JonDonym, або JAP (Java Anonymous Proxy). Направляє трафік через ланцюжок серверів, користувач може сам обирати використовувані "каскади". Є безкоштовний і преміум-доступ. Браузер JonDoFox у ранніх версіях був збіркою Firefox із набором доповнень, а нині це модифікований Tor Browser.

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

8) Віртуальні машини - вирішують низку додаткових завдань безпеки під час анонімної роботи, використовуються в комбінації з іншими засобами. Гарантовано направити весь трафік віртуальної машини в канал VPN або Tor зазвичай легше, ніж зробити це з трафіком основної системи. Браузер всередині віртуальної машини не має доступу до даних про апаратне забезпечення фізичного хоста. Рекомендується використовувати в гостьовій системі оформлення, що помітно відрізняється від основного, 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].

9) Так звані "антидетекти" - збірки браузерів із вбудованою підміною різних ідентифікаторів. Часто створюються для нелегальної діяльності (націлені 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.

10) Інші засоби анонімізації - слабо популярні, недостатньо перевірені або такі, що не забезпечують надійну анонімність, інструменти. Також сюди належать програми та браузерні розширення, призначені для захисту браузера від відстеження. Вони доповнюють систему анонімізації в тих аспектах, які не забезпечуються засобами, перерахованими вище.

2.2. The Onion Router (TOR)

The Onion Router - найбільш значущий і популярний засіб для забезпечення анонімності в Інтернеті. Це вільне і відкрите ПЗ, що працює за принципом так званої цибулевої маршрутизації: усі дані, що потрапляють у мережу TOR, проходять через три вузли мережі, які обирають випадково, а перед надсиланням послідовно шифруються ключами обраних вузлів. Коли перший вузол отримує пакет, він розшифровує "верхній" шар шифру (звідси аналогія з чищенням цибулини) і дізнається, куди відправити пакет далі. Аналогічно чинять другий і третій сервер. Найбільш уразливим місцем у такому ланцюжку стають вихідні вузли (exit nodes), на яких трафік остаточно розшифровується і направляється до цільового ресурсу. На вихідних вузлах трафік може прослуховуватися, і про це слід пам'ятати в тих випадках, коли з'єднання з ресурсом відбувається за небезпечним протоколом - наприклад, відвідується сайт, який не підтримує HTTPS [28].

Фактично, TOR є мережею шифруючих проксі-серверів, або віртуальних тунелів, які підтримуються переважно добровольцями. На 2017 рік, ця мережа має близько 7000 вузлів, з яких 11% є вихідними вузлами [29]. Таким чином, кількість можливих маршрутів дуже велика, до того ж TOR забезпечує зміну маршруту кожні 10 хвилин. Вхідні вузли (entry nodes) забезпечують захист від перехоплення і підробки даних на шляху між вхідним вузлом і клієнтом. Крім того, існують мости (bridges) - ретранслятори, адреси яких не публікуються в загальному каталозі, а надаються за клієнтсь-

ким запитом [30]. Мости забезпечують доступ до мережі в тих випадках, коли інтернет-провайдер блокує відомі вхідні вузли TOR, а також виконують обфускацію (маскування) трафіку, що перешкоджає його ідентифікації та блокуванню системами DPI. Розроблено кілька типів мостів, наразі найефективнішим вважається obfs4.

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

Основний недолік Tor Browser - у тому, що факт його використання легко визначається з боку відвідуваного ресурсу. Перш за все, IP-адреси вихідних вузлів Tor відомі, і деякі сайти обмежують доступ із таких адрес, оскільки Tor нерідко використовується зловмисниками. Також Tor Browser має характерні цифрові відбитки (fingerprints). Механізми боротьби з відстеженням, які використовуються цим браузером, роблять усі екземпляри Tor Browser не відрізняти один від одного (або, принаймні, прагнуть до 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.

Категорично не рекомендується використовувати Tor для BitTorrent. Це не тільки є загрозою для анонімності, а й створює зайве навантаження на мережу Tor. Перелічимо й деякі інші речі, які не слід робити [31]. Не можна заходити через Tor в акаунти, пов'язані з реальною особою, і також не можна заходити без анонімізації в створені через Tor акаунти. Якщо обліковий запис хоча б раз використовувався з реального IP, він більше не є анонімним. Не слід забувати про соціальні методи деанонімізації: не можна розкривати ідентифікаційні дані під час анонімного спілкування або публікацій. Небажано використовувати одну й ту саму цифрову особистість занадто довго - що довше використовується один псевдонім, то більше накопичується профілюючої інформації про нього. Не рекомендується залишатися авторизованим у будь-якому акаунті довше, ніж необхідно. Не можна підключатися до ресурсу одночасно анонімно і неанонімно, оскільки це дає змогу виявити кореляції між двома з'єднаннями. До завантажуваних файлів, особливо виконуваних, потрібно ставитися з максимальною обережністю. Крім того, небажано встановлювати будь-які доповнення в Tor Browser і взагалі змінювати його стандартну конфігурацію.

Мережа Tor вважається відносно надійним засобом анонімізації, але випадки розкриття особи користувачів неодноразово мали місце. Насамперед зазначимо: деанонімізація далеко не завжди пов'язана з уразливістю самого Tor, часто використовуються методи соціальної інженерії, і сам користувач може робити помилки. Проте, "уразливості нульового дня" в Firefox (на якому заснований Tor Browser) успішно експлуатувалися ФБР вже як мінімум двічі [32]. Крім того, деякі методи відстеження браузера, так званий fingerprinting, виявлялися придатними для Tor Browser, хоча до теперішнього часу розробники значно посилили його захист [21]. Також мережа Tor періодично стикалася з проблемою шкідливих вузлів, які здійснювали перехоплення і навіть інфікування трафіку, і це відноситься не тільки до вихідних ретрансляторів - у 2016 році дослідники виявили 110 директорій прихованих сервісів (HSDir), які відстежували запити до onion-ресурсів та використовували для пошуку вразливостей даних ресурсів [33]. Шкідливі вузли в Tor продовжують час від часу виявляти і блокувати мережа.

Уразливість Tor до атак, що аналізують трафік, відома давно. Оригінальна проєктна документація вказує на вразливість системи перед "глобальним пасивним зловмисником", здатним прослуховувати весь трафік вхідних і вихідних вузлів. Зіставивши обидва потоки трафіку, такий зловмисник може деанонімізувати кожного користувача. У реальності це можливо в менших масштабах, оскільки жодна організація не здатна контролювати повністю всю мережу Tor, однак наявність навіть двох контрольованих вузлів (вхідного і вихідного) вже дає шанс ідентифікувати деяку, нехай і мізерно малу, частину користувачів, чий трафік пройде через обидва вузли [34]. Tor від самого початку не був спроєктований для протистояння масштабним атакам, коли зловмисник має безліч точок присутності всередині мережі. Тут доречно згадати мережу I2P, створену з урахуванням того, що кожен вузол може прослуховуватися.

Отже, наразі Tor залишається порівняно ефективним вільним інструментом для забезпечення анонімності та протидії відстеженню (у Tor Browser), продовжує активно розроблятися та отримувати нові механізми захисту. Однак його використання пов'язане з деякими незручностями і не є достатнім для надійної анонімізації. Доцільно розглядати Tor як основу для побудови складніших комбінацій.

2.3. Віртуальна приватна мережа

Технологія Virtual Private Network, призначена для захищеної передачі даних 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 свій 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.

Протоколи. Існує кілька найпоширеніших протоколів VPN:

- PPTP. Швидкий, легко настроюється, але порівняно небезпечний і застарілий. Point-to-Point Tunneling Protocol був винайдений Microsoft і довгий час був стандартним протоколом для VPN. Для забезпечення безпеки він спирається на різні методи аутентифікації. Хоча PPTP зазвичай використовується зі 128-бітовим шифруванням, 1999 року 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 до використання для VPN протоколи L2TP або SSTP [35].
- L2TP/IPsec. Протокол тунелювання рівня 2, на відміну від інших протоколів VPN, не шифрує і не захищає дані. Тому зазвичай використовуються додаткові протоколи, зокрема IPSec, за допомогою якого дані шифруються ще до передачі. Усі сучасні пристрої та системи, сумісні з VPN, мають вбудований протокол L2TP/IPSec. Встановлення та налаштування відбуваються легко і не займають багато часу, однак може виникнути проблема з використанням порту UDP 500, який блокується файрволами NAT. Так що, 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. Проте Едвард Сноуден зазначав, що і цей протокол не такий безпечний. Джон Гілмор, засновник і фахівець із безпеки Electric Frontier Roundation, заявляє, що Агентство національної безпеки США навмисно послаблює протокол. Ба більше, дворазове інкапсулювання даних робить протокол не настільки ефективним, як, наприклад, рішення на основі SSL, і тому він працює повільніше за інші протоколи.
- OpenVPN - порівняно нова технологія з відкритим кодом, яка використовує бібліотеку OpenSSL і протоколи SSLv3/TLSv1 разом із безліччю інших технологій для забезпечення надійного VPN-рішення. Однією з головних переваг є те, що OpenVPN дуже гнучкий у налаштуваннях. Цей протокол може бути налаштований на роботу на будь-якому порту, зокрема на 443 TCP-порті, що дає змогу маскувати трафік усередині OpenVPN під звичайний HTTPS, тому його важко заблокувати. Ще одна перевага - бібліотеки OpenSSL підтримують безліч криптографічних алгоритмів

(наприклад, AES, Blowfish, 3DES, CAST-128, Camelia та інші). Як правило, VPN-провайдери використовують тільки AES і Blowfish.

Швидкість OpenVPN залежить від рівня шифрування, але зазвичай вона вища, ніж у IPSec. І хоча OpenVPN зараз використовується більшістю VPN-провайдерів, він не підтримується за замовчуванням на будь-яких платформах. Однак відповідні сторонні додатки вже розроблено не тільки для ПК, але навіть для Android та iOS. Із цим пов'язана інша проблема OpenVPN - гнучкість може зробити його незручним у налаштуванні. Зокрема, під час при використанні типової програмної реалізації OpenVPN (наприклад, стандартний відкритий клієнт під Windows) необхідно не тільки завантажити та встановити клієнт, а й завантажити конфігураційні файли. Багато VPN-провайдерів вирішують цю проблему шляхом використання попередньо налаштованих VPN-клієнтів.

З урахуванням усіх факторів та інформації, наданої Е. Сноуденом, можна вважати, що протокол OpenVPN є найбезпечнішим на даний момент. Сноуденом, можна вважати, що протокол OpenVPN є найбезпечнішим на даний момент. Також передбачається, що він захищений від втручання Агентства національної безпеки США, оскільки використовує експериментальні методи шифрування. Звісно, ніхто не знає всіх можливостей АНБ, але найімовірніше, OpenVPN - єдиний по-справжньому безпечний протокол на сьогодні [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 і SEIL, він, як і раніше, використовується значною мірою тільки Windows-системами. SSTP використовує SSL v.3 і, отже, пропонує аналогічні переваги, що й OpenVPN (наприклад, можливість використовувати TCP-порт 443 для обходу NAT), а оскільки він інтегрований у Windows, він простіший у використанні та стабільніший, ніж OpenVPN. Однак SSTP не має відкритого вихідного коду, і всі права на нього належать Microsoft, тому OpenVPN використовувати переважно.
- IKEv2 (протокол обміну ключами, версія 2) розроблений Cisco і Microsoft, вбудований у Windows 7 і наступні версії. Протокол допускає модифікації

з відкритим вихідним кодом, зокрема для Linux та інших платформ, також підтримуються пристрої Blackberry. Він добре підходить для встановлення автоматичного VPN-підключення, якщо інтернет-з'єднання періодично розривається. Користувачі мобільних пристроїв можуть скористатися ним як протоколом для бездротових мереж за замовчуванням, він дуже гнучкий і дозволяє легко перемикати мережі. Хоча IKEv2 доступний на меншій кількості платформ порівняно з, наприклад, IPSec, він вважається досить хорошим протоколом з точки зору стабільності, безпеки та швидкості роботи. Недолік - закритий вихідний код.

- SoftEther VPN - мультипротокольний VPN-сервер під ліцензією GPLv2, розробляється з 2013 року, має широкий спектр можливостей. Має власний протокол SSL-VPN, який не відрізняється від звичайного HTTPS-трафіку. Заявлена підтримка L2TP/IPsec, MS-SSTP, OpenVPN, L2TPv3 і EtherIP, причому для L2TP вказана сувора сумісність із вбудованими клієнтами в iOS і Android. Сам сервер має версії під Windows, Linux, OS X, FreeBSD і Solaris. Працює швидше, ніж OpenVPN, не вимагає наявності TUN/TAP, має вбудований NAT і DHCP. Протокол SSL-VPN може працювати через TCP, причому підтримуються множинні TCP-сесії, UDP і навіть ICMP [36].

Проблеми вибору VPN-провайдера. Отже, під час вибору протоколу слід зупинитися на OpenVPN, а якщо йдеться про налаштування власного VPN-сервера, є сенс використовувати SoftEther VPN. Деякі з безкоштовних публічних серверів VPN Gate також надають доступ за протоколом SoftEther (SSL-VPN). Зауважимо, що багато VPN-провайдерів пропонують власні клієнтські програми для підключення - це може бути зручно, але потенційно небезпечно. Протокол OpenVPN має на увазі використання відкритого клієнта і конфігураційного файлу, який і повинен бути наданий провайдером. З іншого боку, застосунок провайдера може мати корисні функції: так званий kill switch (запобігання витоку трафіку в обхід VPN у разі обриву з'єднання), захист від витоків DNS. Утім, надійність їхньої роботи необхідно ретельно протестувати.

До питання вибору VPN-провайдера слід підходити дуже уважно і відповідально. Безкоштовні VPN часто викликають недовіру, оскільки незрозуміло, хто і з якою метою спонсорує сервіс - можливо, всю діяльність користувачів відстежують.

Показовий приклад: 2017 року правозахисна група Center for Democracy and Technology (Центр демократії та технології) і технологій, CDT) викрила популярний сервіс Hotspot Shield у порушенні власної політики конфіденційності. Дослідники виявили, що Hotspot Shield відстежує поведінку користувачів в інтернеті, перенаправляє інтернет-трафік, продає дані своїх користувачів третім сторонам, а також розкриває конфіденційні дані, зокрема назви бездротових мереж, MAC-адреси та ідентифікатори IMEI пристроїв. Крім того, додаток впроваджував код Javascript для рекламних цілей. Як показав реверс-інжиніринг вихідного коду застосунку, Hotspot Shield використовував понад п'ять різних сторонніх бібліотек для відстеження користувачів.

У деяких випадках сервіс перенаправляв трафік на сайти партнерів, зокрема рекламних компаній, для отримання прибутку.

Великі платні VPN-сервіси, як правило, серйозніше ставляться до збереження конфіденційності. Однак не слід довіряти заявам про відсутність ведення логів, найчастіше логгування активності проводиться, але багато що залежить від обсягу зібраних даних, часу їхнього зберігання і можливості надання їх за запитом уповноважених організацій. Корисно поставити технічній підтримці сервісу запитання, чи можливе блокування облікового запису в разі шкідливої активності користувача. Якщо відповідь зводиться до того, що доступ буде блоковано тільки в разі надходження скарг (abuses), то активність справді не відстежується. Також велике значення має можливість анонімної оплати сервісу. Розкриття платіжних даних користувача VPN-провайдеру явно суперечить збереженню анонімності. Якщо сервіс позиціонується як такий, що забезпечує анонімність, він зобов'язаний приймати криптовалюту. Зауважимо, що зазвичай приймається тільки Bitcoin, однак він не забезпечує надійної анонімності, якщо не використовувати міксери. Кращими були б такі криптовалюти, як Monero або Dash, більш орієнтовані на анонімізацію транзакцій, але практично немає VPN-сервісів, які б приймали їх до оплати.

Слід обирати іноземного VPN-провайдера в юрисдикції тієї країни, яка не підтримує дипломатичні відносини з країною користувача, або країни з ліберальним законодавством, де отримання логів сервера буває важко навіть для місцевої поліції. Це

саме стосується використання двох VPN (не DoubleVPN, а різних провайдерів) - бажано вибрати сервери в країнах, які не співпрацюють один з одним [37]. Крім того, слід уникати країн "альянсу Five Eyes" - основних учасників угоди UKUS SIGINT. Взагалі вибір надійного VPN-провайдера є складним завданням навіть для досвідченого користувача. У 2016 році було запущено сайт thatoneprivacysite.net, де наведено детальне порівняння понад ста VPN-сервісів за багатьма параметрами. Таблиця не дає однозначної відповіді "який із VPN найкращий", але лідерами можна назвати Proxy.sh, розташований на Сейшелах, шведські oVPN.se і IPredator, гібралтарський IVPN і ісландський CryptoStorm. Хорошу репутацію також мають Private Internet Access, NordVPN, Mullvad, AirVPN. Також є невелика кількість провайдерів, які розміщують свою рекламу на ресурсах "тіньової" спрямованості, по суті відкрито пропонують свої послуги потенційним зловмисникам. Ставлення до таких провайдерів зазвичай суперечливе. Теоретично, така поведінка має означати, що цей провайдер принципово не співпрацює з правоохоронними органами і забезпечить будь-якому користувачеві надійну анонімність. Реальна ж ситуація може бути прямо протилежною. За відсутності вагомих причин для довіри до такого VPN, краще утриматися від його використання.

Що стосується різних DoubleVPN, TripleVPN, QuadVPN, то більшою мірою це маркетинговий хід, ніж підвищення захищеності, оскільки всі сервери ланцюжка належать одному VPN-провайдеру, і їхня кількість не перешкоджає веденню журналу активності користувача і можливості розкриття цих даних провайдером. Проте заміна звичайного VPN на DoubleVPN знижує ймовірність деанонімізації. Слід враховувати, що це не двошарове шифрування - на відміну від Tor, тут трафік на проміжному сервері розшифровується. Але можливий і Parallel VPN - спосіб підключення через два паралельні VPN-канали, за якого трафік шифрується двічі (канал у каналі). Це дещо знижує швидкість, але вирішує проблему незахищеності трафіку на проміжному вузлі.

Підсумок: VPN не слід розглядати як надійний засіб забезпечення анонімності, але при правильному виборі провайдера і коректному налаштуванні може бути досягнуто високого рівня конфіденційності.

2.4. Використання віртуального приватного серверу VPS

Віртуальний приватний сервер, стосовно анонімізації, використовується для налаштування власного VPN, SSH або проксі-сервера, а іноді й вузла Tor, якщо це дозволяє VPS-хостер. Вартість оренди VPS може виявитися нижчою, ніж купівля VPN. При цьому адміністративний доступ до сервера дає змогу повністю відключити ведення логів і загалом налаштувати VPN-сервер під власні потреби за наявності відповідних навичок. Недоліком такого рішення вважається те, що користувач на сервері всього один, і його значно легше відстежити, ніж під час використання великих платних і безкоштовних VPN. З іншого боку, віртуальних серверів на фізичному сервері кілька, тому для зовнішнього спостерігача, як і раніше, складно буде зіставити вихідні підключення з цього сервера з конкретним користувачем. Під час вибору провайдера керуватися можна тими ж міркуваннями, що і для VPN. Як мінімум, сервер не повинен потрапляти під юрисдикцію спецслужб тієї країни, де перебуває користувач, або країн, що перебувають із нею у співпраці.

Провайдерів VPS існує дуже багато, і значна частина зарубіжних компаній приймає до оплати Bitcoin. Однак, якщо передбачається збереження анонімності під час реєстрації, проблеми можуть виникнути вже на цьому етапі. Багато VPS-хостерів не дозволяють анонімну реєстрацію. У разі присутності антифрод-системи слід врахувати кілька базових чинників: IP-адреса не повинна бути адресою Tor або загальнодоступного проксі-сервера; особисті дані мають бути правдоподібними, не потрібно вводити випадкові комбінації символів замість П. І. Б.; адреса також правдоподібна, країна має відповідати IP-адресі; телефон - той, що належить зазначеній країні [38]. Взагалі, під час будь-якої анонімної реєстрації, коли потрібно вказати персональні дані, бажано створювати максимально правдоподібну особистість-псевдонім, а не привертати увагу введенням безглуздих даних. І, звісно, якщо надалі планується підключатися до VPS з реальної IP-адреси, то анонімна купівля не має сенсу.

Під час вибору сервера потрібно звернути увагу на ліміт трафіку і пропускну здатність. Ємність жорсткого диска практично не важлива, але оперативної пам'яті

рекомендується не менше 512 мегабайт. Для розгортання VPN-сервера необхідна підтримка TUN/TAP (не потрібна для SoftEther). Залежно від конкретного хостера і типу віртуалізації може знадобитися запит до техпідтримки, щоб увімкнути TUN-адаптер. Доступ до сервера надається зазвичай по SSH. Його слід налаштувати на авторизацію за сертифікатом, щоб убезпечити сервер від злому пароля SSH. Потім, імовірно, знадобиться налаштування правил файрволу, і потім уже проводять установку і конфігурацію основного ПЗ. Власний сервер дає змогу налаштувати VPN так, щоб його використання не можна було визначити за MTU або характерними портами. Крім того, існує можливість захистити сервіси від виявлення зловмисниками, використовуючи так званий port knocking. Це неявна форма дозволу доступу до якогось сервісу, за умови проходження попередньо заданої послідовності з'єднань із різними портами цільового сервера. Спеціальне ПЗ на стороні сервера відстежує всі вхідні з'єднання, і, якщо фіксується характерна "ланцюжок підключень" відповідних раніше заданому "еталонному стуку" - тимчасово відкриває доступ до закритого порту і, відповідно, прихованого сервісу на ньому [39].

2.5. Операційні системи для анонімної роботи

Існує низка дистрибутивів Linux, спеціально націлених на забезпечення анонімності та безпеки. Як правило, такі збірки засновані на Debian, використовують мережу Tor і різні додаткові засоби захисту.

Якщо не розглядати системи, розробку яких було припинено, то наразі виокремлюють такі проєкти:

- Whonix
- Tails
- Kodachi
- MOFO Linux
- Subgraph OS
- heads

Розглянемо докладніше два перші пункти цього списку.

Whonix. ОС Whonix - система для анонімної роботи, заснована на Debian, що складається з двох віртуальних машин, одна з яких є шлюзом, що відправляє весь трафік у мережу Tor, а інша - ізольованою робочою станцією, яка під'єднується лише до шлюзу. Існує також варіант фізичного поділу шлюзу і робочої станції. Whonix реалізує в собі механізм так званого ізолюючого проксі-сервера. Робоча станція не отримує зовнішньої IP-адреси в Інтернеті, і це дає змогу нейтралізувати безліч уразливостей, наприклад, навіть якщо шкідливе ПЗ 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 витоки. Навіть такі додатки, 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 застосунків іде через мережу Tor;
- для захисту від профілювання трафіку Whonix реалізує концепцію ізоляції потоків. Попередньо встановлені в Whonix застосунки налаштовані на використання окремого Socks-порту, а оскільки кожен Socks-порт використовує окремий ланцюжок вузлів у мережі Tor, то профілювання неможливе;
- 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-витоків, 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 за цифровим відбитком браузера або системи шляхом використання найзагальніших значень, наприклад, ім'я користувача - user, часова зона - UTC тощо;

- є можливість тунелювати інші анонімні мережі: Freenet, I2P, JAP, Retroshare через Tor, або працювати з кожною такою мережею безпосередньо;
- важливо зазначити, що в Whonix протестовані, документовані й успішно працюють усі схеми комбінування VPN/SSH/Proxy з Tor [41];
- Whonix - повністю відкритий проєкт, що використовує вільне ПЗ.

Встановлення Whonix можливе кількома способами. Запуск віртуальних машин у VirtualBox - найпростіший спосіб. Надійнішим вважається використання Qubes-Whonix, коли в якості хостової операційної системи використовується Qubes OS, а Whonix-Gateway встановлюється через вбудовані засоби віртуалізації. Система Qubes OS використовує гіпервізор Xen для реалізації підходу "безпека через ізоляцію". Також існує можливість запуску Whonix з віртуалізацією KVM за допомогою qemu-kvm, і останній варіант - фізична ізоляція, встановлення двох компонентів Whonix на дві фізичні машини. При цьому рекомендується встановлювати шлюз (Gateway) безпосередньо на "залізо" ПК, а робочу станцію (Workstation) - у віртуальну машину. Зазначимо, що розробники після проведених досліджень визнали Qubes-Whonix безпечнішою, ніж фізичну ізоляцію [42]. Утім, у Xen також можливі вразливості. Ще одна особливість Whonix - можливість підключення через Gateway практично будь-якої віртуальної машини замість Whonix-Workstation.

Наразі встановлення Whonix під Windows максимально спростилося з огляду на появу автоматичного інсталятора, який самостійно завантажує та імпортує у VirtualBox образи віртуальних машин, а потім дає змогу запустити їх натисканням однієї кнопки. Тестування виявило проблему: інсталятор встановлює окремий примірник VirtualBox, навіть якщо VirtualBox вже був присутній у системі. У результаті виникає конфлікт, і обидва екземпляри виявляються непрацездатними. У такій ситуації слід деінсталювати оригінальний VirtualBox, а потім перевстановити його в каталог, який був створений установником Whonix.

TAILS. The Amnesic Incognito Live System здобула популярність як "система, яку використовував Едвард Сноуден" і "найбільш анонімна ОС". Насправді складно

сказати, що Tails краща (або гірша) за Whonix, оскільки їхні концепції суттєво різняться. Tails є Live-дистрибутивом для завантаження з Flash-накопичувача і не залишає слідів на комп'ютері, де використовувалася. 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 в захищеному режимі (AppArmor). Водночас Tails має "Небезпечний браузер" (звичайний Firefox), що дає змогу відвідувати сайти безпосередньо, без Tor. Загалом Tails може здатися менш безпечною, ніж Whonix, оскільки має доступ до фізичної системи, MAC-адреси, реального IP, тоді як Whonix-Workstation ізольований у віртуальній машині. З іншого боку, у випадку Whonix можливі вразливості як у двох її компонентах, так і в VirtualBox і в операційній системі хоста. У принципі запуск Tails у віртуальній машині також можливий, але потрібно використовувати пакет virt-manager у Debian.

Крім Tor Browser, у Tails встановлено набір ПЗ, зокрема:

- Pidgin - Jabber+OTR.
- Electrum - легкий клієнт для Bitcoin.
- KeePassX - менеджер (зберігач) паролів.
- GPG - система асиметричного шифрування.
- MAT - видалення метаданих з різних типів файлів.
- Програми для редагування документів, фото, аудіо, відео тощо.
- Thunderbird - поштовий клієнт.
- Легко поставити Psi або Psi+ (Jabber з підтримкою GPG).

Процедура встановлення Tails з-під Windows дещо своєрідна, для неї потрібні два Flash-накопичувачі. Спочатку інсталяційний образ Tails записується на перший носій (об'ємом 2 Гб) - це "проміжна" Tails, обмежено придатна для роботи (під час встановлення з Linux процедура простіша, і проміжний носій не потрібен). Потім слід завантажити ПК із цього носія. Нерідко на цьому етапі виникає проблема, BIOS не може коректно завантажити образ. У такому разі рекомендується перезаписати Tails на носій, використовуючи програму Rufus замість рекомендованого Universal USB Installer. Зазвичай після цього завантаження проходить успішно. Далі підключається другий накопичувач, і на нього виконується

встановлення "основної" Tails. Для цього слід вибрати в меню Додатки → Tails → Tails Installer → Install by cloning. Після успішного завершення встановлення другий носій готовий до роботи, а перший більше не потрібен. Можна завершити роботу системи.

Здійснюємо завантаження з другого накопичувача. Тепер, щоб мати можливість зберігати будь-які дані в системі, слід створити постійний розділ - криптоконтейнер LUKS. Вибираємо в меню Application → Tails → Configure Persistence і задаємо пароль, бажано криптостійкий. Є можливість вибрати, які дані будуть зберігатися. Усе, що не збережено в постійному розділі, очищається після перезавантаження Tails. Зазначимо, що у Tor Browser є можливість читання і запису тільки в 2 папки, вони є в закладках провідника: Tor Browser і Tor Browser (Persistent). Завантаження і вивантаження файлів можливі тільки в/з них. За наявності дійсно важливих даних слід періодично робити їхню резервну копію на інший носій, оскільки шанс раптового виходу з ладу Flash-накопичувача набагато вищий, ніж жорсткого диска.

Використання VPN у Tails не рекомендовано розробниками, тому така можливість за замовчуванням відсутня, і налаштування VPN вимагає втручання в правила iptables. Вважається, що ланцюжок "VPN через Tor" шкодить анонімності, про це сказано в офіційній документації Tor. Річ у тім, що важливою перевагою Tor є часта зміна маршрутів трафіку, а під час підключення до VPN-сервера через Tor фактично створюється постійний маршрут, фіксоване місце призначення. Проте реалізувати такий ланцюжок дає змогу Whonix. Для Tails можлива схема "Tor через VPN", якщо використовувати роутер із прошивкою dd-wrt і під'єднатися до VPN із роутера.

За необхідності більш надійного приховування шифрованих даних доцільно використовувати TrueCrypt (або VeraCrypt). Наразі творці Tails рекомендують використовувати cryptsetup, заснований на LUKS. Ця програма дає змогу створювати приховані розділи, однак такий розділ прихований не до кінця. Існує можливість виявити заголовок прихованого розділу, що дає змогу встановити його наявність. Заголовок же прихованого розділу TrueCrypt неможливо відрізнити від випадкових даних, і, наскільки відомо, виявити його неможливо (переконливе заперечення) [44].

Під час запуску Tails синхронізує системний годинник. Якщо при цьому виявляється істотна розбіжність часу, Tor Browser припиняє роботу і перезапускається. З погляду зовнішнього спостерігача, така поведінка може бути використана для виявлення користувачів Tails, головним чином тому, що синхронізація відбувається під час кожного запуску системи.

Порівняння Whonix і Tails. Обидві системи засновані на Debian і використовують Tor Browser. Загалом, Whonix більше призначена для встановлення на регулярно використовуваний ПК, у тоді як Tails - скоріше "похідний" інструмент, що дає змогу анонімно вийти в Інтернет із чужого ПК. Нижче представлено деякі з відмінностей.

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 у разі помилок системного ПЗ або зараженні вірусом
Захист від атаки "холодного завантаження"	Ні	Так
Підтримка VPN	Так, документовано	Не передбачено
Приховування MAC-адреси хоста в локальній мережі	Ні	Так
Може слугувати шлюзом у мережу Tor для будь-якої ОС	Так	Ні
Можливість відвідувати сайти напряму, без Tor	Ні, але можна через браузер основної ОС	Через окремий браузер (Firefox)

2.6. Специфіка анонімної поведінки

Анонімна робота в Інтернеті рідко обмежується переглядом веб-сторінок, вона може включати в себе реєстрацію на будь-яких сайтах, публікацію текстів, спілкування на форумах, зв'язок електронною поштою або в Jabber тощо без втрати анонімності. У таких ситуаціях технічна анонімність стає недостатньою, виникає необхідність не допустити витоку інформації від самого себе. Далеко не всім користувачам можуть знадобитися подібні заходи безпеки. Насамперед при створенні альтернативної особистості слід пам'ятати, що вона не повинна перетинатися з реальною навіть побічно.

- Оцінити ступінь довіри до ресурсу, на якому реєструється профіль.
- За можливості використовувати тимчасову e-mail адресу (Dropmail, 10MinuteMail) або постійну, але спеціально створену в анонімному сеансі.
- Не розкривати дату народження або вказати неправильні дані.
- У випадках, коли необхідно вказати ім'я та прізвище, не слід робити їх надмірно екзотичними або абсурдними, щоб не привертати додаткової уваги.
- Іноді доцільно вказати реальне місто проживання, щоб надати профілю більше правдоподібності. Інакше в процесі спілкування може бути помічено, що анонім практично не знає міста, в якому нібито проживає. Якщо ж немає необхідності вказувати місто, то й робити це не потрібно. За можливості - взагалі не розкривати географічні дані, включно з часовим поясом.
- "Мульти-нік": слід використовувати різні нікнейми в різних місцях, якщо немає явного бажання ідентифікувати себе як одну й ту саму особистість.
- "Крос-постинг": повна заборона на однакові тексти та посилання на них з-під різних профілів [45].
- Стиль мови може свідчити про рівень освіти, проф.приналежність тощо.
- Характерні мовні звороти, "коронні фрази", повторювані помилки в мовленні. Може вказати на зв'язок двох профілів або навіть на реальну особистість.
- Під час реєстрації в анонімних мережах - не використовувати свої нікнейми з "звичайного" Інтернету.

- Обов'язково видаляти метадані з файлів, що надсилаються, наприклад, EXIF з фотографій, ім'я користувача з документів. До отриманих файлів від невідомих осіб слід ставитися з особливою обережністю [27]. Наприклад, картинки, отримані з неперевіреного джерела, можуть містити стеганографічну мітку. Якщо планується де-небудь публікувати їх з іншого профілю, є сенс перекодувати їх із втратами.
- Час публікації повідомлень може локалізувати основне проведення часу.
- В анонімному сеансі роботи не можна відвідувати акаунти, пов'язані з реальною особистістю, особливо в соцмережах. Навіть якщо профіль не містить справжніх даних, але був створений під час неанонімного підключення, він уже небезпечний. І навпаки, при звичайній роботі без анонімізації - не входити в анонімний акаунт.
- У деяких випадках, особливо на маловідвідуваних ресурсах, спільність кількох анонімних підключень стає помітною з простого логічного міркування: якщо за короткий проміжок часу зайшли кілька невідомих користувачів із рідкісним відбитком браузера - найімовірніше, користувач один [16].
- Під час копіювання тексту з веб-сайту варто перевірити його на наявність прихованих (недрукованих) символів [46].

ВИСНОВОК ДО РОЗДІЛУ 2

Існує значна кількість програмного забезпечення, орієнтованого на забезпечення анонімності та приватності. Сучасні засоби дають змогу досягти високого рівня безпеки, проте вона завжди залежна від людського фактора. Найпотужнішим інструментом приховування особистості є Tor та анонімні операційні системи на його основі. VPN-сервіси менш безпечні, але більш зручні у використанні. Підключення до VPN через Tor має як переваги, так і недоліки.

РОЗДІЛ 3
ПРОЄКТУВАННЯ ПРОГРАМНОГО КОМПЛЕКТУ

3.1. Вихідні дані та постановка задачі

Оскільки мається на увазі, що підсумковий набір ПЗ призначений для широкого кола користувачів (потреба в анонімності може виникнути в будь-кого, а не тільки в "просунутих"), припускатимемо, що початкова система не анонімна: інтернет-провайдеру відома особистість користувача, ПК який використовується для повсякденної роботи і, найімовірніше, під ОС Windows. Припускається, що рішення не буде повністю безкоштовним, оскільки буде задіяно надійний VPN-сервіс або попередньо налаштований VPS.

Сформулюємо вимоги до реалізації:

- Приховати від відвідуваних сайтів усі дані, пов'язані з вихідною системою і браузером, використовуваним для не-анонімної активності;
- Забезпечити шифрування трафіку, що проходить через обладнання (DPI-системи, СОРМ-3 тощо) інтернет-провайдера;
- Забезпечити можливість багаторазової зміни цифрових відбитків;
- Виключити можливість витоку реального IP в анонімному браузері;
- Сайт не повинен виявляти, що засоби анонімізації використовуються;
- Системи аналізу трафіку не повинні розпізнавати наявність VPN або Tor;
- Рішення має бути придатним для надання користувачеві в уже готовому вигляді, з нескладною процедурою встановлення і швидким налаштуванням.

Очевидно, що в реальності користувач може відмовитися від готового рішення, оскільки не має підстав довіряти розробнику. Крім того, повністю приховати всі дані про реальну особистість зазвичай неможливо через людський фактор. Природно, що користувач із України відвідуватиме переважно україномовні сайти, перемикатиметься на українську мову відображення сторінок, писатиме коментарі та, врешті-

решт, спілкуватиметься рідною мовою. Але слід взяти до уваги, що такі сайти становитимуть лише меншу частину від усього обсягу відвідуваних ресурсів.

Не всі названі вимоги є обов'язковими. Наприклад, якщо інтернет-провайдер не блокує трафік Tor або OpenVPN, то немає і прямої необхідності маскувати його, але користувач може вважати за краще робити це "про всяк випадок". Також далеко не всі сайти будь-яким чином перевіряють наявність засобів анонімізації і тим більше оцінюють правдоподібність відбитків. У рішенні, яке буде описуватися далі, робиться спроба реалізувати всі вищевказані вимоги.

3.2. Вибір ПЗ і необхідної конфігурації

Веб-браузер. З огляду на поставлену мету - максимально приховати факт анонімізації - використання Tor Browser виявляється небажаним, оскільки його легко виявляють і він потенційно привертає увагу. Передбачається, що буде реалізовано ланцюжок "VPN через Tor", за якого на виході є IP-адреса VPN-сервера, що не викликає підозр, на відміну від адрес Tor. Домогтися цього в Tor Browser складно - він направляє трафік виключно в Tor і не приймає альтернативних налаштувань проксі-сервера. Водночас, як згадувалося вище, Tor Browser має характерні цифрові відбитки. Отже, у нашому випадку необхідно використовувати звичайний Firefox, але для цього буде потрібно значно змінити його 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 більша гнучкість налаштувань браузера.

У додатку 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, так чи інакше придатних для посилення захисту. Основна мета такого налаштування - запобігання витоку різних другорядних даних, з урахуванням того, що всі основні функції браузера повинні працювати як зазвичай. Наприклад, вимкнення різних опцій телеметрії - не більше ніж спосіб підвищити конфіденційність, однак вимкнення WebRTC - характерний ознака боротьби з

витоком реального IP під час використання деяких засобів анонімізації, а таких 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, адже будь-які збережені ідентифікатори буде видалено після закриття вікна браузера незалежно від способу їхнього зберігання. Теоретично, можна вимкнути використання кешу і локального сховища, однак на практиці це може викликати деякі проблеми. На вкладці "Приватність" рекомендується заборонити прийом cookies зі сторонніх сайтів. У додаткових налаштуваннях - повністю вимкнути надсилання телеметрії.

В даний час Firefox містить деякі опції протидії "фінгерпринтингу", запозичені з Tor Browser. Відповідний режим активується опцією privacy.resistfingerprinting. Однак, цей режим ми використовувати не будемо, 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 має відповідати геолокації використовуваної IP-адреси. У якості User Agent я обираю Chrome щоб ще більше замаскувати використання Firefox в повсякденному житті.

Крім зміни налаштувань Firefox, потрібно буде використовувати деякі браузерні доповнення для підміни відбитків і блокування відстеження.

- CanvasBlocker - підміняє відбиток Canvas fingerprint. Має опцію повного блокування запиту canvas readout і різні режими підміни, а також підтримує білий і чорний списки. Відбиток генерується випадковим чином під час кожного оновлення сторінки, що унеможливлює відстеження користувача за цим відбитком.
- NoScript - розширення, що дає змогу блокувати виконання JavaScript, Java, Flash та інших потенційно небезпечних компонентів HTML-сторінок. Також надає захист від XSS-атак.
- uBlock Origin - розширення для фільтрації контенту. Дає змогу блокувати не тільки рекламу, а й різні відстежувальні елементи (списки фільтрів у категорії "Приватність" слід активувати). У деяких випадках захищає навіть від фінгерпринти-

нгу: наприклад, якщо сайт використовує стандартний скрипт fingerprint2.js, завантаження скрипта буде заблоковано, оскільки він входить до списку фільтрації. Має опцію запобігання витоку локального IP через WebRTC. Також послужить заміною Safe Browsing завдяки спискам шкідливих доменів.

- Decentraleyes - захищає від відстеження з боку великих CDN (мереж доставки контенту) шляхом надання локальних ресурсів і блокування мережевих запитів до CDN. Може розглядатися як доповнення 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, дає змогу надсилати 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 додатків, але має і деякі унікальні опції: запобігання маніпуляціям з буфером обміну, додавання випадкових малих затримок між натисканнями клавіш.
- User-agent Switcher - підміна User-agent, зокрема через JavaScript.

Слід також згадати доповнення RAS (Random Agent Spoofer), корисне для більш ранніх версій Firefox. Це інструмент для підміни профілю браузера (User-agent і низка супутніх параметрів) із широким списком можливостей (утім, багато його налаштувань просто керують штатними параметрами конфігурації Firefox). Для деяких функцій використовує впровадження скрипта (script injection), підтримує анонімізацію параметра window.name, підміну роздільної здатності екрана, часового поясу (у протес-

тованій версії опція Time Zone Spoofing була відсутня з незрозумілої причини). Розробку цього розширення припинено через труднощі міграції на новий стандарт розширень Firefox WebExtension.

Завершуючи розгляд браузера Firefox, відзначимо нещодавню ініціативу щодо інтеграції Tor у Firefox і, надалі, повного злиття Tor Browser і Firefox у єдиний браузер (проєкт Fusion), який зможе працювати в різних режимах. Це стане логічним продовженням поточного проєкту Tor Uplift. Планується і подальше посилення функцій боротьби з "фінгерпринтингом" браузера, а також підвищення зручності їх використання.

Архітектура системи. Для надійного захисту від можливих витоків і для ізоляції браузера від основної системи було вирішено використовувати віртуальну машину. Оскільки концепція Whonix - дві ВМ, одна з яких слугує інтернет-шлюзом, з'єднані внутрішньою мережею - працює дуже ефективно, її і буде застосовано в цьому випадку. Whonix дає змогу під'єднувати до свого шлюзу не тільки оригінальну Whonix-Workstation, а й будь-яку іншу ВМ. Незважаючи на те, що для анонімної роботи традиційно використовують Linux, вибір зроблено на користь Windows - така машина матиме набагато більш "звичайний" вигляд, оскільки переважна більшість ПК працює під Windows. Спроби маскувати Linux-версію браузера під Windows-версію потенційно ненадійні і тому небажані. Зазначимо, що сучасна Windows 11 містить велику кількість функцій, спрямованих на збір і відсилання даних про користувача і явно невідповідних для анонімної роботи. Навіть застосовуючи всі можливі рекомендації та програми для вимкнення "збору телеметрії", неможливо гарантувати надійне забезпечення приватності. Тому буде встановлено Windows 7, з якої також потрібно видалити кілька оновлень із функціоналом надсилання телеметрії. На сьогодні ця система все ще широко використовується, і її наявність не виглядатиме підозріло.

Шлюз Whonix-Gateway забезпечить анонімізацію трафіку засобами мережі Tor, але необхідно приховати факт використання Tor як від відвідуваних 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 дає змогу налаштувати VPN для максимальної захищеності (відсутність ведення логів, застосування надійних криптографічних алгоритмів, різноманітні заходи для приховування факту використання VPN), однак має дуже суттєвий недолік - сервер тільки 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 VPN-провайдери налаштовують свої сервери так, щоб сайти не могли розпізнати наявність VPN. У практичній частині цієї роботи буде продемонстровано приклад запуску власного VPN-сервера і наведено його конфігурацію.

Під час налаштування VPN-сервера передбачено таке: використовується протокол TCP і порт 443 (інший варіант - нестандартний порт, нехарактерний для VPN і проксі-серверів). Усі DNS-запити спрямовуються через VPN. Адреси DNS взяті зі списку OpenNIC і відносяться до тієї ж 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 в поєднанні з HMAC-аутентифікацією (tls-crypt) в OpenVPN.

Для маскування трафіку Tor (і на випадок можливого блокування доступу до мережі Tor інтернет-провайдером) буде задіяно obfs4 - так званий obfs4. "транспорт, що підключається", додатковий компонент Tor, спеціально призначений для протидії аналізу трафіку DPI-системами. Крім того, доцільно виключити з використання вузли Tor, що знаходяться в країні перебування користувача, у нашому випадку це українські вузли. Ця можливість вбудована в 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.

На основній віртуальній машині, крім браузера і VPN-клієнта, за бажанням користувача може бути встановлено додаткове ПЗ. Наприклад, GPG4Win для шифрування тексту і файлів, Exif Purge для видалення даних EXIF з фотографій, Tox або Jabber-клієнт для безпечного обміну повідомленнями (звісно, якщо співрозмовник

згоден користуватися тим самим додатком). Питання про встановлення антивіруса є дискусійним. З одного боку, комерційний продукт - наприклад, ESET Internet Security - забезпечив був набагато кращий захист від різних загроз, ніж фільтр uBlock зі списком Malware Domains. Однак це вимагає купівлі ліцензії, і тоді антивірус надсилатиме через анонімний канал ідентифікаційні дані. У реальності, найімовірніше, користувач буде періодично шукати пробні ключі в Інтернеті або вибере безкоштовний антивірус. З іншого боку, архітектура системи така, що робоча віртуальна машина в принципі не має доступу до реального IP і файлової системи фізичної машини. Крім того, наявність заздалегідь зробленого знімка стану ВМ (snapshot) дасть змогу скинути її до незараженого стану. Єдиною, хоча й малоймовірною загрозою залишається зараження вірусом, що експлуатує якусь уразливість у VirtualBox, яка дозволила б вірусу "вийти" за межі ВМ.

Підсумкові можливості підміни даних. Цифрові відбитки Firefox підміняються за допомогою вищезазначених браузерних доповнень, деяких можливостей самого Firefox, а також зміною параметрів віртуальної машини. Окремі параметри можна підмінити і за допомогою JavaScript, підключаючи користувацькі скрипти 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 підміняємо тільки версію браузера. Мова браузера - англійська за замовчуванням, допускається встановити українську локалізацію інтерфейсу, але водночас 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 має відповідати геолокації використовуваного VPN-сервера (враховуючи також літній/зимовий час).

"Відбиток шрифтів" має два різновиди:

- відтворення кількох символів Юнікоду в різних накресленнях і вимірювання розмірів отриманих символів;
- виявлення встановлених шрифтів за допомогою механізму CSS Fallback, причому безпосередньо отримати весь список шрифтів не можна, але можна перевіряти наявність кожного конкретного шрифту із заздалегідь підготовленої бази.

У першому випадку відбиток можна спотворити звичайною зміною масштабу сторінки (це саме стосується і відбитка getClientRects), але очевидно, що це не вдасться робити багаторазово. З іншого боку, цінність цього відбитка порівняно невисока. Для боротьби з другим методом Firefox має вбудовану функцію "білого списку" шрифтів, а також режим блокування всіх шрифтів, що задаються веб-сторінкою (замість них використовується невеликий набір стандартних шрифтів браузера). Зазначимо, що в разі встановлення і запуску плагіна Flash сайт зможе отримати доступ до всього списку шрифтів, встановлених у системі.

Доповнення CanvasBlocker підміняє відбиток Canvas і частково WebGL. Браузер Firefox дає змогу перевизначити значення рядків Renderer і Vendor для API WebGL, однак загалом відбиток WebGL залишається найскладнішим. Правдоподібна підміна всіх параметрів для WebGL 2 може бути реалізована тільки за повноцінної емуляції відеокарти у віртуальній машині. Наразі відомий один експериментальний проєкт із такою можливістю - модифікований VirtualBox від Д. Момота (Vektor T13), але його сумісність із Whonix поки ще погано перевірена, і складно гарантувати стабільність, а також є проблеми з цифровими підписами драйверів. У звичайному VirtualBox функціональність WebGL залежатиме від того, чи ввімкнено 3D-прискорення графіки у віртуальній машині та чи встановлені "доповнення гостьової ОС". І нарешті, підміна відбитка AudioContext виконується за допомогою AudioContext Fingerprint Defender, також можна перемикати частоту дискретизації в налаштуваннях динаміків.

Підсумкова схема реалізації має вигляд, представлений на рисунку 3.1:

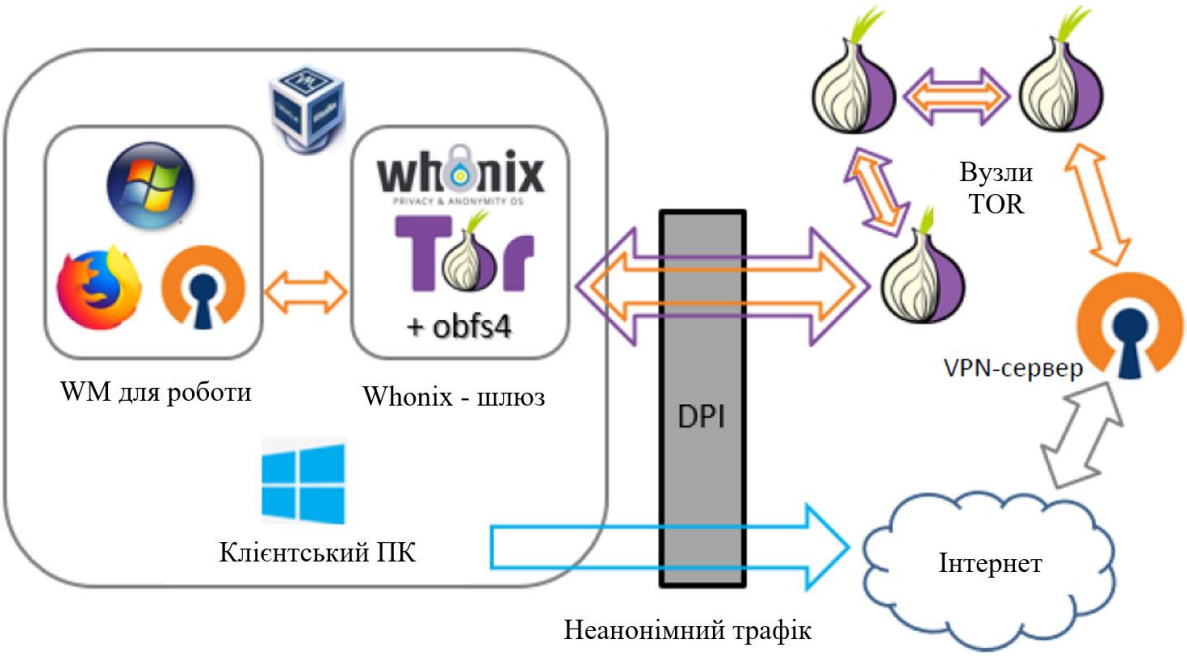

Рис 3.1. Компоненти системи

Під позначенням DPI тут мається на увазі будь-яке обладнання аналізу та запису трафіку (зокрема, системи СОРМ-3), встановлене в інтернет-провайдера. Схема не виключає можливості одночасного відвідування будь-якого сайту з віртуальної машини і з основної системи, але навіть у цьому разі з боку сайту було б дуже складно розпізнати, що відвідувач один і той самий. Зауважимо, що за цієї схеми немає необхідності маскувати трафік OpenVPN, оскільки він перебуває "всередині" каналу Tor з обфускацією. Водночас VPN забезпечить захист трафіку від можливого прослуховування на вихідних вузлах мережі Tor.

ВИСНОВОК ДО РОЗДІЛУ 3

Проєктування програмного комплекту анонімізації трафіку є важливим завданням у сфері інформаційної безпеки та приватності. Для ефективної анонімізації трафіку потрібно розробити програмне забезпечення, яке забезпечує надійний захист особистої інформації користувачів та конфіденційність даних. Важливими аспектами є ефективність, швидкодія та можливість використання в різних областях, забезпечуючи високий рівень безпеки та анонімності в мережі.

РОЗДІЛ 4
ЗАПУСК ТА ТЕСТУВАННЯ

4.1. Налаштування сервера

Попередній етап. VPS (Virtual Private Server) - послуга, в рамках якої користувачеві надається так званий "віртуальний виділений сервер". У плані управління операційною системою вона здебільшого відповідає фізичному виділеному серверу. Зокрема, є root-доступ, власні IP-адреси, порти, правила фільтрування і таблиці маршрутизації. Власник VPS може видаляти, додавати, змінювати будь-які файли, включно з файлами в кореневій та інших службових директоріях, а також встановлювати власні додатки або налаштовувати/змінювати будь-яке доступне йому прикладне програмне забезпечення [48]. Тип віртуалізації сервера може бути будь-яким, проте Xen і KVM (повна віртуалізація) вважаються надійнішими і зручнішими, ніж OpenVZ (загальне ядро ОС).

Відповідно, ми використовуватимемо VPS, щоб встановити та налаштувати на ньому VPN-сервер. Трафік між користувачем і VPN-сервером надійно зашифрований і тим самим захищений від прослуховування. Між сервером і кінцевим ресурсом трафік не шифрується засобами VPN, але може бути зашифрований протоколом TLS, якщо сайт, що відвідується, працює за безпечним з'єднанням HTTPS. З цього випливає важливе зауваження: сервер, на якому розміщується VPS, все ж здатний відстежувати історію підключень до зовнішніх ресурсів, і навіть прослуховувати трафік незахищених з'єднань.

Для тестового запуску VPN у рамках цієї роботи (і для особистого використання надалі) було орендовано недорогий віртуальний сервер у VPS-провайдера HostSailor в ОАЕ. Операційна система - Debian 9 x64, гіпервізор - Xen, сервер розташований у Нідерландах. Для віддаленого доступу до сервера за протоколом SSH використовувався клієнт PuTTY, а також програма WinSCP для зручної роботи з файлами на сервері.

Перш ніж приступати власне до встановлення VPN, слід убезпечити сервер від можливого несанкціонованого доступу. Авторизація

за паролем - не найбезпечніший метод для SSH, тому насамперед було налаштовано вхід за сертифікатом Ed25519, а парольну авторизацію відключено. Ed25519 - це схема сигнатур еліптичної кривої, яка забезпечує кращий захист, ніж ECDSA і RSA, і хорошу продуктивність через невелику довжину ключа. У програмі PuTTYgen генерується пара ключів і задається пароль для закритого ключа, потім публічний ключ копіюється на сервер і додається до списку авторизованих ключів.

Встановлення та налаштування OpenVPN і Easy-RSA. Переконаємося, що підтримка TUN/TAP на VPS увімкнена, для цього в консолі введемо команду cat /dev/net/tun. Висновок "File descriptor in bad state" є нормальним. Якщо ж отримаємо "No such file or directory", то адаптер TUN/TAP не ввімкнено [38]. Залежно від провайдера, потрібно ввімкнути цю функцію через панель управління сервером на сайті, або зробити запит до техпідтримки. На Xen VPS у Hostsailor адаптер був увімкнений від початку.

Для встановлення пакета OpenVPN у Debian виконуємо команди:

```
apt update
apt install openvpn
```

Створимо папку для ключів і перейдемо в неї:

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

Усі операції зі створення ключів і сертифікатів можна виконати за допомогою утиліти openssl, але простіше скористатися спеціально створеною для цього програмою Easy-RSA, яка використовує openssl для виконання дій з ключами і сертифікатами. Раніше Easy-RSA постачалася разом з OpenVPN, але тепер це окремий проєкт. Завантажуємо її, витягаємо і створюємо файл налаштувань із зразка, що додається:

```
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 в ній відкриваємо файл vars. Знаходимо такі 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 обов'язкова для генерації ключа. Значення в лапках можна замінити на будь-які на свій розсуд, вони в цьому разі 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 на sha512. Однак, замість RSA можна використовувати більш сучасну криптографію на еліптичних кривих [49], що дасть експоненціальне зростання криптостійкості за меншої довжини ключа. Наприклад, популярним сьогодні ключам RSA з довжиною 1024-2048 біт відповідає всього 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 підтримуваних кривих 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, використовуваних для підписання та обміну ключами, не існує, і деякі фахівці вважають це малоймовірним. Під час 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 і 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.

Генерування сертифікатів. Нам необхідно створити так звану PKI - інфраструктуру публічних ключів. Загалом, PKI ґрунтується на використанні криптосистеми з відкритим ключем і наявності засвідчувального центру. Ключі створюються

парами - закритий і відкритий. Для обміну з ким-небудь захищеною інформацією ми обмінюємося відкритими ключами. У цьому випадку сервер матиме свій закритий ключ і відкриті ключі клієнтів. У клієнтів є свої закриті ключі і відкритий ключ сервера. А засвідчувати справжність ключів буде засвідчувальний центр, який ми також створимо самостійно, і у всіх учасників обміну кореневий буде його кореневий сертифікат. Порядок дій для створення PKI такий:

1. Ініціалізувати PKI;
2. Створити засвідчувальний центр - Certificate Authority;
3. Згенерувати сертифікати сервера;
4. Згенерувати сертифікати клієнта;
5. Створити файл параметрів Діффі-Геллмана;
6. (Опціонально) Створити список відкликання сертифікатів;
7. (Посилення безпеки) Створити ключ аутентифікації TLS.

Виконуємо команду ініціалізації:

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

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

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

Як і під час генерації ключів SSH, тут потрібно захистити ключ надійним паролем. Також буде запитано "Common Name", можна просто натиснути Enter. Отримуємо файли: ca.crt (кореневий сертифікат, відкритий, буде передаватися клієнтам) і ca.key (закритий ключ, який не повинен бути скомпрометований).

Тепер створимо пару ключів власне для VPN-сервера. Закритий ключ сервера ми не захищатимемо паролем, оскільки вводити цей пароль довелося б під час кожного перезавантаження сервера. Створюємо запит на сертифікат:

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

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

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

Підтверджуємо операцію і вводимо пароль закритого ключа УЦ. Отримаємо підписаний відкритий ключ сервера - server.crt. Повний шлях до нього вийде таким:

```
/etc/openvpn/keys/easyrsa3/pki/issued/server.crt.
```

Далі, у випадку з вибором алгоритму RSA, слід згенерувати файл параметрів Діффі-Хеллмана. Це забезпечить використання надійної схеми шифрування, за якої навіть компрометація секретного ключа не дасть змоги розшифрувати записаний трафік із попередніх сесій. Процес займе деякий час:

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

На виході отримуємо файл dh.pem. У даному ж випадку був обраний алгоритм еліптичної криптографії, який не вимагає створення цього файлу. Також можна створити список відкликаних сертифікатів на випадок втрати будь-якого пристрою з OpenVPN-клієнтом. Процедура відкликання зробить загублений ключ недійсним. Зараз просто створюємо сам список:

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

Нарешті, скопіюємо ключі в папку OpenVPN і перейдемо в цю папку:

```
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 задіємо механізм HMAC (hash-based message authentication code), який служить для перевірки цілісності переданих даних, щоб унеможливити можливість "атаки посередника". Для увімкнення HMAC потрібно згенерувати спеціальний ключ і додати в конфігураційний файл сервера директиву tls-auth, що вказує на цей ключ. Тоді сервер додаватиме підпис HMAC до всіх пакетів рукостискання SSL/TLS. Будь-який UDP-пакет, що 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 самого протоколу SSL/TLS. Це може захистити від:

- DoS-атак або флуду на UDP-порт OpenVPN.
- Сканування портів з метою визначення тих, що прослуховуються сервером UDP-портів.
- Вразливостей, пов'язаних із переповненням буфера в реалізації SSL/TLS.
- Спроб ініціації SSL/TLS-рукостискання від несанкціонованої машини (хоча, зрештою, такі рукостискання не пройдуть автентифікацію, tls-auth може відсікти їх на набагато більш ранній стадії).

Згенеруємо ключ:

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

Цей ключ буде також передано клієнту. Однак сучасні версії OpenVPN мають досконаліший механізм захисту, що активується опцією tls-crypt. Це охоплює не тільки функціонал tls-auth, а й шифрування всіх пакетів керуючого каналу, що ускладнює розпізнавання трафіку OpenVPN. Ключ використовується такий 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 і ta.key мають бути права 0600. На цьому етапі сервер уже готовий до роботи, але необхідно ще створити ключі клієнтів і правильні файли конфігурації. Переходимо знову в папку EasyRSA, створюємо і підписуємо ключ:

```
cd /etc/openvpn/keys/easy-rsa-master/easyrsa3
./easyrsa gen-req client_name nopass
./easyrsa sign-req client client_name
```

Параметр nopass застосовується на розсуд користувача. Якщо захистити ключ паролем, це підвищить безпеку, але доведеться вводити пароль при кожному підключенні до VPN. У цьому ж випадку для підключення достатньо мати закритий ключ. Ім'я client_name - довільне, наприклад, home_pc. Тепер, коли всі ключі створено, конфігуруємо і запускаємо сервер. У папці /etc/openvpn створюємо файл server.conf (або замінюємо наявний). Вміст використаного файлу наведено в додатку Б.

Додаткове налаштування і 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=188.214.122.10
server=46.85.126.16
interface=tun0
```

У цьому разі тут вказано адреси використаних DNS від OpenNIC, а також мережевий 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 за замовчуванням були присутні.

Для перенаправлення трафіку з мережі VPN до зовнішнього інтернету зазвичай використовують механізми NAT і 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
188.214.122.10 iptables -A INPUT -i eth0 -p icmp -j DROP
```

Тут 10.8.0.0/24 - підмережа, яка використовується для VPN, а 188.214.122.10 - публічна статична адреса цього VPS. Друге правило блокує ICMP із зовнішньої мережі, як уже згадувалося - це захід боротьби з розпізнаванням тунелю.

Перезапуск DNSMasq, запуск і 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.

4.2. Налаштування робочого місця

На клієнтський ПК встановлюється VirtualBox, образи двох віртуальних машин Whonix завантажуються з офіційного сайту та імпортуються у VirtualBox. В описуваній схемі використовується тільки Whonix-Gateway, але доцільно завантажити і Whonix-Workstation для тих випадків, коли важливіша підвищена захищеність, ніж зручність і непомітність. Створюється ще одна віртуальна машина, в якій встановлюється Windows 7 (найкращий варіант - заздалегідь створити образ ВМ зі встановленою системою та іншим ПЗ, а потім імпортувати його у клієнта відразу в готовому вигляді). 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 занадто явно вказує на наявність ВМ. У мережевих налаштуваннях самої системи слід задати 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 ввімкнення obfs4 і 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, кожна в окремому рядку
ExcludeNodes {ua}, {??} # ?? – вузли з невідомою геолокацією
```

Під час тестування було використано такі адреси мостів (на момент написання вони залишаються актуальними):

```
bridge obfs4 184.125.18.38:443 9F0BC3AA3CC72F17DC7789D7ABC7A767038F82CB
cert=lINVQVt8EQS5q9DWz3S+RHLosgiRVXueHUXfY3qtas1qHhGXvg7MOu6jECDZ0mbrS7tQLA iat-
mode=0 bridge obfs4 145.59.73.146:59015 1594A9B832D4E0BD356A5988B364F1687814EC5D
cert=3DlWyDr4IwpZlxQbDX+7obB/EZr+eQavtnFbqaQsLym01MgIIsXPIl5E3ftp4ILYK/G+OQ iat-mode=0
bridge obfs4 44.26.192.107:43081 77644CB35D63204974B84855A580155053365935
cert=yI120MhitxPLUcJFhDgspTy+sHOm4VlSAXLegRjYsu9qEd2yR59YNq3tvDnkRiGY/+rQFQ iat-mode=0
```

У систему встановлюється OpenVPN-клієнт і браузер Firefox. Файл конфігурації для клієнта наведено в додатку В (деякі параметри OpenVPN для сервера і клієнта запозичені у сервісу RootVPN). У разі вимкненого VPN весь трафік іде через Tor, що дає змогу відвідувати onion-сайти в Firefox (спочатку необхідно в about:config вимкнути параметр network.dns.blockDotOnion). Важливе зауваження: не слід встановлювати Tor Browser на даній машині, оскільки це призведе до ланцюжка "Tor через Tor".

Вбудований Tor-клієнт браузера працюватиме через Tor-шлюз. Це не тільки знижує швидкодію, а й потенційно небезпечно через можливу появу самопересічного маршруту і скорочення ефективної довжини ланцюжка до одного-двох вузлів. Якщо необхідно використовувати Tor Browser, можна запустити його в основній системі або всередині Whonix-Workstation.

У Firefox встановлюється набір доповнень, згаданих у розділі 3, і застосовуються необхідні налаштування. Повний список можливих параметрів конфігурації досить великий і не має єдиного правильного варіанта. "Білий список шрифтів" застосовується так: на одному із сайтів (наприклад, BrowserLeaks) виявляємо список шрифтів, що розпізнаються в поточній конфігурації. Створюємо строковий параметр font.system.whitelist на сторінці about:config у Firefox. Вміст параметра заповнюємо отриманим списком шрифтів. Тепер "відбиток шрифтів" змінюватиметься при видаленні деяких шрифтів зі списку. Зазначимо, що різні сайти перевіряють наявність різного набору шрифтів, тому видалення (або додавання в систему) якогось 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, узятим з будь-якого реального ПК. Приклад:

webgl.renderer-string-override = ANGLE (Intel(R) HD Graphics 620 Direct3D11 vs_5_0 ps_5_0)

Підміну User-agent зручно виконувати за допомогою User-agent Switcher, однак невідповідність ОС або рушія браузера можна виявити за непрямими ознаками, тому бажано підміняти тільки версію браузера. У доповнення CanvasBlocker рекомендується вибрати режим "fake at input", оскільки він складніший для виявлення. Системний годинник слід періодично синхронізувати. Крім того, у Firefox 60 точність таймера знижено до 2 мс за замовчуванням і до 100 мс у режимі ResistFingerprinting.

Очищення даних (cookies, Local Storage тощо) відбувається під час перезапуску Firefox, а також під час використання функції "Забути" або ручного видалення даних для конкретного сайту (у Firefox 63 розробники планують спростити цю процедуру). Крім того, доповнення Firefox Multi-Account Containers дає змогу відкрити один і той самий сайт у кількох ізольованих вкладках, кожна з яких не має доступу до даних інших вкладок.

4.3. Тестування отриманої збірки

Фактори, що перевіряються, і веб-сайти, що використовуються. Необхідно переконатися, що підміна всіх цифрових відбитків надійно працює, а відвідувані сайти не розпізнають наявність засобів анонімізації. У віртуальній машині з Windows було виконано підключення до налаштованого VPN через Whonix-Gateway, використано Firefox 117 (остання стабільна версія на момент тестування). Під час роботи не було помічено проблем із підключенням OpenVPN за протоколом TCP через ланцюжок Tor і obfs4. Часовий пояс у системі було змінено до запуску браузера.

Для перевірки VPN на предмет "непомітності" використовували такі інтернет-ресурси:

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 "хороший" результат.

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

http://witch.valdikss.org/ - визначає операційну систему за специфічними особливостями TCP і зіставляє з User-agent браузера. Перевіряє значення MTU для виявлення OpenVPN.

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

Основні сайти для визначення цифрових відбитків: https://browserleaks.com/ - дає змогу 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 і його відповідність відомим браузерам.

https://audiofingerprint.openwpm.com/ - відбиток AudioContext API.

https://browserprint.info - комплексний відбиток за низкою параметрів, включно зі шрифтами, Canvas, AudioContext, розміром екрана та іншими.

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

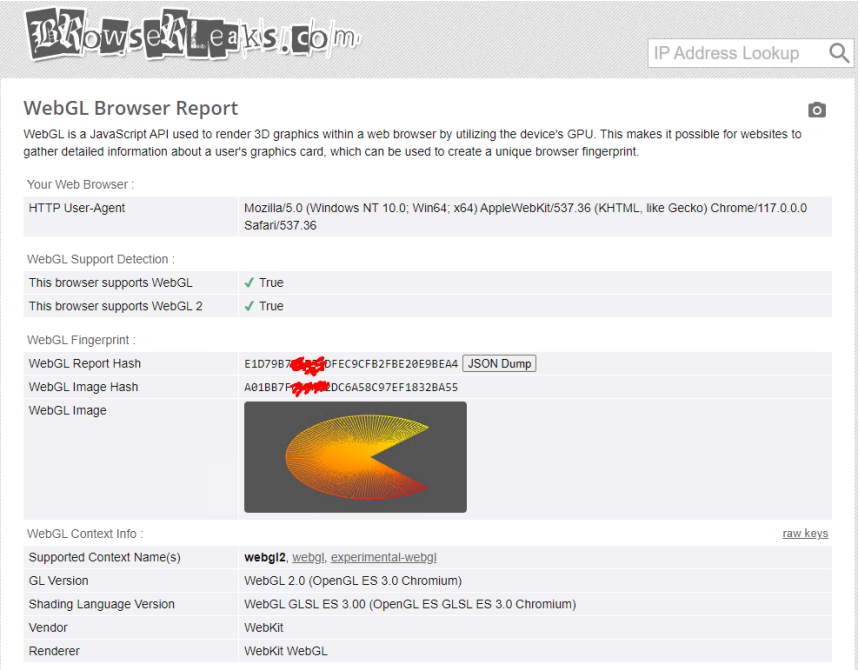

Рис. 4.1. Інформація з браузера, встановленого на ПК

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 підміни. Завдання - упевнитися в наявності можливості змінювати їх багаторазово.

Перевірки на виявлення засобів анонімізації показали практично ідеальні результати, однак слід розуміти, що деякі сайти можуть використовувати більш повні бази IP-адрес хостингів і VPN-провайдерів.

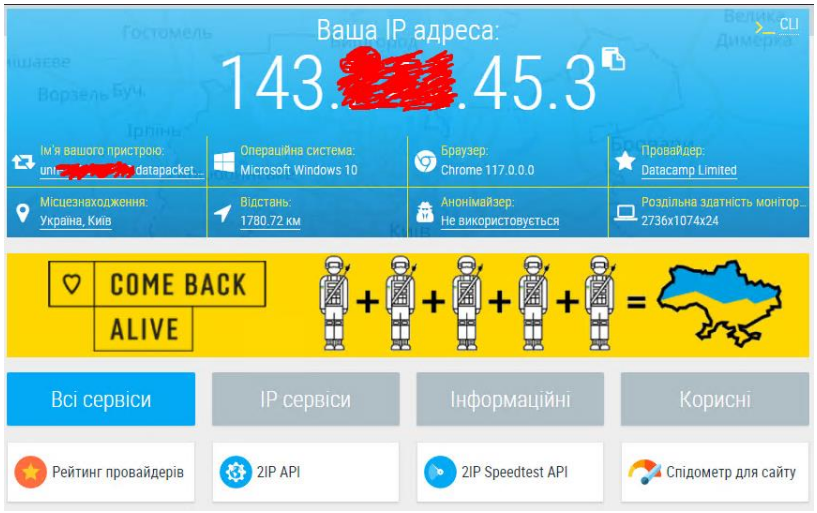

Рис. 4.2. Перевірка на сайті 2ip.ua

Важливо зазначити, що цей ресурс не зміг визначити DNS-адреси і факт приналежності IP до хостинг-провайдера HostSailor. Це є недоліком сайту, а не перевагою VPN-сервера. Імовірність такого розпізнавання існує під час використання практично будь-яких VPN-сервісів і VPS-хостингів, однак вона істотно нижча, ніж для адрес мережі Tor.

Для наочного порівняння наведемо результат цієї перевірки для VPN-провайдера ProtonVPN (у режимі безкоштовного доступу):

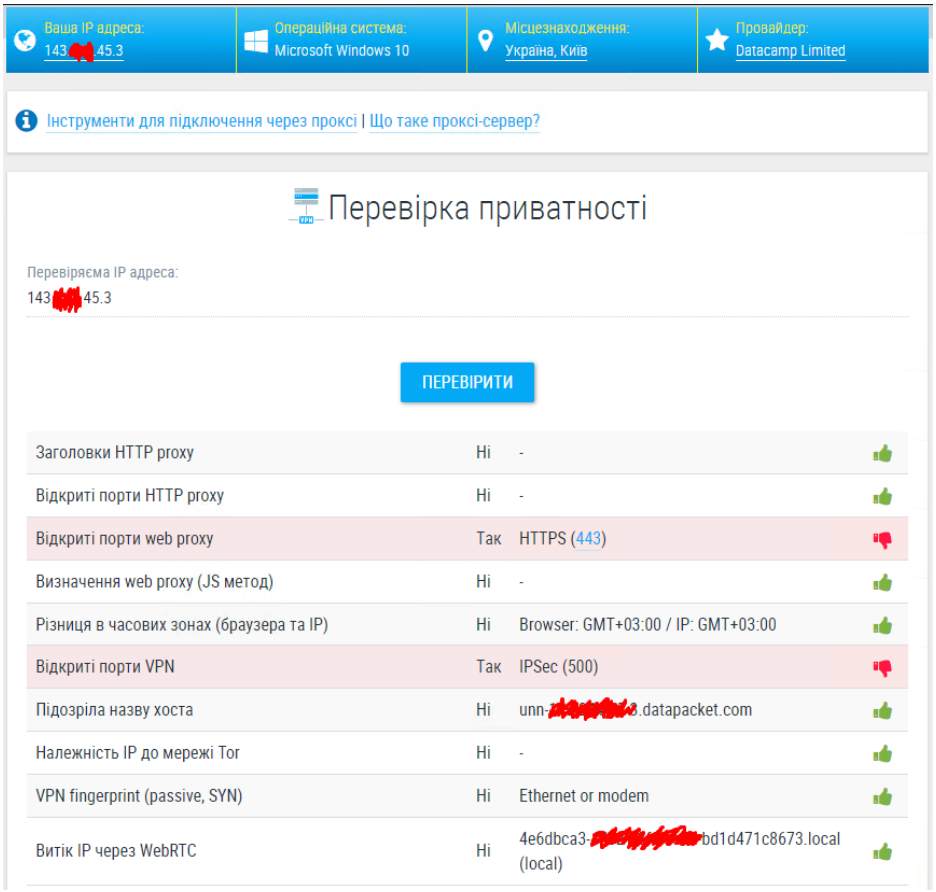

Рис. 4.3. Приклад незадовільного результату

Очевидно, що тут не було виставлено відповідного часового поясу, однак інші три параметри залежать саме від налаштувань сервера.

Тестування на сайті Whoer показало, що витік реального IP через WebRTC не відбувається, але є витік внутрішньомережевої адреси, яка побічно вказує на наявність VPN. Після ввімкнення в uBlock відповідної опції (Prevent WebRTC from leaking local IP addresses) цей витік блокується. Альтернативний спосіб: встановити параметр

media.peerconnection.ice.proxy_only = true у конфігурації Firefox. Результат аналогічний дії uBlock. Після цього цей сайт не виявляє жодних ознак використання анонімайзера:

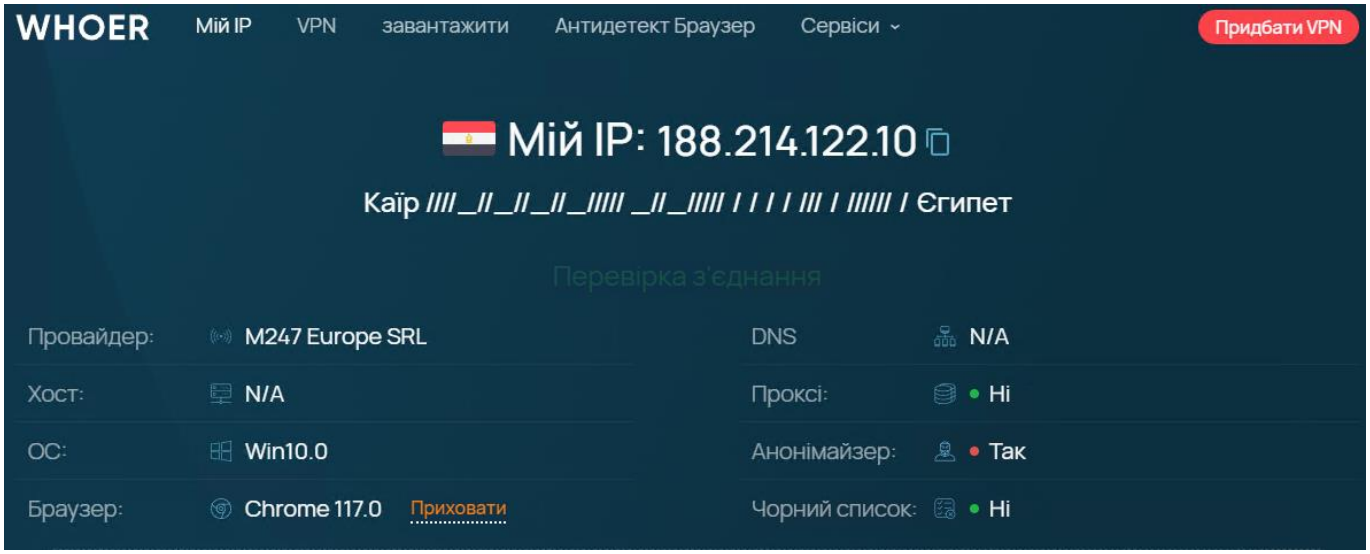

Рис. 4.4. Тест на сайті Whoer.net

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

```
First seen    = 2023/09/15 00:49:21
Last update   = 2023/09/15 00:49:21
Total flows   = 2
Detected OS   = Linux 2.2.x-3.x [generic]
HTTP software = ???
MTU           = 1500
Network link  = Ethernet or modem
Language      = ???
Distance      = 10
Uptime        = 29 days 9 hrs 42 min (modulo 49 days)

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

Рис. 4.5. Відповідь сайту witch.valdikss.org

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

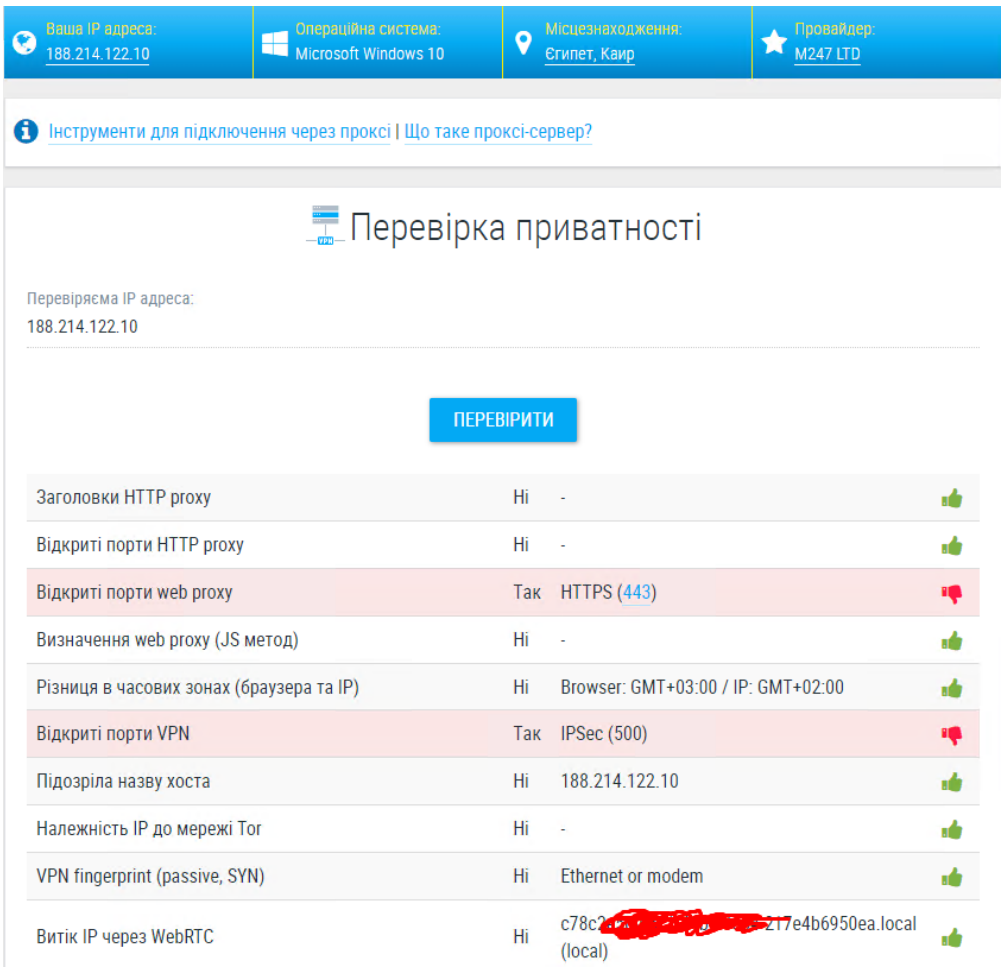

Рис. 4.6. Перевірка адрес DNS

Один із варіантів цифрового відбитка браузера наведено нижче

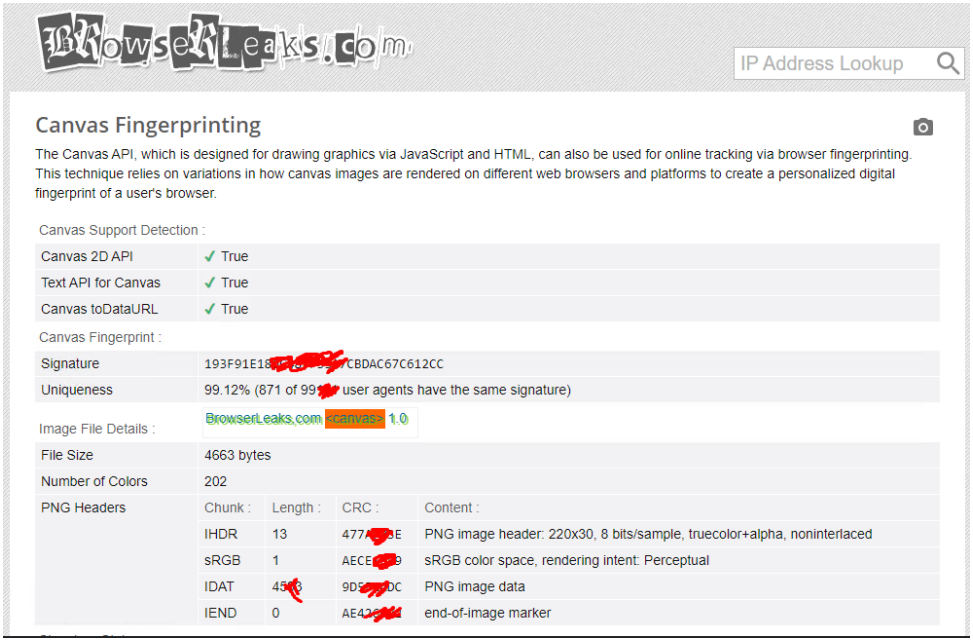

Рис. 4.7. Цифровий відбиток браузера

Відбиток Canvas на сайті BrowserLeaks має такий формат:

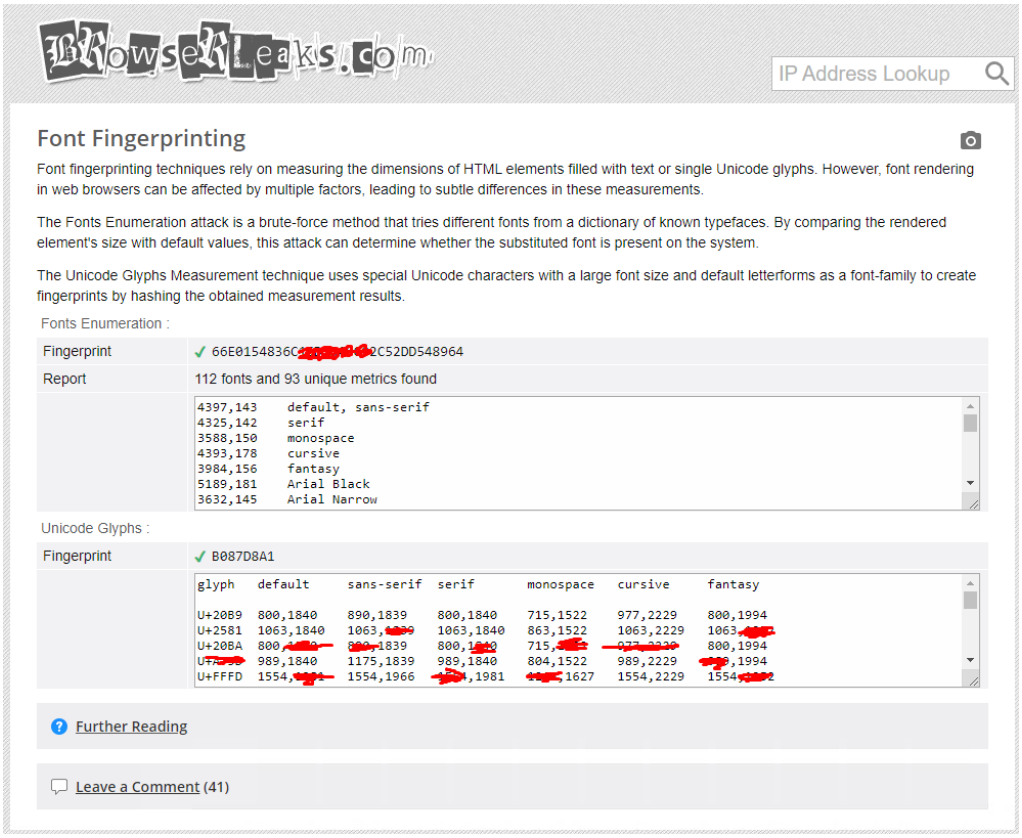

Рис. 4.8. випадковий Canvas Fingerprint з CanvasBlocker

Порівняємо це з оригінальним відбитком і з підміною через вбудовану функцію Firefox ResistFingerprinting:

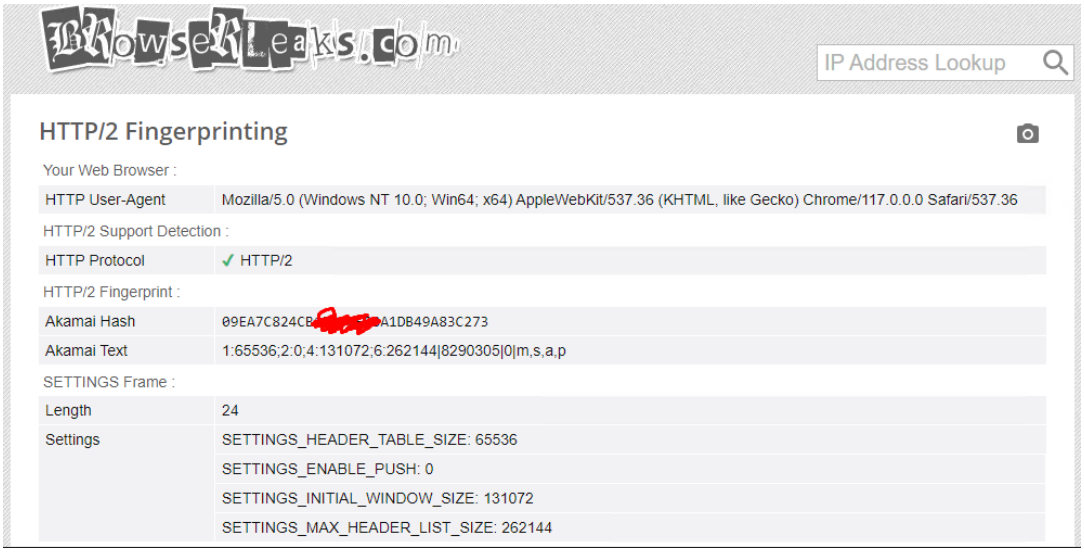

Рис. 4.9. відбитки HTML5 Canvas

1 - Відбиток без використання підміни

2 - Випадковий відбиток при ввімкненому CanvasBlocker

3 - Статична підміна з опцією ResistFingerprinting

Цей сайт не виявляє присутності CanvasBlocker у режимі "fake at input", як і інших підозрілих ознак, крім uBlock:

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

Рис. 4.10. Вихідний відбиток WebGL у VirtualBox

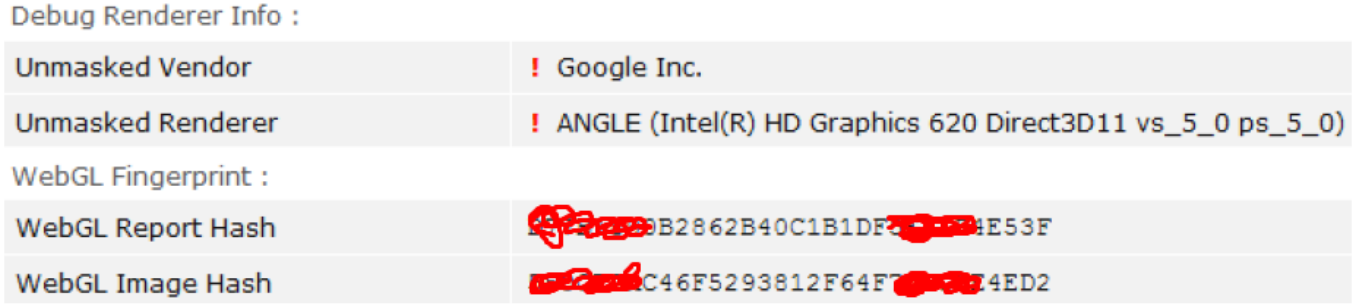

Рис. 4.11. Відбиток після підміни

Тепер встановимо параметр

webgl.enable-debug-renderer-info=false :

Рис. 4.12. Підміна відбитка і приховування даних

CanvasBlocker впливає тільки на значення Image Hash, змінюючи його випадковим чином. Report Hash залежить від вмісту рядків Vendor і Renderer, які перевизначаються через параметри

Firefox (webgl.renderer-string-override).

Відбитки шрифтів:

Рис. 4.13. Відбиток шрифтів до підміни

Рис. 4.14. Відбиток шрифтів після підміни

Приклади Audio Fingerprint було отримано на сайті vektort13.pro з огляду на більш компактне подання, ніж на openwpm.com.

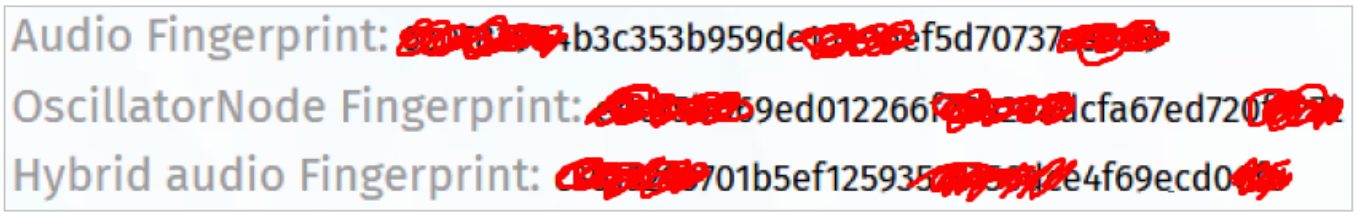

Рис. 4.15. Вихідні відбитки AudioContext

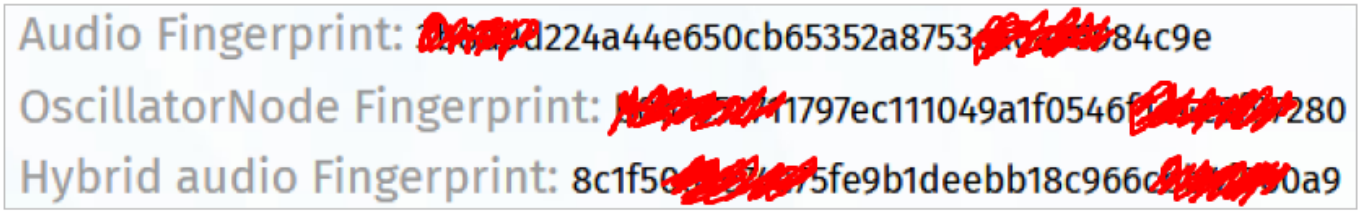

Рис. 4.16. випадкові відбитки AudioContext

Під час тестування було підтверджено можливість зміни цифрових відбитків необмежену кількість разів (Canvas, WebGl Image, Audio Fingerprint) або, щонайменше, неодноразової підміни (шрифти, User-agent, роздільна здатність екрана, WebGL Render, ClientRects тощо).

ВИСНОВОК ДО РОЗДІЛУ 4

Запропонована конфігурація ПЗ забезпечує ефективну протидію різним сучасним методам відстеження, надійну ізоляцію анонімного браузера від не-анонімної системи, захист від розкриття реальних даних про систему, не порушуючи при цьому функціональність браузера. Успішно перевірено також правильність налаштування OpenVPN щодо його маскування. Водночас необхідно враховувати, що підключення VPN через Tor є менш надійним з погляду анонімності, ніж використання тільки Tor, так само як і ОС Windows зазвичай не рекомендується для анонімної роботи, на відміну від спеціальних Linux-дистрибутивів.

Результатом успішної роботи запропонованого методу анонімізації в мережі стала перевірка за допомогою авторитетного веб-ресурсу Cover Your Tracks, що показало (рис. 4.17) надійний захист від відстежування в мережі Інтернет.

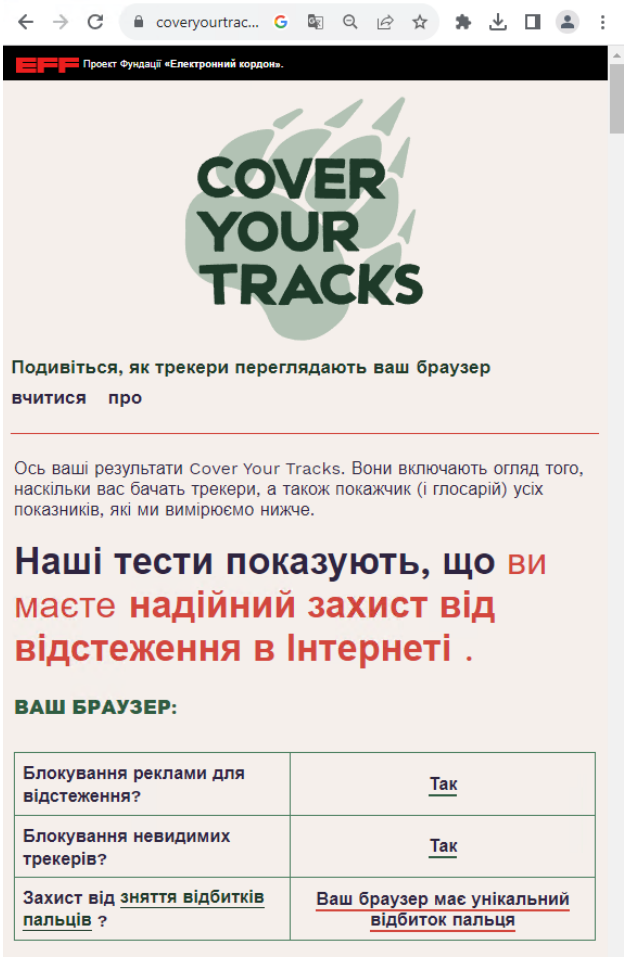

Рис. 4.17. Результати перевірки надійності захисту в мережі інтернет

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

У результаті даної дипломної роботи була створена концептуальна схема комутаційного обладнання з метою анонімізації потоків трафіку. Автор дипломної роботи виступає як інженер-проєктувальник, який здійснив проєктування та аналіз концептуальної схеми абонентського приймача кабельного цифрового телебачення. Локація робочого місця інженера-проєктувальника - проєктувальний відділ на другому поверсі.

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проєктування розташований на другому поверсі п'ятиповерхового будинку. Площа приміщення складає 32 квадратні метри зі сторонами 8 метрів (довжина) та 4 метри (ширина), висота становить 4 метри. Загальний об'єм приміщення складає 128 кубічних метрів. У відділі розміщено 5 робочих місць інженерів-проєктувальників, кожне з яких оснащене комп'ютерами [61].

Площа робочого місця одного співробітника складає:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Робочий об'єм для одного співробітника становить:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

N- кількість співробітників у відділі

$S_{\text{заг.пл}}$ – загальна площа;

$V_{\text{заг.об}}$ – загальний об’єм.

Робоча площа на одне робоче місце повинна відповідати вимогам і становити не менше 6 м^2, а об'єм приміщення для кожного співробітника має складати не менше 20 м3

[61]. В проєктному відділі інженера-проєктувальника забезпечені вимоги до робочого простору.

У приміщенні проєктного відділу температура повітря у теплий період року становить 30°С, а освітлення відбувається природним та штучним світлом. Штучне освітлення виконане у вигляді переривчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, що перевищує норматив у 50 дБ, встановлений Державними санітарними нормами [62].

Робоче місце спроєктоване таким чином, щоб природне світло надходило з лівої сторони і його джерело знаходилося на відстані 1 м від робочого місця. Робочий стіл має відповідні розміри: висота робочої поверхні столу над підлогою складає 750 мм, глибина - 800 мм, ширина - 1300 мм. Також передбачено простір для ніг висотою 650 мм та шириною 600 мм.

Важливо наголосити на створенні сприятливих умов праці для інженера-проєктувальника, оскільки це має значущий вплив як на полегшення його роботи, так і на підвищення продуктивності праці. Відповідно до [63] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення.
2. Недостатня освітленість робочої поверхні.
3. Виробничий шум.
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до джерела [64], робота інженера-проєктувальника у відповідних умовах приміщення з енерговитратами 90-120 ккал/год. відноситься до категорії легких фізичних робіт Іа. Ці роботи виконуються сидячи та не потребують значного фізичного напруження.

Таблиця 5.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Іа	22-24
Теплий період року		23-25

Закінчення таблиці 5.1

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,℃	
		Верхня межа	Нижня межа
Холодний період року	Легка Іа	25	21
Теплий період року		28	22

У проєктному відділі виникають певні проблеми, що стосуються температури, освітленості та шуму.

Температура:

Температура повітря в приміщенні проєктного відділу становить 30℃, що перевищує допустиме значення на 2 ℃. Для забезпечення комфортних умов праці, температуру було скориговано до 23 ℃ за допомогою механічної вентиляції з вентилятором VORTICE VARIO з повітрообміном 680 $м^3$/год.

Освітленість:

У приміщенні встановлені персональні комп’ютери, а також є природне та штучне освітлення. Однак освітленість робочої поверхні не відповідає вимогам, складаючи 370 лк з коефіцієнтом освітленості 1.2%, тоді як вимагається не менше 1.5%. Для поліпшення освітленості можна переглянути розміщення світильників та оптимізувати використання природного світла.

Шум:

У приміщенні виробничий шум виникає від комп’ютера та периферійних пристроїв. Для забезпечення вимог до рівнів звукового тиску, необхідно вжити заходів щодо зниження шуму комп’ютера та периферійних пристроїв.

Загальна мета полягає в тому, щоб забезпечити сприятливі умови праці для інженера-проєктувальника, що сприятиме полегшенню його роботи та підвищенню продуктивності [66]:

Таблиця 5.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Дійсно, рівень шуму у проєктному відділі перевищує допустимі норми, що може негативно впливати на комфорт та продуктивність співробітників. Для зниження шумового навантаження та створення комфортних умов рекомендується вжити наступні заходи:

Місцева звукоізоляція:

Встановлення звукоізолюючих матеріалів або панелей на робочих місцях, які дозволять зменшити розповсюдження шуму та його вплив на співробітників.

Загальна звукоізоляція:

Застосування звукоізоляційних матеріалів для стін, стелі та підлоги приміщення для зменшення загального шумового фону.

Шумопоглинаючі екрани:

Встановлення спеціальних шумопоглинаючих перегородок або екранів, які зменшать проникнення шуму у робочі зони.

Поглинаючі фільтри:

Використання шумопоглинаючих фільтрів для комп’ютерів та периферійних пристроїв для зменшення викидів шуму.

Ці заходи спрямовані на створення комфортних та продуктивних умов праці для співробітників в проєктному відділі, а також на відповідність нормам щодо рівнів шуму.

5.2. Розрахунок повітрообміну за надлишком тепла у проєктному відділі:

Приміщення має розміри 4×8×4, яке розміщується на другому поверсі п’ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні

жалюзі. У приміщенні 5 інженерів-проєктувальників, розташовано $N_{пк} = 5$ персональних комп'ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,} \text{ Вт} \quad (5.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$- кількість тепла від інженерів-проєктувальників

$Q_{рад,}$- кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \eta, \quad (5.2)$$

де N - сумарна потужність джерел освітлення, Вт; η - коефіцієнт теплових витрат (η = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0,55 = 275 \text{ Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп'ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \quad (5.3)$$

де n – кількість комп'ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп}=400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр}=465$ Вт

$$Q_{облад} = 5 \cdot 400 + 465 = 2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проєктувальників:

$$Q_{ін\text{-}пр.} = n \cdot q \text{ , Вт} \tag{5.4}$$

n – кількість інженерів-проєктувальників

q – кількість тепла, що виділяється одним інженером-проєктувальником

Кількість тепла, що виділяється одним інженером-проєктувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \cdot 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад} = m \cdot S \cdot k \cdot q_{скл} \tag{5.5}$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = *150* – південь;

$$Q_{рад} = 1 \cdot 2{,}88 \cdot 0{,}6 \cdot 150 = 259{,}2 \text{ Вт}$$

5. Загальна кількість тепла в проєктному відділі:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад} = 275 + 2500 + 495 + 259{,}2 = 3{,}529 \text{ кВт}$$

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c \cdot \rho \cdot (t_{вид} - t_{зовн})} \text{ , м}^3/\text{год} \tag{5.6}$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$$Q = 3600 \cdot Q_{надл} = 3600 \cdot 3529 = 12704 \cdot \text{Вт} \cdot = \cdot 5328 \cdot \text{кДж;}$$

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС приймається рівною $1{,}01 \cdot 10^3$Дж/кг);

ρ – густина повітря, кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3);

$t_{вид}$– температура повітря, що видаляється, $t_{вид}$=*30*℃

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23℃

$$L = \frac{5328}{1{,}01 \cdot 10^3 \cdot 1{,}2 \cdot (30 - 23)} = 628 \text{ м}^3 \text{/год}$$

Оскільки, в проєктному відділі підвищена температура повітря на 2 ℃ від допустимого значення 28℃, встановили механічну вентиляцію з вентилятором VORTICE VARIO , яка забезпечила надходження до приміщення температури повітря 23 ℃, дане значення є оптимальним.

5.3. Пожежна безпека

У відповідності до [67], це приміщення відноситься до категорії В з погляду вибухово-пожежної та пожежної небезпеки через використання твердих горючих матеріалів з температурою спалаху понад 61℃.

Проєктний відділ обладнаний наступним чином:

Установлено два безпровідних датчики диму SD-02, які сповіщають у разі диму в приміщенні (площа охоплення до 20 м^2).

Встановлено два порошкові вогнегасники ВП-5 для категорії В приміщень (площа до 50 м^2, маса вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників - 2).

Використовується бездротова пожежно-охоронна система LifeSOS LS-30LR, яка реагує на вторгнення та повідомляє сигнал тривоги на центральний блок через радіоканал, активує сирену, повідомляє на пульт централізованого нагляду, надсилає SMS та дзвінки на визначені телефонні номери.

Для запобігання виникненню пожеж проводяться організаційно-технічні заходи пожежної безпеки, включаючи включення питань пожежної безпеки у всі інструкції по техніці безпеки, дотримання експлуатаційних режимів електричних мереж та обладнання, заборону куріння в недозволених місцях, видання необхідних інструктажів та складання планів евакуації.

План евакуації включає графічну та текстову частини. Графічна частина представляє схематичний план поверху, на якому зеленими суцільними стрілками показані шляхи евакуації до основних виходів, а пунктирними зеленими стрілками - до

аварійних виходів. Двері на шляху евакуації відчиняються назовні у напрямку виходу з будівлі. На плані евакуації показано розміщення вогнегасників, пожежних гідрантів, телефонів, аптечок медичної допомоги, електрощитів, датчиків диму та системи охоронно-пожежної сигналізації за допомогою умовних знаків.

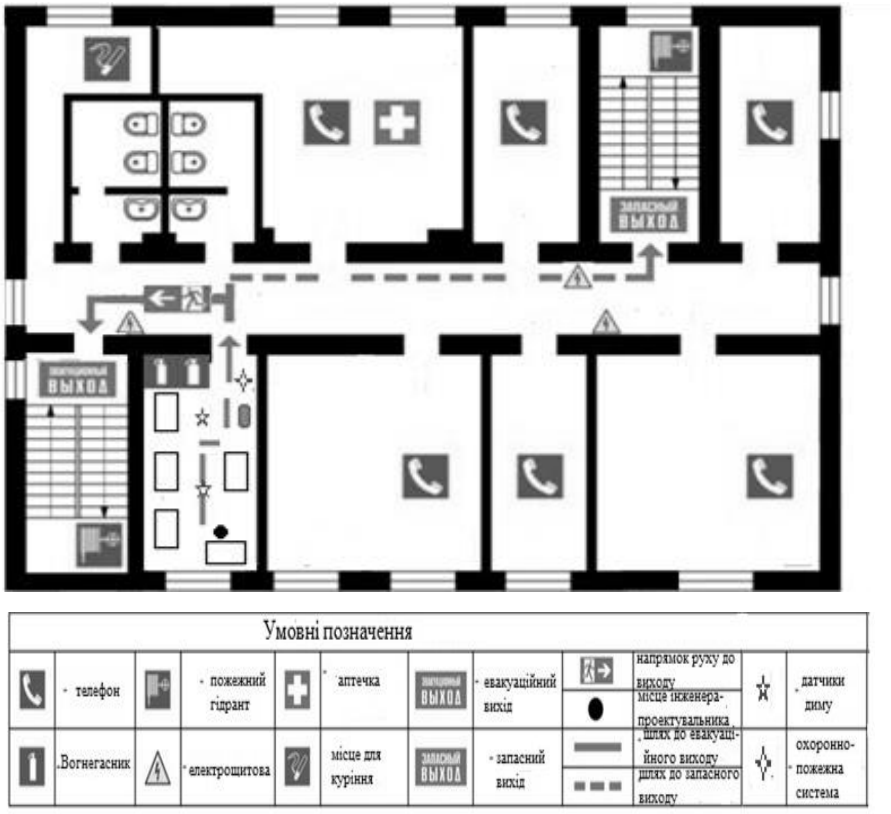

Рис 5.1. План евакуації 2 поверх

5.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Загальні вимоги до облаштування робочого місця з ПК включають наступне:

Робоче місце для працівників, які користуються відеотерміналами, має бути організоване таким чином, щоб вікна, освітлювальні прилади та поверхні, які відбивають світло, не потрапляли в поле зору працівника. Поверхня робочого столу не повинна мати полірованe покриття. Для уникнення блисків на екрані відеомоніторів, особливо влітку та сонячні дні, слід розміщувати екран так, щоб світло від вікна падало збоку, найкраще зліва.

Екран відеомонітора ПК повинен знаходитися на відстані не менше 500-700 мм від очей користувача (оператора) та під кутом зору від 10 до 40 градусів. Рекомендоване розташування екрану перпендикулярно до лінії зору оператора.

Комп'ютер повинен бути розміщений на відстані не менше 1 метра від джерела тепла.

Клавіатура має бути розміщена на поверхні столу або спеціальній підставці на відстані 100-300 мм від краю, що звернений до користувача. Кут нахилу панелі клавіатури до горизонтальної поверхні повинен бути в межах від 5 до 15 градусів.

Висота робочої поверхні столу повинна бути в межах 680-800 мм.

Крісло повинно забезпечувати зручні умови праці для оператора та можливість регулювання висоти сидіння, кута нахилу спинки та її висоти.

Щоб запобігти прямому попаданню сонячних променів на екран відеомонітора, слід встановити сонцезахисні пристрої на вікнах. Розміщення екрану відеомонітора таким чином, щоб світло від вікна приходило збоку, найкраще зліва.

Рекомендується використовувати люмінесцентні лампи як джерело штучного освітлення у приміщеннях, де встановлено ПК. Також можна використовувати лампи розжарювання у світильниках для місцевого освітлення. Освітленість на робочому місці повинна складати не менше 400 лк на горизонтальній площині на висоті 0,8 м від рівня підлоги та не більше 200 лк у вертикальній площині перед екраном. Це сприятиме зменшенню напруження зору та рівномірному розподілу яскравості між робочою поверхнею відеомонітора та навколишнім простором.

У приміщеннях, де працюють з ПК, необхідно здійснювати щоденне вологе прибирання та регулярне провітрювання протягом робочого дня. Необхідно видаляти пил з екрану не рідше одного разу на день.

Для захисту оператора від електромагнітних випромінювань та електростатичних полів, що генеруються відеомонітором, слід використовувати захисні екрани.

Користувачі ПК повинні носити одяг із природних матеріалів або комбінованих з природних і синтетичних волокон.

Вимоги безпеки перед розпочатком роботи включають наступне:

Перед початком роботи слід перевірити цілісність корпусів системного блоку, відеомонітора, принтера та клавіатури шляхом огляду.

Перевірити стан кабелів живлення та їх правильність підключення до розеток електромережі, продовжувачів, розгалужувальних коробок та штепсельних вилок.

Підготувати робоче місце, прибравши речі, які можуть перешкоджати під час роботи.

Увімкнути живлення ПК.

У разі виникнення проблем з запуском комп'ютера або входженням у робочий режим слід повідомити керівника або інженера з відділу інформаційних технологій.

При виявленні пошкоджень або інших недоліків слід повідомити безпосереднього керівника і не приступати до роботи без його дозволу.

Вимоги щодо безпеки під час роботи наступні:

Всі компоненти пристроїв, включаючи клавіатуру, повинні бути надійно розміщені на столі, при цьому передбачається можливість переміщення клавіатури згідно з побажаннями користувача ПК. Розташування та кут нахилу клавіатури повинні бути зручними для користувача. Якщо клавіатура не має спеціального місця для рукопокладання, її слід розміщувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. Під час роботи з клавіатурою слід сидіти прямо і уникати напруження.

Щоб уникнути негативного впливу пристроїв типу "миша" (незручна поза, постійний контроль), необхідно забезпечити вільну площу на поверхні столу для переміщення миші та зручну опору для ліктьового суглоба.

Заборонено сторонні розмови та будь-які роздратовуючі шуми.

Час від часу, коли ПК вимкнено, слід видаляти пил з обладнання за допомогою слабко вологої серветки з милом. Екран і захисний екран слід протирати ватою, змоченою спиртом.

Заборонено використовувати рідини або аерозольні засоби для чищення поверхонь ПК.

Заборонено:

- самостійно ремонтувати пристрої, у яких кінескоп та інші елементи можуть бути під високою напругою (до 25 кВ);
- класти будь-які предмети на обладнання ПК, а також їжу та напої на клавіатуру або біля неї, оскільки це може призвести до поломки;
- блокувати вентиляційні отвори, що може призвести до перегріву та несправностей.

Для зменшення негативного впливу різних ризикових факторів, пов'язаних з роботою на ПК, передбачені регулярні перерви для користувачів ПК:

- кожні 10 хвилин після безперервної роботи;
- кожні 2 години – 15 хвилин.

Якщо можливо, рекомендується змінювати діяльність на не пов'язану з роботою на ПК.

Для уникнення негативного впливу монотонності рекомендується чергувати операції введення тексту та даних, змінюючи зміст та темп роботи.

Під час роботи з лазерними принтерами:

- розташовувати принтер поруч з системним блоком, уникати натягування з'єднувальних кабелів. Заборонено ставити принтер на системний блок;
- перевіряти, що принтер сполучений з системним блоком перед початком роботи;
- використовувати папір, вказаний в інструкції до принтера (зазвичай вагою 60-135 г/м2, типу Canon або Xerox 4024), для забезпечення якісного зображення без пошкоджень апаратури;
- обрізати краї паперу гострим ножем без заусенців для запобігання загинанню паперу;
- вимикати живлення відео монітора при тривалій роботі (понад 20 хвилин), коли втручання користувача не потрібне.

Для збереження тонусу м'язів та профілактики різних проблем, пов'язаних з роботою на ПК, рекомендується виконувати комплекси вправ для очей, спини та рук під час перерв.

Кількість та тривалість мікроперерв слід визначити індивідуально. Форма та характер перерв можуть бути різними, включаючи виконання альтернативних завдань, перекус, виконання рекомендованих вправ.

Рекомендується регулярно виконувати фізичні вправи протягом дня для корекції незручного положення та поліпшення кровообігу. Гімнастика повинна спрямовуватися на полегшення фіксованої пози та покращення кровопостачання.

У разі виявлення несправностей (іскріння, пробоїв, запаху гару, ознак горіння тощо) необхідно негайно зупинити роботу, відключити всю апаратуру від електромережі та негайно повідомити безпосереднього керівника або фахівця з ремонту ПК.

Вимоги безпеки під час завершення роботи на ПК:

Завершіть та збережіть файли, які використовувались під час роботи, у пам'яті ПК. Виконайте всі необхідні кроки для коректного завершення роботи в операційній системі.

Вимкніть принтер та інші зовнішні пристрої, а також вимкніть системний блок. Якщо є пристрій безперебійного живлення (ПБЖ), вимкніть його живлення.

Вимкніть ПК за допомогою кнопки «POWER» (ЖИВЛЕННЯ) та від'єднайте штепсель кабелю живлення від розетки.

Покрийте клавіатуру кришкою, щоб уникнути потрапляння пилу.

Наведіть лад на робочому місці.

Вимоги безпеки у випадку аварійних ситуацій:

Якщо після включення ПК ви відчуваєте запах горілого або відчуваєте електричний струм при доторканні до металевих деталей ПК, негайно відключіть ПК від електромережі та повідомте про це свого керівника.

У разі виникнення пожежі негайно розпочніть гасіння наявними засобами та повідомте за телефоном 101 (міська пожежна охорона) та начальнику ДПД підприємства. Пам'ятайте, що вогнегасники з вуглекислотою та сухим піском мають бути використані для загашення електроустановок, щоб уникнути ураження електричним струмом.

При отриманні травми зупиніть роботу, надайте першу медичну допомогу та викличте швидку медичну допомогу за телефоном 103. При необхідності доставте потерпілого до лікарського закладу.

Дотримуйтеся послідовності надання першої допомоги:

Позбавте організм впливу небезпечних та шкідливих чинників, які загрожують здоров'ю постраждалого (уникайте впливу електричного струму, виведіть з забрудненої атмосфери, загасіть горіння одягу тощо);

Визначте характер та важкість травми та найбільшу загрозу для життя постраждалого, а також заходи для його порятунку;

Виконайте необхідні заходи для порятунку постраждалого за терміновістю (відновіть прохідність дихальних шляхів, проведіть штучне дихання, зовнішній масаж серця, зупиніть кровотечу, іммобілізуйте місце перелому, накладіть пов'язку тощо);

Підтримуйте основні життєві функції постраждалого до прибуття медичного працівника;

Викличте швидку медичну допомогу або лікаря та вживайте заходів для транспортування постраждалого до найближчого лікарського закладу.

Допомогу постраждалому, надану не медичними працівниками, необхідно доповнити медичною допомогою та надавати лише до прибуття лікаря.

Конкретні дії з надання першої допомоги постраждалому при різних ураженнях описані в інструкції № 03-ОП «Про надання першої (долікарської) медичної допомоги при нещасних випадках», яку слід вивчити працівникам підприємства під час первинного та наступних інструктажів з питань охорони праці.

У випадку інших аварійних ситуацій припиніть роботу та повідомте про це керівника робіт.

На основі розрахунку повітрообміну за надлишком тепла, який склав 628 м3/год, було встановлено механічну вентиляцію з вентилятором VORTICE VARIO. Це було обрано через недостатню ефективність природної вентиляції. Механічна вентиляція може забезпечити виведення тепла з проєктного відділу при температурі 30°С та підтримувати температуру повітря на допустимому та оптимальному рівнях.

ВИСНОВОК ДО РОЗДІЛУ 5

В розділі "Охорона праці" кваліфікаційної роботи розглянуті основні аспекти забезпечення безпеки та здоров'я працівників у конкретній галузі та сфері діяльності. Досліджено та проаналізовано усі аспекти, пов'язані з організацією та забезпеченням безпеки праці, вживанням засобів індивідуального та колективного захисту, оцінкою ризиків, попередженням нещасних випадків та професійних захворювань. Важливо зазначити, що даний розділ має велике значення, оскільки належна організація та забезпечення безпеки праці сприяють збереженню здоров'я працівників та підвищенню ефективності їхньої праці. Врахування та впровадження відповідних нормативів та стандартів з охорони праці є невід'ємною складовою успішної та безпечної професійної діяльності.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день важко переоцінити важливість радіотехнічного та електронного виробництва, оскільки суспільство не може уявити своє повсякденне життя без нього. Електронна та радіотехнічна промисловість є високорозвиненою і грає ключову роль у науково-технічній революції. Впровадження електронних пристроїв у різні сфери людської діяльності істотно сприяє успішному вирішенню складних науково-технічних завдань, підвищує продуктивність фізичної та інтелектуальної праці, поліпшує економічні показники виробництва.

6.1. Аналіз впливу техногенних чинників

Широке впровадження електричного та електронного устаткування призвело до покращення якості життя людей, але також породило негативні наслідки для природи та здоров'я людини. Основні негативні та шкідливі впливи на навколишнє середовище включають:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення;
- теплове забруднення;
- радіаційне забруднення.

Шумове забруднення. В сучасному світі, охопленому науково-технічним прогресом, шум стає однією з прояв фізичного (хвильового) забруднення навколишнього природного середовища. Його визначають як всі неприємні та небажані звуки або їх сукупність, які перешкоджають нормальній працездатності, сприйманню потрібної звукової інформації та відпочинку.

Адаптація до шуму майже неможлива. Фоновий рівень шуму в навколишньому середовищі коливається в межах 30-60 децибел. Однак у сучасних умовах до цього природного фону додаються виробничі та транспортні шуми, рівень яких часто перевищує 100 децибел. Джерелами шуму є: промислові підприємства, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, масові зібрання людей та інше.

Умови роботи у шумних промислових об'єктах негативно впливають на працівників: вони розсіюють увагу, сприяють розвитку втоми, уповільнюють реакцію на небезпеку. Це впливає на загальну працездатність та збільшує ризик нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот для робочих місць у виробничих приміщеннях можна знайти в таблиці 6.1 [68]:

Таблиця 6.1.

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Досліджено, що рослини, впливані шумом, демонструють знижену енергію для зростання та виявляють надмірний випад вологи через листя, що може призвести до перебоїв у клітинах та вмирання. Листя та квіти рослин, що знаходяться близько до джерела інтенсивного шуму, гинуть. Для тварин, які спілкуються звуками та аналізують їх для отримання важливої інформації, відсутність шуму особливо важлива. Також шум впливає на тварин. Наприклад, личинки бджіл гинуть від шуму реактивного літака, а самі бджоли втрачають здатність орієнтуватися. В гніздах птахів шкаралупа яєць тріскається через шум. Коливання повітря, створені звуками переносної радіоапаратури, перешкоджають підняттю у повітря комах, таких як жуки та джмелі.

Вібраційне забруднення. Вібрація представляє собою рух твердого тіла, характеризуючийся механічними коливаннями. Її можна розбити на дві категорії: приро-

дну та штучну. Природні вібрації спричиняються природними явищами, зокрема землетрусами. Стосовно штучних вібрацій, їх джерелами є промисловість та транспорт. Тривалі експозиції вібраціями можуть серйозно вразити здоров'я людини, викликаючи від сильної втоми до розладів функцій організму, таких як порушення серцевої діяльності, нервової системи, спазми судин, деформація м’язів, або навіть струс мозку. Особливо небезпечні вібрації з частотою, яка співпадає з резонансною частотою коливання окремих органів або частин тіла людини, що може спричинити їх ушкодження. Продовжена експозиція вібраціям може призвести до професійного захворювання, відомого як вібраційна хвороба.

Електромагнітне забруднення. Біосфера пройшла та продовжує переживати вплив електромагнітного поля (ЕМП) природного походження, включаючи електричне та магнітне поля Землі та космічне електромагнітне випромінювання, особливо від Сонця. Унаслідок науково-технічного прогресу, людство почало створювати та все ширше використовувати антропогенні джерела ЕМП. Сучасні антропогенні ЕМП виявляються набагато сильнішими, ніж природні, та є значущим негативним фактором, вплив якого на людей та навколишнє середовище зростає щороку. Ефекти впливу ЕМП на організм людини залежать від діапазону частот, інтенсивності, тривалості опромінювання, характеру випромінювання (постійного чи модульованого), режиму опромінювання, розміру поверхні тіла, що піддане опромінюванню, та індивідуальних особливостей організму. Електромагнітні поля можуть спричиняти біологічні та функціональні порушення у функціонуванні організму. Функціональні ефекти проявляються у передчасній втомі, частих болях голови, погіршенні сну, порушенні функцій серцево-судинної та центральної нервової систем. Довготривалий та інтенсивний вплив ЕМП може призвести до стійких порушень та захворювань. Негативні біологічні ефекти впливу ЕМП проявляються у тепловій та нетепловій діях. Теплова дія призводить до підвищення температури тіла та місцевого вибіркового нагрівання органів і тканин організму через перетворення електромагнітної енергії в теплову. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією,

таких як головний мозок, очі, нирки, шлунок. Наприклад, випромінювання в сантиметровому діапазоні може спричинити катаракту, що призводить до поступової втрати зору.

Теплове забруднення. Теплове забруднення виникає внаслідок розсіювання теплоти в навколишнє середовище, що виробляється під час численних теплових процесів, переважно пов'язаних зі згорянням палива. Під час процесу згоряння палива, насамперед, утворюється тепло та викидається до 23% кисню, який був синтезований у процесі фотосинтезу на Землі протягом року. Згідно з розрахунками, під час спалювання вугілля у навколишнє середовище потрапляє більше радіоактивних компонентів, ніж усіма атомними електростанціями за той самий період при безаварійній роботі. Теплове забруднення гідросфери відбувається переважно через скидання у водойми підігрітих вод від теплових та атомних електростанцій та інших енергетичних об'єктів. Гаряча вода змінює термічні та біологічні режими водойм, негативно впливаючи на їхніх мешканців.

Радіаційне забруднення. До основних джерел радіаційного забруднення довкілля відносяться наступні:

• Уранова промисловість, яка включає видобування, переробку, збагачення та виготовлення ядерного палива.

• Ядерні реактори різних типів, у яких в активній зоні міститься значна кількість радіоактивної речовини. Ці реактори можуть бути атомними бомбами, а їхні процеси уповільнені до стаціонарного стану.

• Радіохімічна промисловість, де відбувається переробка та відновлення відпрацьованого матеріалу.

• Місця переробки та захоронення радіоактивних відходів, які, унаслідок неможливості забезпечити абсолютну ізоляцію джерела радіації, викидають радіонукліди у природне середовище.

• Використання радіонуклідів у вигляді закритих радіоактивних джерел невеликої потужності у промисловості, медицині, геології, сільському господарстві.

Основну загрозу для навколишнього середовища представляють техногенні радіонукліди, які утворюються під час випробувань ядерної зброї.

6.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач, також відомий як телевізійна приставка, є пристроєм, який приймає сигнал цифрового телебачення, розкодовує його і перетворює на аналоговий сигнал для виведення через роз'єми RCA або SCART, або у цифровий сигнал для виведення через роз'єм HDMI, передаючи його на телевізор.

Перехід до цифрового телебачення спричинив зростання виробництва цифрових абонентських приймачів, що в свою чергу може негативно позначитися на навколишньому середовищі. Абонентський приймач генерує слабкі електричні та магнітні змінні поля у широкому діапазоні частот. Однак особливу увагу слід звернути на проблему впливу електромагнітних випромінювань, які генеруються цими пристроями. Наукові дослідження показали, що електромагнітні випромінювання мають у своєму складі торсіонові поля, які є інформаційною компонентою будь-якого електромагнітного випромінювання. Дослідники з України виявили, що ці торсіонові поля можуть впливати на користувачів, особливо при наявності сучасних дисплеїв, які випромінюють електромагнітні хвилі.

Робоча група Всесвітньої організації охорони здоров'я з гігієнічних аспектів користування моніторами та радіотерміналами виявила порушення стану здоров'я при використанні пристроїв з електромагнітним випромінюванням. Найбільш серйозні з них включають погіршення зору, порушення імунної системи та вплив на психоемоційну сферу, такі як стресовий синдром та агресивність.

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002»[69]. Значення ГДР напруженості електричної ($Е_{гд}$) і магнітної ($Н_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 6.2.

Таблиця 6.2.

Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових

Час перебування персоналу, год	$E_{гд}$, В/м					$H_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

Електромагнітні випромінювання у діапазоні 30 кГц - 300 МГц (НЧ) можуть викликати різні негативні ефекти на організм людини. До цих ефектів відносяться загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в області серця. Особа може відчувати роздратування, втрату уваги та сповільнення рухових та мовних реакцій. Також можуть виникати симптоми, свідчущі про порушення роботи окремих органів, таких як шлунок, печінка та підшлункова залоза.

Для зменшення рівня електромагнітного випромінювання слід обмежити тривалість безперервної роботи абонентського приймача. Україна має норми електромагнітної безпеки, які регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання. Згідно з цими нормами, допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення складають 2,5 мкВт/см2.

Також абонентський приймач створює шум під час роботи, рівень якого становить 54 дБ. Для забезпечення норм звукового тиску важливо дотримуватися встановлених стандартів, де допустимий рівень звукового тиску складає 50 дБ.

Важливо враховувати, що велика кількість звукових сигналів, які надходять до кори головного мозку, може викликати стрес, передчасну втому та інші негативні ефекти. Шум може негативно впливати на центральну нервову систему, систему слуху, серцево-судинну систему, травний процес та інші органи та системи організму. Скарги на роздратування, переживання та порушення сну можуть бути першими проявами негативного впливу шуму на людину.

6.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу електромагнітних полів (ЕМП) на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, важливо вжити різні заходи, які можна розділити на організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи:

Органи санітарного нагляду повинні здійснювати санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи:

Розташування джерел ЕМП повинно мінімізувати їх вплив на працюючих.

Використання дистанційного керування апаратурою, що є джерелом випромінювання.

Екранування джерел випромінювання.

Використання засобів індивідуального захисту, таких як халати, комбінезони із металізованої тканини з виводом на заземлюючий пристрій.

Захист очей за допомогою захисних окулярів, які мають вбудовану захисну плівку для зменшення інтенсивності електромагнітної енергії при світлопропусканні.

Засоби індивідуального захисту слід використовувати тільки тоді, коли інші захисні засоби неможливі чи недостатньо ефективні, при проходженні через зони опромінення підвищеної інтенсивності, ремонтних та налагоджувальних роботах в аварійних ситуаціях, при короткочасному контролі та зміні інтенсивності опромінення.

Лікарсько-профілактичні заходи:

Проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП.

Обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань.

Видача працюючим безкоштовного лікарсько-профілактичного харчування.

Перерви санітарно-оздоровчого характеру.

Зазначені заходи спрямовані на зменшення впливу ЕМП на здоров'я персоналу та населення, забезпечення безпеки та здоров'я людей у зоні дії радіоелектронних засобів.

Захист від шуму. Так, для зменшення та ліквідації шуму застосовують цілий комплекс заходів, який називається шумозахистом. Ось деякі з них:

Використання звукопоглинаючих матеріалів:

Звукопоглинаючі матеріали дозволяють поглинати частину звукової енергії та зменшувати відбивання звуку.

Раціональне розміщення будівельних об'єктів:

Правильне планування та розміщення будівель може зменшити звукові впливи, особливо якщо об'єкти з найбільшим шумовим навантаженням знаходяться подалі від житлових зон.

Створення екранів:

Створення шумовідбиваючих екранів у вигляді земляних валів, стін та інших конструкцій, що допомагають знижувати рівень шуму.

Використання шумовідбиваючих конструкцій:

Використання спеціальних конструкцій, які відбивають звук та не допускають його поширення в певні області.

Використання шумовідбиваючих матеріалів у будівництві:

Використання матеріалів з високою шумовідбиваючою ефективністю для будівництва стін, підлог та дахів.

Технічні заходи:

Встановлення шумозахисних вікон, дверей, утеплення приміщень для поглинання звуку.

Ці заходи спрямовані на створення більш комфортних умов для проживання та роботи, а також збереження здоров'я людей у умовах шумного середовища.

Проблема електронних відходів. Подолання проблеми електронних відходів в Україні дійсно потребує комплексного підходу як в організаційно-правовому, так і в соціально-інформаційному аспектах. Ось кілька ключових напрямків для розв'язання цієї проблеми:

Регулююча та правова база:

Законодавче врегулювання та впровадження ефективних норм та стандартів для управління електронними відходами.

Впровадження та зміцнення відповідальності для виробників щодо обов'язкового збору та утилізації електронних відходів.

Організаційні заходи:

Створення фондів виробників для фінансування збору та утилізації електронних відходів.

Підтримка та розвиток підприємств, які спеціалізуються на утилізації відходів.

Соціально-інформаційні заходи:

Проведення освітніх кампаній для свідомого споживання та усвідомлення проблеми електронних відходів серед населення.

Розробка та впровадження інформаційних платформ для надання інструкцій щодо правильної утилізації електронних відходів та місць їх здачі.

Інновації та технології:

Розвиток та впровадження новітніх технологій утилізації електронних відходів з ефективним використанням ресурсів.

Важливо сприяти формуванню сталого способу споживання, збалансовано враховуючи інтереси споживачів, виробників та довкілля.

ВИСНОВОК ДО РОЗДІЛУ 6

Так, абонентські приймачі дійсно можуть створювати негативний вплив на навколишнє середовище через електромагнітне випромінювання та шумове забруднення. Для зменшення цього впливу та мінімізації ризику для здоров'я та навколишнього середовища можна застосовувати інженерно-технічні заходи, такі як екранування, правильне розташування антен та приймачів, а також використання засобів шумозахисту.

Управління електронними та електричними відходами є надзвичайно важливим завданням для збереження довкілля. Створення пунктів збору відходів електронного та електричного обладнання, які розташовані в зручних для населення місцях та надають послуги з утилізації цих відходів, сприяє відокремленню та належній обробці електронних відходів, що є дуже важливим для збереження природних ресурсів та запобігання забрудненню навколишнього середовища.

ВИСНОВКИ

У кваліфікаційній роботі за темою "Метод протидії відстеження та ідентифікації користувачів мережі Інтернет" було детально проаналізовано та досліджено важливі аспекти, пов'язані з приватністю, конфіденційністю та безпекою користувачів у сучасному цифровому середовищі.

У ході дослідження були розглянуті та вивчені основні методи та технології, спрямовані на запобігання відстеженню та ідентифікації користувачів у мережі Інтернет. Були досліджені алгоритми шифрування, використання віртуальних приватних мереж (VPN), методи анонімізації IP-адрес, а також інші технічні та організаційні засоби для забезпечення конфіденційності та безпеки користувачів.

Також були досліджені та проаналізовані правові аспекти захисту особистих даних у Інтернеті, зокрема, в контексті загального регламенту з питань захисту даних (GDPR) та інших відповідних стандартів.

Спроєктована система має й очевидні недоліки, найістотніший з яких - високі системні вимоги. Віртуальна машина з Windows 7 займає значний об'єм місця на жорсткому диску і в оперативній пам'яті, при тому що браузер Firefox (втім, як і Chrome) сам по собі споживає порівняно багато пам'яті, що призводить до необхідності виділяти віртуальній машині багато системних ресурсів, а це, відповідно, викликає брак пам'яті в основній системі. У результаті, швидкодія віртуальної машини - незадовільна. Далеко не кожен користувач матиме досить потужний ПК з великим запасом оперативної пам'яті.

Використовуваний ланцюжок "VPN через Tor", за всіх його переваг, можна визнати анонімним тільки за умови, що клієнту вдалося зберегти анонімність під час реєстрації та особливо під час оплати VPN-сервісу або VPS-хостингу. Для цього, вочевидь, він уже повинен володіти надійним інструментом анонімізації - отже, такий клієнт може просто не потребувати додаткових заходів захисту.

Результати дослідження підтверджують, що питання захисту особистої інформації та приватності користувачів у мережі Інтернет мають велике значення та потребують постійного вдосконалення методів та технологій. Висновки роботи служать основою для подальшого вдосконалення заходів та стратегій захисту конфіденційності та безпеки в онлайн середовищі з урахуванням сучасних викликів та тенденцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. O. Fajana, G. Owenson and M. Cocea, "TorBot Stalker: Detecting Tor Botnets Through Intelligent Circuit Data Analysis," 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2018, pp. 1-8.
2. N. Mandela, A. A. S. Mahmoud and A. K. Agrawal, "A Forensic Analysis of the Tor Network in Tails Operating system," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 546-551.
3. M. Traudt, R. Jansen and A. Johnson, "FlashFlow: A Secure Speed Test for Tor," 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), DC, USA, 2021, pp. 381-391.
4. L. Chiaraviglio et al., "Measuring EMF and Throughput Before and After 5G Service Activation in a Residential Area," in IEEE Open Journal of the Communications Society, vol. 4, pp. 1179-1195.
5. J. Jin and X. Wang, "On the effectiveness of low latency anonymous network in the presence of timing attack," 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, Lisbon, Portugal, 2009, pp. 429-438.
6. W. Shao and Q. Chen, "Rotationally Reconfigurable Single-Element Prism for Enhancing Scanning Flexibility of Risley Prism Antenna System," in IEEE Antennas and Wireless Propagation Letters, vol. 22, no. 3, pp. 507-511, March 2023.
7. V. Sucasas, G. Mantas, M. Papaioannou and J. Rodriguez, "Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 168-184, 1 Jan.-March 2023.
8. W. Oogami, T. Komura and Y. Okabe, "Secure ID Transformation for Robust Pseudonymity against Backflow of Personal Information in SAML Federation,"

2012 IEEE 36th Annual Computer Software and Applications Conference Workshops, Izmir, Turkey, 2012, pp. 64-69.

9. S. Roy, C. Pani and S. Bera, "Design and Performance Analysis of Electro Optic ToR(EO-ToR) for Low Latency Data Center Network," 2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE), Shillong, India, 2023, pp. 1-6.
10. Y. D. Mane and U. P. Khot, "A Systematic Way to Implement Private Tor Network with Trusted Middle Node," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-6.
11. A. Khajehpour, F. Zandi, N. Malekghaini, M. Hemmatyar, N. Omidvar and M. J. Siavoshani, "Deep Inside Tor: Exploring Website Fingerprinting Attacks on Tor Traffic in Realistic Settings," 2022 12th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, Islamic Republic of, 2022, pp. 148-156.
12. C. A. Caldeira, O. A. de O. Souza, O. Goussevskaia and S. Schmid, "OpticNet: Self-Adjusting Networks for ToR-Matching-ToR Optical Switching Architectures," IEEE INFOCOM 2023 - IEEE Conference on Computer Communications, New York City, NY, USA, 2023, pp. 1-10.
13. J. Lingyu, L. Yang, W. Bailing, L. Hongri and X. Guodong, "A hierarchical classification approach for tor anonymous traffic," 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), Guangzhou, China, 2017, pp. 239-243.
14. Y. Jin, K. Kakoi, M. Tomoishi and N. Yamai, "Efficient detection of suspicious DNS traffic by resolver separation per application program," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2017, pp. 87-92.
15. S. Ding, D. Zhang, J. Ge, X. Yuan and X. Du, "Encrypt DNS Traffic: Automated Feature Learning Method for Detecting DNS Tunnels," 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing,

Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), New York City, NY, USA, 2021, pp. 352-359.

16. G. Goth, "Privacy Gets a New Round of Prominence," in IEEE Internet Computing, vol. 15, no. 1, pp. 13-15, Jan.-Feb. 2021.
17. A. Bremler-Barr, S. T. David, D. Hay and Y. Koral, "Decompression-free inspection: DPI for shared dictionary compression over HTTP," 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 2022, pp. 1987-1995.
18. N. I. Daud, G. R. Haron and S. S. S. Othman, "Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor," 2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Langkawi, Malaysia, 2017, pp. 152-156.
19. M. S. Prathima, S. P. Milena and P. Rm, "Imposter detection with canvas and WebGL using Machine learning.," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-6.
20. Y. Zheng, J. Liu and S. Zhang, "An infringement detection system for videos based on audio fingerprint technology," 2020 International Conference on Culture-oriented Science & Technology (ICCST), Beijing, China, 2020, pp. 308-312.
21. D. Kim, H. -I. Kim and W. Woo, "Mutual Space Generation with Relative Translation Gains in Redirected Walking for Asymmetric Remote Collaboration," 2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), Singapore, Singapore, 2022, pp. 674-677.
22. A. Abouollo and S. Almuhammadi, "Detecting malicious user accounts using Canvas Fingerprint," 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2017, pp. 358-361.
23. I. Dolnák, "Implementation of referrer policy in order to control HTTP Referer header privacy," 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stary Smokovec, Slovakia, 2017, pp. 1-4.

24. S. Sureshkumar, "Classification of DDoS Attacks and Flash Events using Source IP Entropy and Traffic Cluster Entropy," 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2021, pp. 1-5.
25. K. Sasaki, M. Hanai, K. Miyazawa, A. Kobayashi, N. Oda and S. Yamaguchi, "TCP Fairness Among Modern TCP Congestion Control Algorithms Including TCP BBR," 2018 IEEE 7th International Conference on Cloud Networking (CloudNet), Tokyo, Japan, 2018, pp. 1-4.
26. N. Fukuda and H. Nakazato, "Hash-Collecting System : Applying Freenet Routing Method to Named Data Networking," 2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN), Paris, France, 2022, pp. 91-95.
27. S. Salsano, P. L. Ventre, L. Prete, G. Siracusano, M. Gerola and E. Salvadori, "OSHI - Open Source Hybrid IP/SDN Networking (and its Emulation on Mininet and on Distributed SDN Testbeds)," 2014 Third European Workshop on Software Defined Networks, Budapest, Hungary, 2014, pp. 13-18.
28. N. K. Jadav, R. Gupta and S. Tanwar, "AI and Onion Routing-based Secure Architectural Framework for IoT-based Critical Infrastructure," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 559-564.
29. Y. Chen, Y. Su, M. Zhang, H. Chai, Y. Wei and S. Yu, "FedTor: An Anonymous Framework of Federated Learning in Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18620-18631, 1 Oct.1, 2022.
30. J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko and K. Wehrle, "Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments," 2019 IEEE 27th International Conference on Network Protocols (ICNP), Chicago, IL, USA, 2019, pp. 1-12.
31. D. Marks, F. Tschorsch and B. Scheuermann, "Unleashing Tor, BitTorrent & Co.: How to relieve TCP deficiencies in overlays," IEEE Local Computer Network Conference, Denver, CO, USA, 2020, pp. 320-323.

32. A. Abdelbari, "MDA: Multiple Decentralized Anchors for Hiding Communication Information," 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2022, pp. 591-596.
33. C. Wang, Z. Ling, W. Wu, Q. Chen, M. Yang and X. Fu, "Large-scale Evaluation of Malicious Tor Hidden Service Directory Discovery," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, London, United Kingdom, 2022, pp. 1709-1718.
34. A. Sanatinia and G. Noubir, "Honey Onions: A framework for characterizing and identifying misbehaving Tor HSDirs," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 2019, pp. 127-135.
35. S. Narayan, C. J. Williams, D. K. Hart and M. W. Qualtrough, "Network performance comparison of VPN protocols on wired and wireless networks," 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2019, pp. 1-7.
36. Z. Wu and M. Xiao, "Performance Evaluation of VPN with Different Network Topologies," 2019 IEEE 2nd International Conference on Electronics Technology (ICET), Chengdu, China, 2019, pp. 51-55.
37. W. Wu, T. Yan, W. Cao and H. Li, "Research on the application of cross-domain VPN technology based on MPLS BGP," 2022 6th International Conference on Wireless Communications and Applications (ICWCAPP), Haikou, China, 2022, pp. 151-155.
38. I. Plotog, G. Varzaru, C. Turcu, T. C. Cucu, P. Svasta and N. D. Codreanu, "VPS solution for lead-free soldering in EMS industries," 2018 2nd Electronics System-Integration Technology Conference, Greenwich, UK, 2018, pp. 121-124.
39. W. KeHe, Z. Peng, C. WenChao, Z. XianKang and C. AJun, "Tunneling SSL VPN Based on PF_RING," 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2019, pp. 1-4.
40. H. Sasanuma, H. Tsukagoshi and M. Okui, "Socks Type Actuator That Provides Exercise for Ankle and Toes from the Medical Point of View," 2018 IEEE/ASME

International Conference on Advanced Intelligent Mechatronics (AIM), Auckland, New Zealand, 2018.

41. G. D'Addio et al., "Development of a Prototype E-Textile Sock," 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Berlin, Germany, 2019, pp. 17498-1752.
42. P. Lugoda et al., "Classifying Gait Alterations Using an Instrumented Smart Sock and Deep Learning," in IEEE Sensors Journal, vol. 22, no. 23, pp. 23232-23242, 1 Dec.1, 2022.
43. Y. D. Mane and U. P. Khot, "A Systematic Way to Implement Private Tor Network with Trusted Middle Node," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-6.
44. L. Zhang, Y. Zhou and J. Fan, "The forensic analysis of encrypted Truecrypt volumes," 2019 IEEE International Conference on Progress in Informatics and Computing, Shanghai, China, 2019, pp. 405-409.
45. A. Kazim, F. Almaeeni, S. A. Ali, F. Iqbal and K. Al-Hussaeni, "Memory Forensics: Recovering Chat Messages and Encryption Master Key," 2019 10th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2019, pp. 58-64.
46. N. Mandela, A. A. S. Mahmoud and A. K. Agrawal, "A Forensic Analysis of the Tor Network in Tails Operating system," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 546-551.
47. D. Han et al., "Cutting Onions With Others' Hands: A First Measurement of Tor Proxies in the Wild," 2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain, 2023, pp. 1-9.
48. A. I. Levin and I. A. Voronov, "The investigation of the possibility of automated collection of information in the hidden segment of the Internet," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow and St. Petersburg, Russia, 2018, pp. 66-68.

49. M. Zhang and S. Zonouz, "Use-After-Free Mitigation via Protected Heap Allocation," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 2018, pp. 1-8.
50. A. Buchet, P. Snyder, H. Haddadi and C. Pelsser, "Detecting IP-tracking proof interfaces by looking for NATs," 2023 7th Network Traffic Measurement and Analysis Conference (TMA), Naples, Italy, 2023, pp. 1-4.
51. B. Gulmezoglu, "XAI-Based Microarchitectural Side-Channel Analysis for Website Fingerprinting Attacks and Defenses," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 4039-4051, 1 Nov.-Dec. 2022.
52. J. P. Podolanko, R. Pobala, H. Mucklai, G. Danezis and M. Wright, "LiLAC: Lightweight Low-Latency Anonymous Chat," 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 2017, pp. 141-151.
53. M. Side, F. Yao and Z. Zhang, "LockedDown: Exploiting Contention on Host-GPU PCIe Bus for Fun and Profit," 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 2022, pp. 270-285.
54. B. Shanmugam, S. Azam, K. C. Yeo, J. Jose and K. Kannoorpatti, "A critical review of Bitcoins usage by cybercriminals," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2017, pp. 1-7.
55. M. Traudt, R. Jansen and A. Johnson, "FlashFlow: A Secure Speed Test for Tor," 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), DC, USA, 2021, pp. 381-391.
56. J. A. Stone, N. Saxena and H. Dogan, "Systematic Analysis: Resistance to Traffic Analysis Attacks in Tor System for Critical Infrastructures," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 2018, pp. 2832-2837.
57. M. J. Ryan, M. Chowdhury, F. Jiang and R. R. Doss, "Avoiding Geographic Regions in Tor," 2020 IEEE 19th International Conference on Trust, Security and

Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 802-809.

58. P. Blanco-Medina, E. Fidalgo, E. Alegre and F. Jáñez-Martino, "Improving text recognition in Tor darknet with rectification and super-resolution techniques," 9th International Conference on Imaging for Crime Detection and Prevention (ICDP-2019), London, UK, 2019, pp. 32-37.
59. S. M. M. Monterrubio, J. E. A. Naranjo, L. I. B. López and Á. L. V. Caraguay, "Black Widow Crawler for TOR network to search for criminal patterns," 2021 Second International Conference on Information Systems and Software Technologies (ICI2ST), Quito, Ecuador, 2021, pp. 108-113.
60. W. Kim, J. Kim, H. -S. Kim, S. -J. Lee and D. Yoon, "A Study on the Driver's Response Performance according to Modality of Planned TOR in Automated Driving," 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2019, pp. 1471-1473.
61. ДСанПіН 3.3.2-007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»
62. ГН 3.3.5-8-6.6.1-2002 «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу»
63. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»
64. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення»
65. НПАОП 0.00-1.29-97 «Правила захисту від статичної електрики»
66. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони»
67. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом»
68. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги»

69. НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні»
70. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.
71. Клап Я. А., Яремкевич О. С., Червецова В. Г., Заярнюк Н. Л., Новіков В. П., Дослідження впливу електромагнітних, постійних магнітних та акустичних полів на організм людини // Вісник Нац. ун-ту "Львівська політехніка". – 2016 – № 812. – С. 365–372.
72. Сучасний стан досліджень впливу електромагнітних випромінювань на організм людини [Електронний ресурс]/[А. П. Чорний, В. В. Никифоров, Д. І. Родькін, В. Ю. Ноженко] // Інженерні та освітні технології в електротехнічних та комп'ютерних системах: щоквартальний науково-практичний журнал. – Кременчук: КрНУ, 2013.
73. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.
74. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.

ДОДАТОК А
ВМІСТ ФАЙЛУ КОНФІГУРАЦІЇ СЕРВЕРА OPENVPN

```
port 443
proto tcp
dev tun
server 10.[redacted].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.[redacted].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-SHA256:
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
remote-cert-tls client
tls-server
status-version 2
script-security 2
sndbuf 39[redacted]16
rcvbuf 39[redacted]16
reneg-sec 2592000
hash-size 1024 1024
verb 3
mute 3
replay-window 128
compress
log /dev/null
```

ДОДАТОК Б
ВМІСТ ФАЙЛУ КОНФІГУРАЦІЇ КЛІЄНТА OPENVPN

```
client
dev tun
dev-type tun
remote 185.[redacted].27.[redacted] 443 tcp
nobind
persist-tun
cipher AES-256-GCM
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256:
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 39[redacted]16
rcvbuf 39[redacted]16
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>
```