Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Скорохода Максима Сергійовича*

академічної групи *125м-22-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи протидії відстеженню та ідентифікації користувачів інтернету*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доцент Сафаров О.О.	85	добре	
розділів:				
спеціальний	асистент Мілінчук Ю.А.	85	добре	
економічний	к.е.н., доц. Пілова Д.П.	92	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Скороходу Максиму Сергійовичу* **академічної групи** *125м-22-3*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи протидії відстеженню та ідентифікації користувачів інтернету*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ ___

Розділ	Зміст	Термін виконання
Розділ 1	Проблематика збереження анонімності та приватності	02.12.2023
Розділ 2	Спеціальна частина	16.12.2023
Розділ 3	Економічна частина	30.12.2023

Завдання видано _____ Мілінчук Ю.А.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Скороход М.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота містить 107 с., 16 рис., 1 табл. 54 джерела.

Об'єктом дослідження є сучасні методи та засоби забезпечення анонімності та протидії відстеженню користувачів при роботи з Інтернет-ресурсами.

Мета роботи – забеспечення анонімності під час роботи в мережі Інтернет поєднануючи такі якості, як безпека, зручність та непомітність. У процесі дослідження проводилися: збір та аналіз актуальної теоретичної інформації, вивчення аналогів, проектування практичного рішення, експерименти щодо перевірки його ефективності.

Основні конструктивні, технологічні та техніко експлуатаційні методи: реалізується приховування та підміна даних про користувачеві, шифрування та обфускація трафіку, маскування наявності коштів анонімізації, ізоляція веб-браузера від основної системи, захист від випадкових витоків реальних даних.

В результаті дослідження був підібраний, налаштований та протестований комплекс програмного забезпечення, що вирішує поставлені завдання найкращим чином.

Область застосування: різна, схожа із застосуванням Tor Browser та інших популярних інструментів забезпечення анонімності. Економічна ефективність/значущість роботи: використовується тільки безкоштовне та переважно відкрите ПЗ, єдиними витратами на проектом була оренда недорогого віртуального сервера для тестів VPN.

В економічному розділі визначено капітальні витрати на програмні розробки.

У майбутньому планується подальше покращення отриманої збірки з метою автоматизації деяких функцій та підвищення зручності роботи.

ІНФОРМАЦІЙНА БЕЗПЕКА, АНОНІМНІСТЬ, ЗАХИСТ ВІД ВІДСТЕЖЕННЯ, ШИФРУВАННЯ, ІНТЕРНЕТ.

ABSTRACT

Qualification work 107 p., 16 fig., 1 tab. 54 sources.

The object of research is modern methods and methods for ensuring the anonymity and prevention of corruption while working with Internet resources.

Meta work - to ensure anonymity while working on the Internet by combining such qualities as security, convenience and invisibility. The follow-up process included: selection and analysis of relevant theoretical information, development of analogues, designing a practical solution, experiments to re-verify its effectiveness.

The main constructive, technological and technical operational characteristics: the implementation of capturing and maintaining data about the data, encryption and obfuscation of traffic, masking the visibility of the code in anonymization, isolation of the web browser from the main data in the real systems, protection

As a result of the follow-up of the subdivisions, the implementation and protests of the software security complex, which violated the orders of the highest rank.

Steps in the development: a software test suite for installing and testing, launching the VPN server successfully wins for recognition.

Staging area: cost similar to those of Tor Browser and other popular anonymity security tools. Economical efficiency/significance of work: only cost-free and more importantly open software, the only project was to rent an inexpensive virtual server for VPN testing.

In the economic section the capital costs of establishing developed programs have been calculated.

In the future, it is planned to further reduce the omission of the collection with the method of automation of certain functions and the improvement of the efficiency of work.

INFORMATION SECURITY, ANONYMITY, PROTECTION OF INFORMATION, ENCRYPTION, INTERNET.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

DPI – Deep Packet Inspection (система глибокого аналізу пакетів).

SSH – Secure Shell (безпечна оболонка), протокол віддаленого доступу.

TLS – Transport Layer Security (Протокол захисту транспортного рівня).

VPN – Virtual Private Network (віртуальна приватна мережа).

VPS – Virtual Private Server (віртуальний приватний сервер).

ВМ – віртуальна машина.

ПЗ – програмне забезпечення.

ЗМІСТ

ВСТУП

Проблема приватності в цифровому світі стає все більш складною, і захист особистої інформації вимагає постійного удосконалення технологій та стратегій. Розвиток і впровадження ефективних методів захисту відстеження і приховування особистої інформації є критичним завданням для забезпечення приватності і безпеки користувачів у цифровому середовищі.

На сьогоднішній день існує проблема створення та використання програмних засобів, які забезпечують анонімність та захист від відстеження під час роботи в Інтернеті. Значна кількість подібних інструментів таких як VPN-сервіси разом з різними "анонімайзерами" стають все популярнішими. Проте, практично всі вони мають свої недоліки.

По-перше, забезпечення максимальної анонімності є складним завданням, оскільки воно включає багато факторів, і багато сервісів можуть вирішувати це завдання лише частково. Навіть мережа TOR, яка часто рекламується як найбезпечніша, не завжди гарантує повну анонімність. Деякі VPN-провайдери також можуть зберігати історію дій користувача та відстежувати його, що може бути передано державним службам.

По-друге, використання таких інструментів часто зводить на низьку швидкість з'єднання та обмеження функціональності браузера. Для надійного захисту може знадобитися відключення деяких функцій, які можуть призвести до витоку даних, але це може ускладнити роботу на багатьох сайтах. Насамперед сюди належить відключення JavaScript та заборона прийому Cookies.

По-третє, сам факт використання анонімізації може бути помічений та викликати увагу до користувача, що може ускладнити його роботу. Наприклад, деякі сайти можуть обмежувати доступ з IP-адрес TOR, існують фактори, які дозволяють зовнішньому спостерігачеві визначити, що користувач намагається приховати свою особистість. Таким чином, непомітність, скритність є ще

одним важливим параметром надійного засобу анонімізації, але більшість існуючих рішень це не забезпечують.

Нарешті, не всі інструменти або схеми забезпечення мережевої анонімності є простими у використанні, особливо якщо вони повинні бути зрозумілі для будь-якого користувача, а не лише для експерта в цій галузі. Забезпечення мережевої анонімності вимагає розуміння принципів та деталей налаштування.

Дослідження має на меті оцінку та вивчення можливостей створення засобу анонімізації, який би ефективно поєднував надійність, зручність, непомітність використання та простоту налаштування. Задачі включають збір та аналіз інформації про існуючі засоби анонімізації, вивчення факторів відстеження користувача в мережі, аналіз можливих витоків даних та розробку рекомендацій для технічної анонімізації та правил поведінки.

У ході дослідження вирішуються такі завдання:

- збір та аналіз інформації про засоби та методи забезпечення анонімності в Інтернеті, актуальних на даний час;
- конкретизація та аналіз факторів, за якими можливо відстеження користувача під час роботи в мережі;
- аналіз шляхів витоку даних, що призводить до порушення анонімності;
- складання рекомендацій щодо технічної анонімізації та правил поведінки для різних моделей загроз.

Теоретична значущість роботи полягає у систематизації та узагальненні інформації про анонімність в Інтернеті.

Практична значущість роботи виявляється в розв'язанні проблем анонімності в Інтернеті та протидії цензурі та відстеженню.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Потреба у забезпеченні анонімності та захисту від відстеження

Проблема забезпечення конфіденційності в Інтернеті існує з моменту виникнення Всесвітньої мережі, але отримала особливу актуальність по всьому світу у 2013 році, коли Е. Сноуден розкрив правду щодо програм глобального стеження, таких як американська система PRISM та інших комплексів таємного масового збирання даних. Навіть тоді цю ситуацію визнали безпрецедентним вторгненням у приватне життя громадян. Щодо України, на сьогодні проблеми стеження та інтернет-цензури стають дедалі більш актуальними, навіть без урахування діяльності зарубіжних організацій. За оцінкою Фонду «Freedom House», Україна вже не вважається країною з вільним інтернетом [5].

Початково Інтернет існував як "територія свободи". Проте зараз бажання держави та деяких комерційних структур "знати все" про кожного користувача мережі призвело до необхідності реальної боротьби за недоторканність особистих даних. Сам факт наявності стеження викликає дратування, незалежно від того, яку саме активність в Мережі здійснює користувач – чи це незаконна, чи абсолютно легальна діяльність [6]. Право на приватність є однією з фундаментальних прав сучасної людини, включаючи його в інтернеті.

В першу чергу розглянемо сутність поняття анонімності. У контексті використання Інтернету, анонімність означає неможливість встановлення зв'язку між активністю користувача та його реальною особистістю та місцезнаходженням. Проте слід визначити формальну різницю між повною анонімністю та "псевдонімом" (іноді використовується терміни "anonymity" та "pseudonymity" відповідно). Анонімне підключення до сервера передбачає, що сервер не може визначити початкове походження (реальний IP-адреса клієнта) та пов'язати його з будь-яким ідентифікатором. У випадку наявності будь-якого

ідентифікатора (наприклад, кукі-файлу, унікального відбитка браузера і т.д.), за допомогою якого сервер може визначити, що клієнт підключався раніше, ми вже можемо говорити про "псевдонімність" [7]. Фактично, у багатьох випадках цього вже достатньо, існує необов'язковість робити кожне підключення абсолютно унікальним. Тим не менше, при тривалому використанні одного й того ж "псевдоніму" накопичується профільна інформація про активність, тому його рекомендується періодично змінювати, щоб уникнути втрати анонімності користувача.

Можна помилково припустити, що анонімність пов'язана з повністю відсутнім набором даних про користувача. Проте в деяких випадках це є або неможливим, або недоцільним. Наприклад, власний IP-адрес можна приховати під час відвідування веб-сайту, але технічно неможливо забезпечити повну відсутність IP-адреси (і при цьому отримати необхідний контент). Тобто IP-адреса, в кінцевому підсумку, не може бути абсолютно відсутньою, її можна лише замаскувати. Інший приклад - "User-agent" браузера. Хоча його можна замінити порожнім рядком, це недоцільно. Такий браузер вирізнятиметься серед інших і втратить анонімність, перетворившись на особливий та унікальний. Крім того, багато веб-сайтів можуть некоректно працювати з таким браузером. Важливо відзначити, що "User-agent" сам по собі не є унікальним і не може однозначно ідентифікувати або відстежувати користувача. Проте поєднання великої кількості "неунікальних" даних часто формує унікальний цифровий відбиток.

У травні 2015 року Рада з прав людини ООН оприлюднила звіт про засідання, приурочене обговоренню анонімності та шифрування в мережі Інтернет [8]. Основний висновок цього документа полягає в тому, що можливість анонімного користування Інтернетом та використання шифрування особистих даних та комунікацій повинні розглядатися як необхідна інтегральна частина прав людини. Навіть при тому, що засоби анонімізації часто використовуються зловмисниками, можливість бути анонімним в Інтернеті визнається як засіб, який може мати різні цілі та мотивації. Незважаючи на це,

існує думка, що "звичайному законослухняному користувачеві" анонімність просто не потрібна, оскільки немає потреби щось приховувати від держави, а її діяльність в Інтернеті нікого не цікавить [9]. Важливо відзначити, що факт збору даних сам по собі не усувається, і відстеження користувачів здійснюють як спецслужби, так і багато інтернет-компаній (наприклад, "Google" - один з наочних прикладів), а також більшість веб-сайтів [10]. Історія дій користувача в Інтернеті вважається особистою інформацією і не призначена для сторонніх очей, так само, як і особисте листування. Позиція "мені нема чого приховувати" фактично вказує на "мене не турбує недоторканність мого приватного життя". Розробники "TOR" дотримуються принципу "можливо, це і не секрет, але це просто не ваша справа". У цьому контексті американський юрист Г. Грінвальд висловився особливо образливо в 2014 році:

«Останні 16 місяців, що я обговорював цю тему по всьому світу, кожен що казав мені: «Я не особливо турбуюся з приводу вторгнення в особисту життя, тому що мені нема чого приховувати». Я завжди відповідаю їм однаково. Я дістаю ручку, пишу адресу своєї електронної пошти та кажу: «Ось моя пошта. Я хочу, щоб ви, прийшовши додому, відправили мені паролі до всіх ваших облікових записів, не тільки до банальної, пристойної робочої пошти, але до всіх, тому що я хотів би мати можливість покопатися в тому, що ви робите онлайн, почитати, що захочу, опублікувати те, що здасться мені цікавим. І 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 її надзвичайну важливість» [11].

Зрештою, для деяких осіб анонімність є необхідною внаслідок специфіки їхньої діяльності. Наприклад, показовим є використання "Tor" у легальних цілях. Корпорації використовують його як безпечний засіб для проведення аналізу на конкурентному ринку та як доповнення до віртуальної приватної

мережі (VPN). Журналісти можуть використовувати "Tor" для безпечного спілкування з інформаторами та дисидентами, а соціальні працівники – для взаємодії з урахуванням особливостей соціальної сфери на чатах та веб-форумах для біженців та жертв насильства. Нурядові організації використовують "Tor" для підключення своїх співробітників до необхідних сайтів під час закордонних відряджень, коли важливо не розголошувати їхню роботу. Деякі громадські організації рекомендують "Tor" для забезпечення безпеки своїх членів. Спецслужби використовують "Tor" для забезпечення конфіденційності під час виконання особливих завдань. Громадянські активісти з Фонду електронних рубежів (EFF) підтримують розробку "Tor", оскільки вбачають у ньому засіб для захисту базових цивільних прав та свобод в Інтернеті[12].

1.2. Збереження анонімності: можливості та методи

В сучасному світі надійна інтернет-анонімність може бути актуальною для практично будь-якої особи. Однак рівень безпеки, який вважається достатнім, варіюється в залежності від конкретних потреб користувачів. Наприклад, для одних осіб життєво важливо залишатися невидимими, тоді як для інших це може бути просто засобом отримати доступ до блокованих веб-сайтів. Вибір методу забезпечення анонімності розпочинається з чіткого визначення, для чого саме потрібна ця анонімність. EFF (Електронні рубежі) пропонує п'ять основних питань для моделювання загроз під час захисту персональних даних:

1. Що ви хочете захистити?
2. Від кого ви плануєте це захищати?
3. Яка ймовірність того, що вам доведеться це захищати?
4. Які можливі наслідки, якщо ви зазнаєте невдачі?
5. Які ресурси ви готові витратити на запобігання цим наслідкам?

Ідеальна безпека неможлива, і кожне рішення включає в себе певний компроміс. На думку деяких, анонімності в Інтернеті не існує, але можливо забезпечити анонімну роботу в Інтернеті за необхідності. При цьому важливо пам'ятати:

1. Постачальники Інтернету або власники точок доступу Wi-Fi часто можуть моніторити значну частину трафіку, але, як правило, не мають зацікавленості в активному відстеженні та деанонімізації користувача. Щодо власників використовуваних ресурсів, таких як веб-сайти, проксі/VPN-сервери, вони мають різноманітні інструменти для відстеження, такі як відплив DNS, Flash плагіни, банерні мережі, різні "відбитки браузера" та різні види куки (cookies). Зазвичай вони також мають суттєвий комерційний інтерес в ефективному відстеженні користувачів для цілей таргетування реклами та продажу даних. Уряд та спецслужби можуть отримувати доступ до даних, які зібрані веб-сайтами, а також до інформації, яка зберігається у постачальниках Інтернет-послуг. Таким чином, ті, хто мають можливість та бажання відстежувати користувачів, можуть мати доступ до більшості можливих каналів витоку особистої інформації.

2. Витік інформації може статися за допомогою різних методів, таких як раптове відключення від VPN, визначення реального IP через WebRTC або Flash-плагіни браузера, а також відправка серійного номера програмного забезпечення при спробі оновлення. Притому регулярно виявляються нові шляхи витоку, і нові методи постійно з'являються. Таким чином, спроба блокувати кожен із цих методів окремо, використовуючи унікальні для кожного з них заходи, може бути неефективною, оскільки завжди існує можливість, що з'явиться новий спосіб витоку, який не був врахований. Це підкреслює потребу в комплексному підході до захисту приватності та конфіденційності в мережі, який включає в себе не лише технічні заходи, а й правильне навчання користувачів, використання надійних засобів шифрування, анонімізації та

безпеки, а також постійне оновлення методів захисту для врахування нових викликів і загроз.

3. Вихід до мережі Інтернет може бути здійснений за допомогою різних пристроїв та паралельно супроводжуватися роботою різного роду додатків, месенджерів, клієнтів тощо. При цьому інформація, що передається за допомогою означених каналів часто перетинається і дозволяє зв'язати їх між собою (.torrent файл, завантажений з сайту, завантажується в торрент-клієнт, посилання в листі/повідомленні що відкривається у браузері тощо). Додамо до цього те, що сама ОС і багато програм регулярно з'єднуються з мережею для пошуку оновлень та з інших причин, передаючи різну інформацію, яка також може виявитися ідентифікуючою [14].

Отже, часткова "анонімність" насправді не є повноцінною анонімністю. Вона може бути достатньою для вирішення деяких завдань, але є майже безплідною в ситуаціях, де необхідна дійсно повна анонімність. Розуміється, що жодна схема не може бути абсолютно надійною, і, крім того, деанонімізація часто відбувається через помилки у поведінці самого користувача - аспекти соціальної анонімності не можна забезпечити технічними методами. Соціальна інженерія завжди залишається ефективною. Рекомендації щодо анонімної поведінки також будуть розглянуті далі, проте основною темою дослідження є технічна анонімність - те, що залишається в межах можливостей програмного забезпечення.

Захист від відстеження має свої технічні обмеження, оскільки блокування його можливе не завжди. З одного боку, багато веб-сайтів використовують відстежувальні елементи[10], сторонні трекери для реклами, аналітики та інших маркетингових інструментів; в даний час популярні браузерні розширення для "захисту від відстеження" - більшість таких трекерів можна дійсно заблокувати. З іншого боку, всі підключення до сервера фіксуються в логах, тому факт відвідування сайту буде зафіксовано незалежно від рівня анонімності клієнта. Наприклад, якщо провайдер може прослуховувати весь трафік, то використання VPN не впливає на процес перехоплення, хоча і робить його менш ефективним.

Таким чином, правильніше говорити не про захист від відстеження, а про захист конфіденційності даних в умовах відстеження. Виключити відстеження повністю неможливо.

1.3. Ідентифікація та відстеження

1.3.1. Основні шляхи витоку даних

1) IP-адреса є одним з найбільш простих способів відстеження та ідентифікації, оскільки надає можливість визначити провайдера та подальше встановлення геолокації самого користувача. Навіть за умови використання різних анонімайзерів, IP-хост, наданий провайдером, залишається незмінним.

2) провайдер DNS - у певних випадках запити DNS можуть виконуватися поза каналом, що використовується для анонімізації користувача, обходячи анонімний канал.

3) Атаки профілювання. Суть вказаного методу ідентифікації та відстеження полягає в тому, що інформація, яка протягом тривалого періоду часу подається до мережі Інтернет через один вузол, може бути розкрита через інші канали, внаслідок чого встановлюється зв'язок між конкретною діяльністю та відповідним псевдонімом [15].

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

5) Використання двох каналів (відкритого та закритого) для синхронного підключення до сервера може стати фактором, що сприяє ідентифікації користувача в разі розірвання інтернет-з'єднання через порівняння часу від'єднання користувачів на сервері.

6) Виявлення інформації про конкретного користувача в анонімному сеансі може включати в себе використання публічних сервісів, на яких вже міститься інформація про цього користувача.

7) MAC-адреса - це унікальний ідентифікатор, складений із шести пар шістнадцяткових цифр, і використовується для ідентифікації обладнання в комп'ютерних мережах.

8) Інформація із браузерів уособлює значну та громіздську категорію методів, за допомогою яких можна здійснити відстеження та ідентифікувати користувача і потребує більш детального розгляду.

1.3.2. Відстеження через веб-браузер

- Стандартні **HTTP Cookies** при первинному відвідуванні веб-сайту не порушують конфіденційність даних, але подальше їх використання полягає в ролі ідентифікатора користувача. Важливо зауважити, що повне блокування прийому Cookies може виявитися неприйнятним, оскільки це може вплинути на нормальну взаємодію з веб-сайтом. Зазвичай як захист використовується періодичне очищення cookies, а іноді їх модифікація.
- **Cookies** від **сторонніх** ресурсів (3rd party) встановлюються екстернальними ресурсами, які з'єднані з веб-сайтом. Їх основне використання пов'язане з таргетуванням реклами, і важливо відзначити, що блокування їх прийому, як правило, не впливає на нормальну функціональність сайту.
- **LSO** (Local Shared Objects) або Flash Cookies є загальними для всіх браузерів і залишаються після стандартного очищення cookies. Властивості Flash Player дозволяють вимкнути зберігання LSO.
- **HSTS SuperCookies** використовують прапори HSTS, збережені у браузері, для створення бінарного ідентифікатора. Ці дані знищуються під час очищення звичайних cookies.
- **HTTP Etag** призначений для контролю вмісту кешу, але може служити ідентифікатором. Аналогічне використання можливе з заголовком

Last-Modified, який може містити довільний рядок, замість дати. Etag, збережені, видаляються через очищення кешу.

- **Evercookie** [16], відомий як "кукі, що не видаляються", використовує різноманітні механізми зберігання та відновлення з резервних копій після часткового очищення. Це включає всі вищезазначені методи, а також зберігання ідентифікатора властивості window.name, використання сховищ HTML5 (localStorage, sessionStorage, indexedDB), ізольованого сховища Silverlight та інші методи залежно від їх доступності.
- **HTML5 AppCache** також дозволяє зберігати унікальні дані як ідентифікатор. Це є проміжним між HTML5-механізмами зберігання даних та звичайним кешем браузера.
- **SDCH-словники**, розроблені Google, використовують алгоритм компресії на основі словників, що надаються сервером. Ці словники можуть використовуватися для зберігання унікальних ідентифікаторів, які можна включити як у ID словників, так і у сам контент [17].
- **Ubercookie**, описаний як "сучасна версія Evercookie", фактично представляє собою метод отримання цифрового відбитка (browser fingerprinting). Для цього використовуються AudioContext API (для отримання даних про аудіопідсистему) та метод getClientRects (який надає унікальний набір координат). Загалом такі методи відстеження можуть використовувати різноманітні параметри, комбінація яких буде унікальною для кожного браузера.

1.3.3 Цифровий відбиток веб-браузера

- **Canvas fingerprinting** — Відображення прихованого зображення з використанням HTML5 canvas і наступним переведенням його в бінарну форму [18]. Причому малюється текст, з використанням доступних системі шрифтів та рендерера. Набір шрифтів та методи згладжування трохи відрізняється на різних машини. Рендерер залежить від версії браузера, ОС та від GPU. В

підсумку відмальоване зображення майже унікальне (залишається невелика ймовірність збіги). Існують браузерні доповнення, що дозволяють або блокувати малювання, або замінювати відбиток. При цьому хибне значення може мати 100% унікальність, але відстежувати по ньому неможливо, оскільки при кожному відвідуванні сторінки генерується новий відбиток.

- **WebGL fingerprinting** [19] - рендеринг зображення, як і в canvas fingerprint, але з використанням API WebGL. За наявності підтримки WebGL 2 доступний набір даних дуже збільшується. З урахуванням того, що більшість сайтів не використовують WebGL для роботи, відключення WebGL у браузері зазвичай не викликає 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 у системних налаштуваннях динаміків.
- Метод **getClientRects** дозволяє отримати точний розмір та положення прямокутника у наявному елементі DOM. Дані значення можуть і з високою часткою ймовірності різнитися 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 прокручування колеса миші та руху курсору, доступні для відстеження з допомогою JavaScript. Спосіб відстеження користувачів за рухами миші спочатку здавався безглуздим, але, за деякими даними, він успішно використовується практично [21]. Таку технологію можна зарахувати вже до поведінкового аналізу.
- Заголовки **HTTP_Accept** містять набір значень, які можуть здатися стандартними для багатьох браузерів, але ймовірність їх збігу у двох браузерів становить близько 1:1700.

- Список встановлених **плагінів**, а також **розширень** (частково). Від плагінів залежить і список підтримуваних MIME-типів.

- Набір встановлених **шрифтів**, крім впливу на відбиток canvas, може використовуватись і окремо. На їх основі генерується так званий Font fingerprint.

- **Хід годинника**. Якщо система не синхронізує свій годинник зі стороннім сервером часу, то вони почнуть відставати чи поспішати, що створить унікальну різницю між реальним та системним часом, яку можна виміряти [17] з точністю до мікросекунди за допомогою JavaScript. Але навіть за синхронізації з NTP-сервером будуть невеликі відхилення, які також можна буде виміряти. Для оцінки значущості ознак може бути використаний ентропійний підхід. Під ентропією розуміється кількість інформації, що припадає на одне елементарне повідомлення джерела, що виробляє статистично незалежні повідомлення. Оскільки характеристики на кшталт «майже унікальний» або «незначний» не є точними, дослідники з Electronic Frontier Foundation запропонували кількісну оцінку у бітах ентропії [22]. Так, для Canvas fingerprint ентропія становить близько 15,5 біт, унікальність цього відбитка (якщо не включено заміну) - 1 на 48000. Навпаки, інформація про те, що в браузері дозволено прийом Cookies, має найнижчу цінність - близько 0,2 біт. Далі наведені ознаки щодо низькою ентропією, придатні для відстеження тільки в поєднанні з набором інших властивостей.

- Роздільна здатність монітора та розмір вікна браузера (включаючи параметри другого монітора у разі мультимоніторної системи), а також глибина кольору. Окремо визначається «доступна область» (availWidth і availHeight), часто відрізняється від основної. Може бути отримано не лише через JavaScript, а й без нього за допомогою медіа-запитів CSS.

- User-Agent. Показує версію браузера та ОС. Може бути легко змінено, але це не завжди має сенс, тому що 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 заміни User-Agent торкаються та navigator.userAgent, але інші параметри нерідко ігноруються і легко видають невідповідність. Функціонал для їх заміни помічений у розширенні "User-agent Switcher".

- Заголовок HTTP Referer дозволяє серверу визначити, що користувач перейшов на цю сторінку з іншого сайту, що допомагає відстежувати переміщення. Часто буває необхідним для нормального функціонування сайту.
- Мова браузера (JavaScript navigator.language) та віддана мова відображення сторінок (HTTP Accept-Language).
- Часовий пояс.
- Значення заголовка DNT (Do not track).
- Довжина історії вкладок — Атрибут history.length.
- Наявність сенсорного екрана та кількість торкань, що підтримується.
- Рівень заряду батареї (за наявності) через Battery Status API.
- Доступна інформація про CPU та GPU.
- Результат обчислення деяких математичних функцій. Приклад з сайту browserprint.info: функція Math.tan(-1e300) у Windows та у 64-бітному Linux повертає зовсім різний результат..

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

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

Загалом можна виділити такі принципи анонімізації браузера: дані з низькою ентропією можуть взагалі не потребувати захисту, а якщо захист виробляється, слід замінювати параметр на максимально поширене значення, не надаючи йому штучної нестандартності. Але слід періодично змінювати всі або деякі з цих параметрів, оскільки сукупності вони все одно утворюють патерн із високою ентропією. що ж стосується даних на кшталт canvas-відбитка, що мають найбільшу цінність, їх слід змінювати щоразу, коли потрібно «змінити особистість».

1.3.4. Особливості деяких протоколів

1. "Origin Bound Certificates" (ChannelID) - це самопідписані сертифікати, які дозволяють встановити зв'язок між клієнтом та HTTPS-сервером. Для кожного нового домену створюється індивідуальний сертифікат, який використовується для майбутніх з'єднань. Використання OBC може визначати користувачів в межах сайтів, не викликаючи спостережливих дій для клієнта. Унікальний ідентифікатор може бути представлений криптографічним хешем сертифіката, який клієнт надає як частину легітимного SSL-рукостискання.

2. Аналогічно, у TLS існують два механізми - "session identifiers" та "session tickets", які дають можливість клієнтам відновлювати перервані HTTPS з'єднання без проведення повного рукостискання. Це досягається за допомогою використання закешованих даних. Обидва цих механізми протягом короткого періоду дозволяють серверам ідентифікувати запити від одного й того ж клієнта.

3. Більшість сучасних браузерів впроваджують свій власний внутрішній DNS-кеш для прискорення процесу розв'язання імен і, у деяких випадках, для зниження ризику атак DNS rebinding. Цей кеш може використовуватися для зберігання невеликих обсягів інформації. Наприклад, якщо доступно 16 IP-адрес, близько 8-9 закешованих імен може бути достатньо для ідентифікації кожного комп'ютера в Інтернеті. Однак цей підхід обмежений розміром

внутрішнього DNS-кешу браузера та може викликати можливі конфлікти при розв'язанні імен із DNS-провайдера [17].

1.3.5. Виявлення присутності засобів анонімізації

1) Витік реального IP через Flash стає актуальним у випадках, коли анонімізується лише трафік браузера, а не всієї системи. За використання проксі-сервера можна примусово направити трафік Flash через нього за допомогою програми, такої як Proxifier чи іншої аналогічної. Якщо Flash-плагін необов'язковий для анонімної роботи, рекомендується вимкнути його [24].

2) Розкриття реального IP через WebRTC може статися, навіть якщо використовується VPN. Зазвичай веб-сайтам не потрібен WebRTC для нормальної роботи, і вимкнення його в браузері не призводить до проблем. Однак існують методи, які дозволяють замінити IP, що може викривати його.

3) Витік DNS призводить до відкритої невідповідності між IP-адресою та використовуваним DNS-сервером, а також косвено може розкривати ім'я інтернет-провайдера. Використання публічних DNS-серверів, таких як Google, вважається безпідозренковим. У випадку, коли VPN-клієнт не забезпечує надійний захист від такого витоку, рекомендується використовувати DNSCrypt. При цьому бажано обирати DNS-адресу з країни, яка відповідає зміненій IP-адресі. Навіть у випадку, коли відповідність не може бути гарантована, це захистить від витоку оригінального DNS.

4) Відмінності між інформацією браузера про операційну систему та характеристиками TCP цієї ОС виникають через унікальний спосіб формування TCP-пакетів різними системами. Застосунок p0f дозволяє точно визначити операційну систему та її приблизну версію, аналізуючи параметри цих пакетів [25].

Проте при використанні проксі-сервера визначається операційна система, на якій працює сам проксі, оскільки він генерує вихідні пакети. В результаті відмінності між цими даними та User-Agent браузера можуть вказувати на

заміну User-Agent або використання проксі-сервера.5) Приналежність IP-адреси до мережі Tor очевидно вказує на використання Tor, оскільки адреси всіх вихідних вузлів відомі. Використання VPN через TOR – один із шляхів вирішення проблеми.

6) Розбіжність часового поясу: IP-адреса має певну геолокацію, що дозволяє співвідносити його з часовим поясом. Невідповідність системному часу означає заміну IP. Майже всі анонімайзери не замінюють часовий пояс у браузері, за винятком деяких браузерних розширень. Зазвичай потрібно змінювати 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 основна IP є адресою проксі сервера. Так працює, наприклад, плагін Dolus.

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

9) Так званий VPN fingerprint - виявлення використання VPN за характерним значенням MTU/MSS та деяким іншим ознакам, особливо актуально для OpenVPN [25].

10) Сумнівна назва хоста може виникнути, якщо при з'єднанні за кінцевою IP-адресою використовується ім'я хоста, яке не повинно включати слова типу "vpn", "hide", "proxy" тощо. Під час конфігурації власного VPN або проксі-сервера рекомендується уникати використання "розмовляючих" імен, а також утримувати повну відсутність імені, яке стане доступним для зовнішніх обернених DNS-запитів.

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

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

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

1.3.6. Атаки перетину та підтвердження в анонімних мережах

Атаки підтвердження (як приватний випадок атак перетину) базуються на тому, що атакуючий має припущення про те, які мережеві ресурси відвідує конкретний користувач через анонімну мережу. Йому потрібно лише підтвердити або спростувати цю гіпотезу. Для цього атакуючому потрібно аналізувати дані трафіку від точки входу користувача в анонімну мережу до точки виходу або самого ресурсу. У мережах із невеликою затримкою передачі даних можуть спостерігатися очевидні кореляції, такі як кількість пакетів, час їх відправлення та інші параметри, що дозволяють визначити користувача з високою ймовірністю (понад 90%), при цьому ймовірність помилки може бути дуже низькою (менше тисячних часток відсотка).

У випадках, коли атакуючий використовує активні методи, такі як введення затримок у трафік чи пошкодження пакетів, для повного виявлення користувача може бути достатньо навіть одного пакета даних.

Ці атаки стають трохи більш складними в разі прихованих ресурсів, таких як Tor, або закритих файлообмінних мереж, наприклад, Freenet. Оскільки противнику невідомо, звідки точно знімати трафік, навіть якщо він знає, до

якого ресурсу користувач хоче звернутися. Тим не менше, подібні атаки можуть бути достатньо ефективними навіть у таких випадках.

Ще один варіант атаки перетину виникає, коли противнику невідомий ресурс, до якого користувач хоче звернутися, але він контролює кілька вузлів анонімної мережі. Якщо трафік користувача випадково проходить через ці вузли в початковій та кінцевій точках, достатньо кореляції статистичних параметрів трафіку (без розшифрування трафіку) між вхідним вузлом (або між точкою входу у мережу у провайдера користувача та кінцевим вузлом ланцюжка). Це дозволяє провести атаку перетину та визначити, до якого ресурсу звертається користувач з останнього ланцюжка вузла. При цьому кількість вузлів між першим і останнім вузлом ланцюжка не відіграє вирішальної ролі проти більшості атак такого роду, і збільшення довжини ланцюжка більше трьох вузлів є марним. Такий сценарій атак серйозно обмежує рівень анонімності користувача у мережах, подібних до Tor.

Важливо зауважити, що анонімні мережі, які захищають від аналізу трафіку (наприклад, Tor) або забезпечують цензурозахищеність інформації (як у Freenet), все ж не є ідеально захищеними від атак підтвердження отримання інформації, яку противник може свідомо знати, або інших видів статистичних атак перетину. Побудова мереж, які враховують ці умови, є складним теоретичним завданням. У дизайні існуючих анонімних мереж атаки перетину та підтвердження в більшості випадків ігноруються або обмежуються мінімальними заходами захисту, оскільки захист від противника такого рівня виявляється надто складним, хоча й меншим, ніж у випадку "глобального спостерігача". Різноманітні атаки на кореляцію практично завжди виявляються на 100% ефективними та виконуються досить просто проти окремих шифруючих проксі та VPN, які іноді використовуються для досягнення невисокого рівня "анонімності" [26].

1.4. Основні категорії анонімізаційних засобів

У ході теоретичного аналізу наукової літератури за проблематикою роботи було визначено, що до засобів анонімізації відносять наступні: «Proxy-сервери», «VPN», «SSH-тунелі», «Dedicated-сервери», «Tor», «JonDonym», «I2P», «віртуальні машини», «антидетекти». Проаналізуємо детальніше.

"Проксі-сервери" представляють собою "систему або програму в комп'ютерних мережах, які дозволяють здійснювати непрямі запити до мережевих сервісів". На сьогодні існує кілька типів проксі-серверів, кожен з яких має свої характеристики та особливості застосування. Проте для анонімізації найчастіше використовують "SOCKS5", який комбінують з використанням VPN. Важливо відзначити, що в науковій громаді проксі-сервери вважаються недостатньо надійними для забезпечення анонімізації, оскільки вони не забезпечують шифрування трафіку і можуть легко бути деанонімізовані навіть у випадку створення ланцюжка проксі. Послідовне аналізування логів на кожному сервері ланцюжка дозволяє визначити реальний IP навіть при будь-якій довжині ланцюжка.

Kulbir Saini Squid Proxy Server 3.1: Beginner's Guide. Packt Publishing Ltd, 2011. 308 p.

Ще одним засобом анонімізації є "VPN" або "віртуальна приватна мережа". У науково-довідковій літературі, зокрема в словниках, термін "VPN-сервіси" тлумачиться як "загальна назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри". Виходячи із цього визначення, можна виділити ряд переваг та недоліків у використанні VPN-сервісів. Основною перевагою є високий рівень надійності шифрування каналу. Проте серед недоліків можна відзначити наступне:

- Запис логів. Постачальники VPN не можуть надати повних гарантій своїм користувачам, щодо відсутності записів, оскільки перевірка останнього неможлива;

- Викриття IP-адреси. Ця проблема може виникнути при раптовому відключенні VPN. Однак за допомогою додаткового налаштування правил файрвола можна уникнути виявлення цієї проблеми.

Також важливо відзначити, що більшість VPN-сервісів пропонують свої послуги за плату. Це ствердження підтверджує Файльнер Маркус у своїй статті "Віртуальні приватні мережі нового покоління" у журналі "Сетеві рішення/LAN" з листопада 2005 року, де він детально розглядає сучасні технології VPN.

Наступним засобом для забезпечення анонімізації в Інтернеті є SSH. Абревіатура "SSH" походить від англійського виразу "Secure Shell", що перекладається як "безпечна оболонка". Загалом, "SSH" представляє собою мережевий протокол, який використовується для віддаленого управління операційною системою та проксування TCP-з'єднань.

Не дивлячись на те, що від початку основна задача SSH полягала у іншому, наразі SSH-тунелі активно використовуються й для забезпечення анонімізації. У той же час, слід відмітити, що подібно до VPN SSH-тунель здійснює шифрування даних, однак влаштований за іншим принципом. Проаналізуємо детальніше.

SSH-тунель має подвійне використання. З одного боку, він служить для передачі TCP-пакетів, а з іншого боку - для трансляції IP-заголовка під час передачі інформації, при умові попередньо заданого правила. Таким чином, використання та створення SSH-тунелів більше схоже на перенаправлення портів поверх протоколів, аніж на справжнє "тунелювання". Порівняно з VPN, SSH-тунель має трошки меншу швидкість роботи і часто використовується як локальний проксі-сервер [15].

"Dedicated-сервери" представляють собою форму хостингу, при якій надається окремий фізичний сервер окремій особі для використання в якості власного VPN-сервера. Зазвичай використовується віртуалізація, така як "VPS" (віртуальний приватний сервер), що передбачає розміщення кількох віртуальних серверів на одному фізичному хості з метою ускладнення відстеження підключень до конкретного сервера [15].

"Tor" – це браузер, спрямований на забезпечення анонімності користувачів в мережі Інтернет. Ще недавно цей браузер вважався одним з

найбільш надійних, проте останнім часом виявляються випадки розкриття анонімності, обумовлені прослуховуванням трафіку на вихідних вузлах та підозрілістю IP-адрес, що належать Tor.

"JonDonym" або "JAP" ("Java Anonymous Proxy") представляє собою анонімайзер, який використовує Proxy-сервер для анонімного перегляду веб-сторінок. Анонімність досягається відправкою запиту через ланцюжок проксі та змішуванням потоків даних від декількох користувачів. "JonDonym" підтримує різні платформи, що підтримують "Java", і працює як на платній, так і на безкоштовній основі.

"I2P" або "Invisible Internet Project" - це комп'ютерна мережа, яка використовується для забезпечення анонімності користувачів при доступі до мережі Інтернет. У "I2P" існує ряд особливостей функціонування, таких як:

- оверлійність – здатність до роботи поверх інших мереж;

- стійкість, що передбачає функціонування мережі навіть у випадку відключення вузла;

- надійність, що обумовлена шифруванням даних під час їх передачі між вузлами мережі;

- анонімність, що забезпечується унеможливленням відстеження IP-адреси вузла;

- децентралізованість – відсутність центрального сервера.

У той же час, слід відмітити, що «I2P» демонструє досить низький рівень анонімності через зовнішній інтернет, що обумовлено нестабільністю та досить тривалим часом підключення, особливо коли публічна IP-адреса відсутня. *Juan Pablo Timpanaro, Isabelle Chrisment, Olivier Festor.* Monitoring the I2P network // INRIA Nancy-Grand Est. — Henri Poincar´e University, France, 2011. — С. 5—7.

Ще одним методом анонімізації у мережі Інтернет є використання "віртуальних машин". Ці машини уособлюють певне програмне середовище, що імітує реальний комп'ютер з усіма його складовими компонентами. Для забезпечення високого рівня анонімізації часто використовують віртуальні машини спільно з іншими засобами [27].

"Антидетекти" або також відомі як "мультиаккаунтні браузери" - це програмне забезпечення, яке дозволяє змінювати чи маскувати цифровий слід браузера шляхом управління інформацією про пристрій користувача і операційну систему. Ці засоби доступні сайтам через API браузера, що надається цим програмним забезпеченням.

Дуже часто програмне забезпечення "антидетект" може використовуватися у нелегальних діяльностях, воно недоступне для вільного використання, функціонує на платній основі та має високу вартість. Важливо зазначити, що термін "антидетект" може застосовуватися не тільки до програмного забезпечення, але й до віртуальних машин, які модифікуються для маскування під реальний комп'ютер.

Для досягнення анонімності в мережі Інтернет також використовують інші засоби, проте їх надійність та здатність до захисту можуть бути під сумнівом. Сюди включають програми та браузерні розширення, які призначені для захисту від відстеження браузера. Ці засоби доповнюють систему анонімізації в аспектах, які не забезпечуються іншими засобами, зазначеними вище.

1.4.1. TOR як засіб забезпечення анонімності в мережі Інтернет

The Onion Router (TOR) – це найбільш важливий і популярний інструмент для забезпечення анонімності в Інтернеті. Це вільне та відкрите програмне забезпечення, яке працює на основі принципу цибульової маршрутизації: всі дані, що входять в мережу TOR, проходять через три вузли мережі, які обираються випадковим чином. Перед відправленням дані послідовно шифруються ключами обраних вузлів.

Коли пакет досягає першого вузла, він розшифровує верхній шар шифру (аналогія зі зборкою цибулі) і дізнається, куди відправити пакет далі. Аналогічні операції виконуються на другому та третьому серверах. Найбільш

уразливі - вихідні вузли (exit nodes), де трафік остаточно розшифровується та надсилається до цільового ресурсу.

На вихідних вузлах може виникати ризик прослуховування трафіку, і це важливо враховувати, особливо коли з'єднання з ресурсом відбувається за небезпечним протоколом, наприклад, на сайті, який не підтримує HTTPS [28].

Фактично, TOR є мережею шифруючих проксі-серверів, або віртуальних тунелів, що підтримуються переважно добровольцями. На 2017 рік, ця мережа налічує близько 7000 вузлів, і 11% з них є вихідними вузлами [29]. Таким чином, кількість можливих маршрутів дуже велика, особливо з урахуванням того, що TOR змінює маршрути кожні 10 хвилин. Вхідні вузли (entry nodes) забезпечують захист від перехоплення та підробки даних на шляху між вхідним вузлом та клієнтом. Крім того, існують мости (bridges) - ретранслятори, адреси яких не публікуються у загальному каталозі і надаються за запитом клієнта [30]. Мости забезпечують доступ до мережі у тих випадках, коли інтернет-провайдер блокує відомі вхідні вузли TOR, а також виконують обфускацію (маскування) трафіку, що перешкоджає його ідентифікації та блокуванню системами глибокого аналізу пакетів (DPI). Розроблено кілька типів мостів, і на даний час найбільш ефективним вважається obfs4.

Можливо, для багатьох користувачів ознайомлення з Tor обмежується використанням Tor Browser. Цей набір включає програму Tor і змінену версію браузера Firefox. На сучасний момент Tor Browser є відносно надійним та доступним інструментом для захисту від відстеження та забезпечення анонімності. Багато поліпшень, внесених до Tor Browser, поступово впроваджуються у звичайний Firefox за допомогою проекту Tor Uplift. Важливо розрізняти Tor Browser і сам Tor, оскільки Tor може бути використаний і без браузера. Раніше популярним був додаток Vidalia, який був графічним інтерфейсом для керування вузлом Tor, але його розробка була припинена. AdvOR (Advanced Onion Router) також існує і дозволяє направляти трафік додатків через Tor та налаштовувати різні параметри. Основний Tor Browser також може використовуватися як проксі-сервер для різних додатків, надаючи

локальний інтерфейс, де ви можете переглядати параметри SOCKS5 у налаштуваннях проксі-сервера Tor Браузер. Для програм, які не підтримують роботу через проксі, можна скористатися програмами Proxifier або вищезгаданим AdvOR. Важливо враховувати, що Tor підтримує лише TCP-трафік, тому в разі необхідності функціонування UDP слід використовувати додаткове тунелювання UDP-трафіку через VPN.

Основний недолік Tor Browser полягає в тому, що його використання легко виявляється з боку відвідуваних ресурсів. По-перше, IP-адреси вихідних вузлів Tor відомі, і деякі веб-сайти обмежують доступ з таких адрес через те, що Tor часто використовується зловмисниками. Крім того, Tor Browser має типові цифрові відбитки (fingerprints). Механізми, які використовує цей браузер для боротьби з відстеженням, роблять усі копії Tor Browser схожими одна на одну (або, принаймні, прагнуть до цього), тому ідентифікувати конкретного користувача дуже важко, але легко визначити, що використовується саме Tor Browser. Зрозуміло, це не стосується внутрішніх сайтів мережі Tor, так званих onion-ресурсів, призначених для відвідування через Tor.

Категорично не рекомендується використовувати Tor для BitTorrent. Це не тільки є загрозою для анонімності, але й створює надмірне навантаження на мережу Tor. Перелічимо й деякі інші речі, які слід робити [31]. Не можна заходити через Tor в акаунти, пов'язані з реальною особистістю, а також не можна заходити без анонімізації у створені через Tor акаунти. Якщо облікова запис хоча б раз використовувався з реального IP, він більше не є анонімний. Не слід забувати про соціальні методи деанонімізації: не можна розкривати ідентифікуючі дані при анонімному спілкуванні або публікаціях. Небажано використовувати ту саму цифрову особистість надто довго - чим довше використовується один псевдонім, тим більше накопичується профілюючої інформації про нього. Не рекомендується залишатися авторизованим у якомусь акаунті довше, ніж необхідно. Не можна підключатися до ресурсу одночасно анонімно та неанонімно, оскільки це дозволяє виявити кореляції між двома сполуками. До файлам, що виконуються, особливо виконуваним, потрібно

ставитися з максимальною обережністю. Крім того, небажано встановлювати якісь доповнення в Tor Browser і взагалі змінювати його стандартну конфігурацію.

Мережу Tor вважають надійним інструментом для анонімізації, але не було прикладів розкриття особистої інформації користувачів. Важливо зауважити, що деанонімізація не завжди пов'язана з самою уразливістю Tor; часто використовуються методи соціальної інженерії, і користувач може допускати помилки.

Однак були випадки використання "уразливостей нульового дня" у браузері Firefox, на основі якого побудований Tor Browser, ФБР, що вказує на важливість патчінгу можливих слабких місць у додатках [32]. Нещодавні заходи, вжиті розробниками, суттєво покращили безпеку Tor Browser.

Також було виявлено деякі методи fingerprinting, які були ефективними відносно Tor Browser, але розробники вжили заходів для їх ефективного врегулювання [21]. Важливо відзначити, що проблеми, пов'язані із шкідливими вузлами, періодично виникають у мережі Tor, і дослідження виявляли випадки перехоплення та інфікування трафіку, включаючи вихідні ретранслятори [33]. Заходи приймаються для виявлення та блокування шкідливих вузлів для забезпечення безпеки мережі.

Tor має відому уразливість до атак, спрямованих на аналіз трафіку, що вже багато років відома. Оригінальна документація проекту зазначає наявність вразливості системи перед "глобальним пасивним зловмисником", який може прослуховувати весь трафік вхідних та вихідних вузлів. Шляхом порівняння обох потоків трафіку такий зловмисник може деанонімізувати користувача. У реальності це можливо в обмеженому масштабі, оскільки неможливо повністю контролювати всю мережу Tor. Однак наявність навіть двох контрольованих вузлів вже створює можливість ідентифікації частини користувачів, чий трафік проходить через обидва вузли [34]. Оригінально Tor не був спроектований для протистояння масштабним атакам, де зловмисник може мати безліч точок

присутності всередині мережі. У цьому відношенні мережа I2P була розроблена з врахуванням можливості прослуховування кожним вузлом.

На сьогоднішній день Tor залишається досить ефективним та вільним інструментом для забезпечення анонімності та протидії відстеженню, зокрема в складі Tor Browser. Проект активно розробляється і отримує нові механізми захисту. Однак використання Tor пов'язане з певними незручностями і не завжди забезпечує повну анонімізацію. Розглядати Tor як базовий елемент для побудови складніших комбінацій є доцільним підходом.

1.5. Віртуальна приватна мережа

Технологія віртуальної приватної мережі (VPN), призначена для безпечної передачі даних через зашифрований тунель між двома вузлами, на сьогоднішній день стала популярним засобом забезпечення конфіденційності в Інтернеті і часто розглядається користувачами як альтернатива Tor. Однак важливо зауважити, що збереження анонімності в разі VPN повністю залежить від довіри до постачальника VPN, за винятком сценаріїв, де користувач налаштовує власний VPN-сервер. Точніше буде стверджувати, що VPN забезпечує конфіденційність даних, наприклад, дозволяє приховати від інтернет-провайдера історію активності користувача. При цьому в платних VPN-сервісах, як правило, швидкість з'єднання значно вища, ніж у Tor.

1.5.1. Протоколи

Існує кілька найпоширеніших протоколів VPN:

• **PPTP** (Point-to-Point Tunneling Protocol) - це швидкий і легко налаштовуваний протокол VPN, який був розроблений Microsoft і довгий час використовувався як стандартний протокол VPN. Однак він вважається порівняно небезпечним і застарілим. PPTP для забезпечення безпеки

використовує різні методи аутентифікації. Незважаючи на те, що PPTP, як правило, використовує шифрування з 128-бітною ключовою довжиною, у 1999 році було виявлено кілька уразливостей. Найбільш серйозною з них була вразливість протоколу аутентифікації MSCHAP v.2, що призвело до зламу PPTP за два дні. Хоча Microsoft виправила цю помилку, перехід до протоколу аутентифікації PEAP із заміною MSCHAP, вона рекомендує використовувати для VPN скоріше протоколи L2TP або SSTP [35].

• **L2TP/IPsec -** це протокол тунелювання на рівні 2, який, на відміну від деяких інших протоколів VPN, не надає шифрування та захисту даних. Зазвичай його використовують із додатковими протоколами, зокрема IPSec, для шифрування даних перед їх передачею. Усі сучасні пристрої та системи, сумісні з VPN, включають вбудований протокол L2TP/IPsec. Встановлення та налаштування зазвичай є простими та швидкими, хоча можуть виникнути проблеми з використанням порту UDP 500, який може бути заблокований файрволом NAT. Таким чином, може бути необхідна переадресація портів, якщо протокол використовується з файрволом. Відомо про вразливості IPSec, але за правильного використання він забезпечує надійний захист даних. Однак Едвард Сноуден відзначав, що і цей протокол не є абсолютно безпечним. Засновник і експерт з безпеки Electric Frontier Foundation, Джон Гілмор, вказує на те, що Національне агентство безпеки США (NSA) може намагатися послабити цей протокол, і дворазове інкапсулювання даних може зробити його менш ефективним, порівняно з рішеннями на основі SSL, що може призвести до повільнішої роботи порівняно з іншими протоколами.

• **OpenVPN** є порівняно новою технологією з відкритим кодом, яка використовує бібліотеку OpenSSL та протоколи SSLv3/TLSv1, а також ряд інших технологій для забезпечення надійного VPN-рішення. Однією з основних переваг є гнучкість налаштувань OpenVPN. Цей протокол може бути налаштований для роботи на будь-якому порту, включаючи 443 TCP-порт, що дозволяє маскувати трафік усередині OpenVPN під звичайний HTTPS, що ускладнює його блокування. Ще однією перевагою є те, що бібліотеки OpenSSL

підтримують різноманітні криптографічні алгоритми, такі як AES, Blowfish, 3DES, CAST-128, Camelia та інші. Зазвичай VPN-провайдери обирають використання лише AES та Blowfish.

Швидкість OpenVPN залежить від рівня шифрування, але, зазвичай, вона вища, ніж у IPSec. Хоча більшість VPN-провайдерів використовують OpenVPN, він не є підтримуваним за замовчуванням на всіх платформах. Проте існують сторонні програми, розроблені для різних платформ, включаючи ПК, Android та iOS. Ще однією проблемою OpenVPN є його гнучкість, яка може зробити його незручним для налаштування. Зокрема, використання типової програмної реалізації OpenVPN (наприклад, стандартного відкритого клієнта для Windows) вимагає завантаження та встановлення клієнта, а також конфігураційних файлів. Багато VPN-провайдерів вирішують цю проблему, надаючи передналаштовані VPN-клієнти.

На основі всіх наданих факторів та інформації, яку надав Е. Сноуден, можна вважати, що на даний момент протокол OpenVPN вважається одним з найбільш безпечних. Зазначається, що він має експериментальні методи шифрування, які призначені для захисту від можливих втручань, включаючи потенційні дії Агентства національної безпеки США. Звісно, неможливо повністю передбачити всі можливі сценарії втручання, і хоча існує невизначеність щодо можливостей розвідувальних служб, OpenVPN вважається одним з найбільш надійних і безпечних протоколів на сьогоднішній день [35].

• **SSTP** (Secure Socket Tunneling Protocol) - це протокол безпечного тунелювання сокетів, який був введений компанією Microsoft у Windows Vista SP1. Навіть як він тепер доступний на платформах Linux, RouterOS і SEIL, він залишається популярним переважно серед систем Windows. SSTP використовує SSL v.3, що надає йому аналогічні переваги, як і OpenVPN (наприклад, можливість використовувати TCP-порт 443 для уникнення проблем з NAT). Оскільки SSTP вбудований у Windows, його легше використовувати та вважається більш стабільним порівняно з OpenVPN. Однак важливо відзначити,

що SSTP не має відкритого вихідного коду, і всі права на нього належать Microsoft, що робить OpenVPN більш популярним вибором в спільноті.

• **IKEv2** (Internet Key Exchange version 2) був розроблений компаніями Cisco та Microsoft, і він вбудований у операційну систему Windows та наступні версії. Цей протокол також підтримує модифікації з відкритим вихідним кодом для різних платформ, включаючи Linux, і є сумісним з пристроями Blackberry. Він особливо підходить для автоматичного встановлення VPN-підключення, особливо в ситуаціях, коли інтернет-з'єднання періодично розривається. Користувачі мобільних пристроїв можуть використовувати його як протокол для бездротових мереж за умовчанням, і він дуже гнучкий, дозволяючи легко перемикатися між мережами. Хоча IKEv2 доступний на обмеженій кількості платформ порівняно з IPSec, він вважається досить надійним протоколом з точки зору стабільності, безпеки та швидкості роботи. Однак його недолік полягає в тому, що він має закритий вихідний код.

• **SoftEther VPN** - це мультипротокольний VPN-сервер, розповсюджуваний під ліцензією GPLv2, і його розробка триває з 2013 року. Цей сервер вражає своєю різноманітністю можливостей. Він використовує власний протокол SSL-VPN, який маскується під звичайний HTTPS-трафік, що робить його важко відзначити. Крім того, SoftEther VPN заявляє підтримку протоколів L2TP/IPsec, MS-SSTP, OpenVPN, L2TPv3 та EtherIP. Зокрема, для L2TP вказана сумісність із вбудованими клієнтами в iOS та Android. Сервер доступний для різних операційних систем, включаючи Windows, Linux, OS X, FreeBSD та Solaris. В порівнянні з OpenVPN, SoftEther VPN відзначається вищою швидкістю роботи, не вимагає наявності TUN/TAP, має вбудований NAT та DHCP. Протокол SSL-VPN може працювати через TCP, підтримує множинні TCP-сесії, UDP і навіть ICMP [36].

1.5.2. Проблеми вибору VPN-провайдера

Під час вибору протоколу VPN розумно обрати увагу на OpenVPN, а якщо розглядається можливість налаштування власного VPN-сервера, то SoftEther VPN може бути доречним вибором. Деякі з безкоштовних публічних серверів VPN Gate також дозволяють доступ через протокол SoftEther (SSL-VPN). Важливо зауважити, що багато VPN-провайдерів надають власні клієнтські програми для підключення, що може бути зручно, але при цьому належить бути обережним щодо можливих ризиків. Протокол OpenVPN передбачає використання відкритого клієнта та конфігураційного файлу, який повинен бути отриманий від провайдера. З іншого боку, клієнтська програма від провайдера може включати корисні функції, такі як kill switch (запобігання витоку трафіку поза VPN при втраті з'єднання) та захист від витоків DNS. Однак слід ретельно перевірити надійність їхньої роботи.

При розгляді вибору VPN-провайдера, важливо підходити до цього питання з особливою уважністю та відповідальністю. Безкоштовні VPN-сервіси часто викликають сумніви, оскільки невідомо, хто та з якою метою фінансує цей сервіс. Існує можливість, що діяльність користувачів може бути відстежена. Для ілюстрації цього підходу можна згадати випадок із 2017 року, коли правозахисна організація Center for Democracy and Technology (Центр демократії та технологій, CDT) викрила порушення політики конфіденційності популярного сервісу Hotspot Shield. Дослідження виявило, що Hotspot Shield відстежує онлайн-поведінку користувачів, перенаправляє їхній трафік, продає особисті дані третім сторонам і розкриває конфіденційні дані, такі як назви бездротових мереж, MAC-адреси та ідентифікатори IMEI пристроїв. Додатково, програма вбудовувала код JavaScript для рекламних цілей та використовувала більше п'яти сторонніх бібліотек для відстеження користувачів, і навіть перенаправляла трафік на сайти партнерів для здобуття прибутку.

Багато великих платних VPN-сервісів зазвичай приділяють велику увагу забезпеченню конфіденційності своїх користувачів. Проте, слід бути обережним щодо заяв про відсутність ведення журналів, оскільки часто провайдери фактично ведуть логи активності, і хоча багато залежить від обсягу

та тривалості зберігання цих даних, а також від можливості їхнього надання на запит відповідним організаціям. Корисно питати технічну підтримку сервісу, чи передбачено блокування облікового запису в разі виявлення шкідливої активності користувача. Якщо сервіс гарантує блокування тільки при отриманні скарг, це може означати, що його система не відстежує активність без наявності конкретних скарг. Також важливою є можливість анонімної оплати сервісу. Розкриття платіжних даних користувача VPN-провайдеру є прямим порушенням анонімності. Якщо сервіс виступає за забезпечення анонімності, він повинен приймати криптовалюту. Зазвичай вживається термін "анонімна оплата" в контексті Bitcoin, проте слід зазначити, що Bitcoin сам по собі не завжди гарантує повну анонімність, якщо не використовувати додаткові інструменти, такі як міксери. Використання інших криптовалют, таких як Monero або Dash, більше спрямованих на анонімізацію транзакцій, може бути більш ефективним, але на жаль, нинішні VPN-сервіси зазвичай не приймають їх для оплати.

Важливо вибирати іноземного VPN-провайдера, юрисдикція якого не підтримує дипломатичних відносин із країною користувача або країною з ліберальним законодавством, щоб ускладнити можливість отримання логів сервера, навіть для місцевої поліції. Також рекомендується використовувати два різних VPN-провайдери, вибираючи сервери у країнах, що не співпрацюють між собою [37]. Важливо уникати країн, які є частинами альянсу Five Eyes, основних учасників угоди UKUS SIGINT. Слід зазначити, що вибір надійного VPN-провайдера є складним завданням, навіть для досвідченого користувача. Сайт thatoneprivacysite.net, запущений у 2016 році, надає детальне порівняння понад ста VPN-сервісів за різними параметрами. Ця таблиця не надає однозначної відповіді на питання "який VPN найкращий", але лідерами можна вважати такі сервіси, як Proxy.sh (Сейшельські острови), oVPN.se та IPredator (Швеція), IVPN (Гібралтар), та CryptoStorm (Ісландія). Також отримали хорошу репутацію Private Internet Access, NordVPN, Mullvad та AirVPN. Варто враховувати, що є невелика кількість провайдерів, які публікують рекламу на

"тіньових" ресурсах, відкрито пропонуючи свої послуги потенційним зловмисникам. Ставлення до таких провайдерів може бути суперечливим. Хоча теоретично це може свідчити про те, що провайдер не співпрацює з правоохоронними органами і гарантує анонімність, реальність може бути іншою. Зазвичай рекомендується утриматися від використання таких VPN-провайдерів без вагомих причин для довіри.

Щодо використання різних рівнів DoubleVPN, TripleVPN, QuadVPN, важливо враховувати, що це часто є більше маркетинговим трюком, ніж практичним засобом підвищення безпеки. У більшості випадків всі сервери ланцюжка належать одному VPN-провайдеру, тому кількість рівнів не перешкоджає веденню журналу активності користувача чи можливості розкриття даних провайдером. Тим не менш, перехід на DoubleVPN може зменшити ризик деанонімізації. Важливо зауважити, що DoubleVPN не забезпечує двошарового шифрування, відмінно від Tor. Тут трафік на проміжному сервері розшифровується, але такий підхід все одно може мати свої переваги. Також можливий Parallel VPN, який використовує два паралельні VPN-канали для подвійного шифрування. Це може призвести до зниження швидкості, але вирішує проблему незахищеності трафіку на проміжному вузлі. Висновок полягає в тому, що VPN слід розглядати як інструмент для забезпечення конфіденційності, але вибір правильного провайдера та належне налаштування є ключем до досягнення високого рівня анонімності.

1.6. Використання віртуального приватного сервера (VPS)

Віртуальний приватний сервер (VPS), коли його використовують для анонімізації, зазвичай використовується для налаштування власного VPN, SSH або проксі-сервера, а іноді і вузла Tor, якщо це дозволяє хостер VPS. Це може бути економічно вигідніше, ніж використання платних VPN, особливо з урахуванням можливості повного адміністративного доступу до сервера, що дозволяє повністю контролювати ведення логів і налаштовувати VPN-сервер

під власні потреби, якщо є відповідні навички. Однак недоліком цього підходу є те, що на одному сервері може бути тільки один користувач, і його активність може бути легше відстежити, ніж при використанні великих платних або безкоштовних VPN-сервісів. З іншого боку, на фізичному сервері може бути розміщено кілька віртуальних серверів, що робить важким для зовнішніх спостерігачів зіставлення конкретних підключень із конкретним користувачем. При виборі провайдера VPS, аналогічно вибору VPN, важливо враховувати його юрисдикцію і уникати країн, що можуть співпрацювати з правоохоронними органами.

Ринок провайдерів віртуальних приватних серверів (VPS) є широким, і значна частина з них має міжнародний охоплення та підтримку оплати Bitcoin. Проте, якщо планується збереження анонімності під час реєстрації, можуть виникнути проблеми ще на цьому етапі. Багато хостинг-провайдерів VPS не дозволяють анонімну реєстрацію. При цьому важливо враховувати кілька базових факторів, щоб уникнути проблем:

1. IP-адреса: Вона не повинна бути адресою Tor або загальнодоступного проксі-сервера.

2. Особисті дані: Мають бути правдоподібними, не слід вводити випадкові комбінації символів замість П.І.Б.

3. Адреса: Також повинна виглядати правдоподібно, і країна повинна відповідати IP-адресі [38].

4. Телефон: Повинен належати вказаній країні.

При анонімній реєстрації рекомендується створювати максимально правдоподібний псевдонім, щоб уникнути привертання уваги через введення безглуздих даних. Очевидно, що анонімна покупка може бути безсмисленою, якщо подальше підключення до VPS планується з реального IP-адреси.

При виборі сервера для налаштування власного VPN слід звертати увагу на декілька ключових параметрів:

1. Ліміт трафіку та пропускна спроможність: Важливо обрати сервер із достатньою пропускною здатністю, яка задовольнить ваші потреби у використанні трафіку.

2. Оперативна пам'ять (RAM): Рекомендується обирати сервер із не менше ніж 512 мегабайт оперативної пам'яті для ефективного функціонування VPN-серверу.

3. Підтримка TUN/TAP: Якщо ви обираєте VPN-сервер, який використовує протокол TUN/TAP (наприклад, OpenVPN), переконайтеся, що обраний хостер і тип віртуалізації підтримують ці функції. Деякі хостери можуть вимагати запиту на технічну підтримку для увімкнення TUN-адаптера.

4. Доступ через SSH: Забезпечте доступ до сервера через SSH та налаштуйте авторизацію по сертифікату для додаткового захисту.

5. Налаштування файрволу: Після отримання доступу до сервера, налаштуйте правила файрволу для забезпечення безпеки.

6. Можливість конфігурації VPN: Налаштуйте необхідне програмне забезпечення для VPN і здійсніть його конфігурацію відповідно до ваших потреб.

7. Характеристики безпеки VPN: Власний сервер дає можливість настроїти VPN так, щоб його використання не було легко визначити за MTU або характерними портами. Ви також можете розглядати заходи безпеки, такі як port knocking, який дозволяє ховати доступ до сервісів за умови попередньо заданої послідовності з'єднань.

Обираючи сервер, слід ретельно дотримуватися ваших конкретних потреб та забезпечити необхідність безпеки для ефективного та захищеного використання VPN [39].

1.7. Операційні системи для анонімної роботи

На сьогоднішній день існує кілька дистрибутивів Linux, спеціально створених для забезпечення анонімності та безпеки користувачів. Багато з цих

дистрибутивів використовують мережу Tor та інші інструменти для забезпечення конфіденційності. Деякі з таких проектів на сьогодні включають:

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

Розглянемо докладніше два перші пункти цього списку.

1.7.1. Whonix як операційна система для анонімної роботи

Whonix, операційна система, призначена для анонімної роботи, базується на Debian та складається з двох віртуальних машин. Одна з них виступає в якості шлюзу, направляючи весь трафік у мережу Tor, тоді як інша є ізольованою робочою станцією, яка з'єднується лише з шлюзом. Існує також можливість фізичного розділення шлюзу та робочої станції. Whonix впроваджує механізм, відомий як ізолюючий проксі-сервер. Робоча станція не має зовнішньої IP-адреси в Інтернеті, що дозволяє нейтралізувати різноманітні вразливості. Навіть у випадку, якщо шкідливе програмне забезпечення отримає root-доступ до робочої станції, воно не матиме змоги виявити реальну IP-адресу [40].

Whonix, за словами розробників, успішно пройшла безліч тестів на витік інформації. Навіть такі програми, як Skype, BitTorrent, Flash, Java, які відомі своєю здатністю виходити в Інтернет обхідом Tor, були успішно протестовані на предмет відсутності компрометуючих витоків даних. Операційна система Whonix впроваджує різноманітні механізми анонімізації, такі як:

- Весь мережевий трафік програм в Whonix маршрутизується через мережу Tor.

• Для запобігання профілюванню трафіку Whonix застосовує концепцію ізоляції потоків. Попередньо налаштовані програми у Whonix використовують окремі Socks-порти, а кожен такий порт має свій власний ланцюжок вузлів у мережі Tor, що унеможливлює профілювання.

• Забезпечено безпечний хостинг сервісів Tor Hidden Services. Навіть при вторгненні в web-сервер, зловмисник не зможе викрасти закритий ключ Hidden-сервісу, оскільки цей ключ зберігається на Whonix-шлюзі.

• Whonix захищений від DNS-витоків завдяки ізольованому проксі. Усі DNS-запити перенаправляються на DnsPort Tor.

• Підтримка obfuscated bridges - мостів Tor.

• Використання технологій «Protocol Leak Protection and Fingerprinting Protection», що зменшують ризик ідентифікації цифрового відбитка браузера або системи за допомогою стандартних значень, таких як ім'я користувача – user, тимчасова зона – UTC тощо.

• Можливість тунелювання інших анонімних мереж, таких як Freenet, I2P, JAP, Retroshare через Tor, або безпосереднє використання кожної з цих мереж.

• В Whonix протестовані, документовані та успішно використовуються всі схеми комбінування VPN/SSH/Proxy з Tor [41].

• Whonix – повністю відкритий проект, що використовує вільне програмне забезпечення.

Існує кілька методів для встановлення Whonix, кожен з яких має свої особливості. Запуск віртуальних машин у VirtualBox вважається найпростішим способом. Однак, для більшої надійності рекомендується використовувати Qubes-Whonix, де Qubes OS використовує гіпервізор Xen для застосування концепції "безпека через ізоляцію". Існує також можливість використання віртуалізації KVM за допомогою qemu-kvm. Ще одним варіантом є фізична ізоляція, коли компоненти Whonix встановлюються на дві різні фізичні машини. Рекомендацією при цьому є встановлення шлюзу (Gateway) безпосередньо на фізичний комп'ютер, а робочої станції (Workstation) - у віртуальну машину. Після проведених досліджень розробники визнали Qubes-

Whonix безпечнішою альтернативою фізичній ізоляції [42], навіть з урахуванням можливих вразливостей у Xen. Не менш важливою особливістю Whonix є можливість підключення практично будь-якої віртуальної машини через Gateway, замість використання Whonix-Workstation.

На сьогоднішній день встановлення Whonix на Windows значно спростилось завдяки наявності автоматичного інсталятора. Цей інсталятор самостійно завантажує та імпортує образи віртуальних машин у VirtualBox, а потім дозволяє запустити їх за допомогою одного натискання кнопки. Проте варто відзначити, що в ході тестування виявлено певну проблему: інсталятор встановлює окремий екземпляр VirtualBox, навіть якщо програма вже була встановлена в системі. Це може призводити до конфліктів, і обидва екземпляри можуть виявитися непрацездатні. У разі виникнення цієї ситуації рекомендується деінсталювати оригінальний VirtualBox та потім перевстановити його у каталог, створений інсталятором Whonix.

1.7.2. TAILS як операційна система для анонімної роботи

Amnesic Incognito Live System, відома як Tails, отримала популярність завдяки статусу "системи, якою користувався Едвард Сноуден" та репутації "найанонімнішої операційної системи". Однак порівняти Tails із Whonix складно, оскільки їх концепції суттєво відрізняються. Tails є Live-дистрибутивом, який можна завантажити з Flash-накопичувача і не залишає слідів на комп'ютері, на якому він використовується. Як і Whonix, Tails базується на Debian. У Tails всі вихідні з'єднання прокладаються через мережу Tor, і будь-які спроби неанонімних з'єднань блокуються [43]. Tor Browser працює у захищеному режимі (AppArmor). Проте Tails також має "Небезпечний браузер" (звичайний Firefox), який дозволяє відвідувати сайти безпосередньо, без використання Tor. Загалом може вважатися, що Tails є менш безпечною, оскільки має доступ до фізичної системи, MAC-адрес, реальний IP, в той час як Whonix-Workstation ізольований у віртуальній машині. З іншого боку, Whonix

може мати вразливості як у двох своїх компонентах, так і в VirtualBox та операційній системі хоста. Також існують можливі вразливості у використанні Tails, і при використанні у віртуальній машині потрібно використовувати пакет virt-manager у Debian.

Крім Tor Browser, Tails встановлений набір ПЗ, зокрема:

• Pidgin – Jabber+OTR

• Electrum – легкий клієнт для Bitcoin

• KeePassX – менеджер (зберігач) паролів

• GPG – система асиметричного шифрування

• MAT – видалення метаданих із різних типів файлів

• Програми для редагування документів, фотографій, аудіо, відео тощо.

• Thunderbird – поштовий клієнт

• Легко встановити Psi або Psi+ (Jabber з підтримкою GPG)

Процедура встановлення Tails з-під Windows є дещо особливою і включає в себе використання двох Flash-накопичувачів. Спочатку настановний образ Tails записується на перший носій обсягом 2 Гб – це так званий «проміжний» Tails, який обмежено придатний для роботи (процедура спрощується при встановленні з Linux, і проміжний носій не потрібний). Потім необхідно завантажити ПК з цього носія. Іноді на цьому етапі може виникнути проблема, коли BIOS не може коректно завантажити образ. У такому випадку рекомендується перезаписати Tails на носій, використовуючи програму Rufus замість рекомендованої Universal USB Installer. Зазвичай це дозволяє успішно завантажити систему. Після цього потрібно підключити другий накопичувач, і на нього виконати установку «основного» Tails. Для цього слід вибрати в меню Програми → Tails → Tails Installer → Install by cloning. Після успішного завершення встановлення другий носій стає готовим до роботи, а перший вже не потрібний. 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 Applications → Tails → Configure

Persistence та задаємо пароль, бажано криптостійкий. Є можливість вибрати, які дані зберігатимуться. Все, що не збережено в постійному розділі, очищається після перезавантаження Tails. Зазначимо, що Tor Browser має можливість читання та запису тільки в двох папках, які знаходяться в закладках провідника: "Tor Browser" та "Tor Browser (Persistent)". Скачування та вивантаження файлів можливі лише з/у цих папках. За наявності справді важливих даних рекомендується періодично робити їхню резервну копію на інший носій, оскільки ризик раптового виходу з ладу Flash-накопичувача набагато вищий, ніж у випадку жорсткого диска.

Використання VPN у Tails не рекомендовано розробниками, тому така можливість за замовчуванням відсутня, і налаштування VPN вимагає втручання у правила iptables. Вважається, що ланцюжок "VPN через Tor" може шкодити анонімності, і про це йдеться в офіційній документації Tor. Справа в тому, що важливою перевагою Tor є часта зміна маршрутів трафіку, а при підключенні до VPN-сервера через Tor фактично створюється постійний маршрут, фіксоване місце призначення. Тим не менш, реалізувати такий ланцюжок дозволяє Whonix. Для Tails можлива схема "Tor через VPN", якщо використовувати роутер з прошивкою dd-wrt та підключитися до VPN з роутера. При необхідності надійнішого приховування шифрованих даних доцільно використовувати TrueCrypt (або VeraCrypt). На сьогодні творці Tails рекомендують використовувати cryptsetup, що базується на LUKS. Ця програма дозволяє створювати приховані розділи, проте такий розділ прихований не до кінця. Існує можливість виявити заголовок прихованого розділу, що дозволяє встановити його наявність. Заголовок прихованого розділу TrueCrypt не відрізняється від випадкових даних, і, наскільки відомо, виявити його неможливо (переконлива заперечуваність) [44].

У момент запуску, Tails автоматично синхронізує системний годинник. Якщо при цьому виявляється суттєва розбіжність часу, Tor Browser автоматично припиняє роботу та перезапускається. Це заходи безпеки, призначені для уникнення виявлення користувачів Tails ззовні, особливо через

аналіз часових відміток. Такий підхід допомагає утримати високий рівень анонімності для користувачів операційної системи.

1.7.3. Порівняння Whonix та Tails

Обидві операційні системи мають Debian як базу і використовують Tor Browser. Загалом, Whonix спрямована на встановлення на ПК, що використовується регулярно, надаючи інструменти для постійного анонімного та безпечного користування Інтернетом. У той час як Tails вважається більше інструментом для "похідного" використання, дозволяючи анонімно з'єднатися з Інтернетом на чужому ПК. Нижче подані деякі з відмінностей між ними.

Таблиця 1.1 Порівняння дистрибутивів

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

1.8. Специфіка анонімної поведінки

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

- Оцінити рівень довіри до ресурсу, на якому реєструється профіль.
- По можливості використовувати тимчасову e-mail адресу (Dropmail, 10MinuteMail) або постійний, але спеціально створений 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 залучати додаткового уваги.
- Іноді доцільно вказати реальне місто проживання, щоб додати профілю більше правдоподібності. Інакше в процесі спілкування може бути помічено, що анонім практично не знає місто, в якому нібито мешкає. Якщо ж немає потреби вказувати місто, то й робити це не потрібно. За можливості — взагалі не розкривати географічні дані, включаючи вартовий пояс.
- «Мульти-нік»: слід використовувати різні нікнейми у різних місцях, якщо немає явного бажання ідентифікувати себе як одну й ту саму особу.
- «Крос-постинг»: повна заборона на однакові тексти та посилання на них з-під різних профілів [14].
- Стиль мови може говорити про рівень освіти, проф. і т.п.
- Характерні мовні звороти, «коронні фрази», що повторюються помилки у мові. Може вказати на зв'язок двох профілів або навіть реальний особистість.
- При реєстрації в анонімних мережах – не використовувати свої нікнейми з "звичайного" Інтернету.

- Обов'язково видаляти метадані з файлів, що відправляються, наприклад, EXIF з фотографій, ім'я користувача із документів. До отриманих файлів від невідомих осіб слід ставитись з особливою обережністю [14]. 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 головне проведення часу.

Таким чином, існує значна кількість програмного забезпечення, орієнтованого забезпечити анонімність та приватність. Сучасні засоби дозволяють досягти високого рівня безпеки, проте вона завжди залежить від людського фактора. Найбільш потужним інструментом приховування особи є Tor та анонімні операційні системи на його основі. VPN сервіси менш безпечні, але зручніші у використанні. Підключення до VPN через Tor має як переваги, так і недоліки.

1.9. Вихідні дані та постановка задачі

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

Постановка задачі:

• приховати від відвідуваних сайтів усі дані, пов’язані з вихідною системою та браузером, що використовується для не-анонімної активності;

• забезпечити шифрування трафіку, що проходить через обладнання (DPI системи, СОРМ-3 і т.д.) інтернет-провайдера;

• забезпечити можливість багаторазової зміни цифрових відбитків;

• виключити можливість витоку реального IP в анонімному браузері;

• сайт не повинен виявляти, що використовуються засоби анонімізації;

• системи аналізу трафіку не повинні розпізнавати наявність VPN або Tor;

• рішення має бути придатним для надання користувачеві вже готовому вигляді, з нескладною процедурою встановлення та швидким налаштуванням.

Очевидно, що насправді користувач може відмовитися від готового рішення, оскільки немає підстав довіряти розробнику. Крім того, повністю приховати всі дані про реальну особистість зазвичай неможливо через людського фактора. Очевидно, що користувач із України відвідуватиме в основному україномовні сайти, переключатися на українську мову відображення сторінок, писати коментарі та, зрештою, спілкуватися рідною мовою. Але слід взяти до уваги, що такі сайти становитимуть лише меншу частина всього обсягу відвідуваних ресурсів.

Не всі ці вимоги є обов'язковими. Наприклад, якщо інтернет-провайдер не блокує трафік Tor або OpenVPN, то ні і прямий необхідності маскувати його, але користувач може вважати за краще робити це «про всяк випадок». Також, далеко не всі сайти перевіряють наявність засобів анонімізації і більше оцінюють правдоподібність відбитків. У рішенні, яке описуватиметься далі, робиться спроба реалізувати все вищезазначені вимоги.

1.10. Висновки до розділу 1

Сучасні технології відстеження перейшли значно за межі традиційних методів, таких як використання cookie-файлів, і викликали серйозні виклики у сфері приватності. Боротьба з цими технологіями стала вкрай складною задачею. Приховування особистості здавалося б відносно простим завданням, але насправді воно містить численні неочевидні аспекти.

Одним із важливих викликів є потреба не лише приховувати ідентифікуючі дані, але й регулярно змінювати їх. Статичний "псевдонім" може

бути схильний до відстеження так само, як і реальна особистість. Це означає, що потрібно розробляти механізми для постійної зміни ідентифікуючих даних, ускладнюючи таким чином спроби третіх сторін стежити за користувачем.

Іншим важливим аспектом є необхідність заміни цифрових відбитків зі збереженням їхньої повної правдоподібності. Спритні алгоритми відстеження можуть легко розрізняти ідентифікуючі дані, які були випадково змінені, від реальних. Таким чином, техніки заміни цифрових відбитків повинні бути ефективними, а також зберігати реалістичність, щоб ускладнити відстеження для алгоритмів і систем.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1. Вибір програмного забезпечення та необхідної конфігурації

2.1.1. Веб-браузер

Зважаючи на поставлену мету – максимально приховати факт анонімізації. використання «Tor Browser» виявляється небажаним, оскільки він легко виявляється та потенційно привертає увагу. Передбачається, що буде реалізовано ланцюжок «VPN через Tor», при якому на виході є IP адреса VPN-сервера, що не викликає підозр, на відміну від адрес Tor. Домогтися цього в «Tor Browser» складно – він спрямовує трафік виключно в Tor не приймає альтернативних налаштувань проксі-сервера. У той же час, як згадувалося вище, «Tor Browser» має характерні цифрові відбитки. Отже, у нашому випадку необхідно використовувати звичайний Firefox, але для цього потрібно значно змінити його конфігурацію. Варіанти з Chromium-браузерами не розглядаються, оскільки для анонімної роботи практично завжди рекомендується Firefox – цьому сприяє і репутація Mozilla, що активно

виступає за збереження приватності, і велика гнучкість налаштувань браузера. У **додатку В** наведено деякі параметри, які доступні через службову сторінку «about:config» (деякі відсутні за замовчуванням, але працюють, якщо їх створити) [47]. Крім них, існує ще безліч параметрів, однак придатних для посилення захисту. Основна ціль такий налаштування – запобігання витоку різних другорядних даних, з урахуванням того, що всі основні функції браузера повинні працювати як завжди. Наприклад, відключення різних опцій телеметрії – лише спосіб підвищити конфіденційність, проте відключення WebRTC – характерне ознака боротьби з витоком реального IP при використанні деяких засобів анонімізації, а подібних ознак слід уникати.

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

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

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

• «CanvasBlocker» – заміняє відбиток «Canvas fingerprint». Має опцію повного блокування запиту canvas readout і різні режими заміни, а також

підтримує білий та чорний списки. Відбиток генерується випадковим чином при кожному оновленні сторінки, що виключає можливість відстеження користувача за цим відбитком.

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

• «uBlock Origin» – розширення для фільтрації вмісту. Дозволяє блокувати не тільки рекламу, але й різні елементи, що відстежують (Списки фільтрів у категорії «Приватність» слід активувати). У деяких випадках захищає навіть від фінгерпринтінгу: наприклад, якщо сайт використовує стандартний скрипт «fingerprint2.js», завантаження скрипту буде блокована, тому що 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 великих «CDN» (мереж доставки контенту) шляхом надання локальних ресурсів та блокування мережевих запитів до CDN Може розглядатися як доповнення до фільтрів. Не викликає проблем із функціональністю сайтів.

• «Privacy Badger» – засіб блокування елементів, що відстежують, створений Фондом електронних рубежів (EFF), здатний до самонавчання.

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

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

• «AudioContext Fingerprint Defender» – спотворює відбитки «AudioContext» шляхом додавання випадкового шуму.

• «ScriptSafe» – містить безліч функцій анти-відстеження, частково повторює функціонал «NoScript», «uBlock» та інших доповнень, але має і деякі

унікальні опції: запобігання маніпуляціям з буфером обміну, додавання випадкових затримок між натисканнями клавіш.

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

Слід також згадати доповнення «RAS» («Random Agent Spoofer»), корисне для попередніх версій Firefox. Це інструмент для заміни профілю браузера («User-agent» та ряд супутніх параметрів) з широким списком можливостей (втім, багато його налаштувань просто управляють штатними параметрами конфігурації Firefox). Для деяких функцій використовує використання скрипта («script injection»), підтримує анонімізацію параметра «window.name», підміну роздільної здатності екрану, часового поясу (у протестованій версії опція «Time Zone Spoofing» була відсутня з неясної причини). Розробка даного розширення припинено через труднощі міграції на новий стандарт розширень «Firefox WebExtension». Це означає, що з Firefox 57 і вище Random Agent Spoofer несумісний.

Завершуючи розгляд браузера Firefox, відзначимо нещодавню ініціативу з інтеграції Tor у Firefox і, надалі, повному злиттю «Tor Browser» та Firefox в єдиний браузер (проект «Fusion»), який зможе працювати в різних режими. Це стане логічним продовженням проекту «Tor Uplift». Планується і подальше посилення функцій боротьби з «фінгерпринтінгом» браузера, а також підвищення зручності використання.

2.1.2. Архітектура системи

Для надійного захисту від можливих витоків та для ізоляції браузера від основною системою було вирішено використовувати віртуальну машину. Оскільки концепція «Whonix» – дві ВМ, одна з яких є інтернет-шлюзом, з'єднані внутрішньою мережею – працює дуже ефективно, вона і буде застосована у разі. Whonix дозволяє підключати до свого шлюзу не тільки оригінальну Whonix-Workstation, а й будь-яку іншу ВМ. Незважаючи на те, що

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

Шлюз «Whonix-Gateway» забезпечить анонімізацію трафіку засобами мережі Tor, але необхідно приховати факт використання Tor як від відвідуваних сайтів, так і від інтернет-провайдера (якщо в цьому є потреба). IP-адреса не повинен бути адресою вузла Tor, тому додатково використовується VPN. Можливі два варіанти – персональний VPN-сервер, запущений на VPS, або використання будь-якого VPN-сервісу. Перший варіант дозволяє налаштувати VPN для максимальної захищеності (відсутність ведення логів, застосування надійних криптографічних алгоритмів, різні заходи для приховання факту використання VPN), проте має дуже істотний недолік – сервер тільки одна, 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 будь-якої миті. З іншого боку, далеко не всі VPN-провайдери налаштовують сервери так, щоб сайти не могли розпізнати наявність VPN. У практичній частині даної роботи буде продемонстровано приклад запуску свого VPN-сервера і наведено його конфігурацію.

Під час налаштування VPN-сервера передбачено таке: використовується протокол TCP та порт 443 (інший варіант – нестандартний порт, нехарактерний

для VPN та проксі-серверів). Всі запити DNS надсилаються через VPN. Адреси DNS взяті зі списку «OpenNIC» і належать до тієї країни, де розташований вибраний VPS. Сервер блокує зовнішні ICMP-запити, тому метод «двостороннього пінгу» для визначення тунелю не працює. Значення MTU примусово встановлюється в 1500 стиснення трафіку (характерна ознака «OpenVPN») вимкнено. Задіяно опцію шифрування керуючого каналу у поєднанні з «HMAC-автентифікацією (tls-crypt) OpenVPN».

Для маскування трафіку Tor (і на випадок можливого блокування доступу) до мережі Tor інтернет-провайдером) буде задіяний «obfs4» – так званий «підключається транспорт», додатковий компонент Tor, спеціально призначений протидії аналізу трафіку DPI-системами. Крім того, доцільно виключити з використання вузли Tor, що знаходяться в країні перебування користувача, у разі це українські вузли. Дана можливість вбудована у додаток Tor і легко налаштовується. Усі зміни конфігурації Tor потрібно виконати на Whonix-Gateway. За винятком цих дій, втручатися в налаштування на шлюзі не рекомендується.

На основній віртуальній машині, крім браузера та VPN-клієнта, бажання користувача може бути встановлено додаткове ПЗ. Наприклад, «GPG4Win» для шифрування тексту та файлів, «Exif Purge» для видалення даних «EXIF» з фотографій, «Tox» або «Jabber-клієнт» для безпечного обміну повідомленнями (очевидно, якщо співрозмовник згоден користуватися тим самим додатком). Питання встановлення антивіруса є дискусійним. З одного боку, комерційний продукт – наприклад, «ESET Internet Security» – забезпечив набагато кращий захист від різних загроз, ніж фільтр «uBlock» зі списком «Malware Domains». Однак це вимагає покупки ліцензії, і тоді антивірус відсилатиме через анонімний канал ідентифікуючі дані. Насправді, швидше за все, 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 та файлової системи фізичної машини. Крім того, наявність заздалегідь зробленого знімка стану ВМ

(«snapshot») дозволить скинути її до незараженого стану. Єдиною, хоч і малоймовірною загрозою залишається зараження вірусом, що експлуатує певну вразливість «VirtualBox», яка б дозволила вірусу «вийти» за межі ВМ.

2.1.3. Підсумкові можливості заміни даних

Цифрові відбитки Firefox підміняються за допомогою вищезгаданих браузерних доповнень, деяких можливостей Firefox, а також зміна параметрів віртуальної машини. Окремі параметри можна підмінити і за допомогою JavaScript, підключаючи користувацькі скрипти через додаток «Tampermonkey», але це спрацьовує не завжди. Наприклад, роздільну здатність екрана краще змінювати для самої ВМ через налаштування «VirtualBox». «User-agent» залишаємо без змін або підмінюємо лише версію браузер. Мова браузера – англійська за замовчуванням, дозволяється встановити українську локалізацію інтерфейсу, але при цьому видалити українську зі списку мов, на яких запитуються веб-сторінки (це впливає на заголовок «HTTP Accept-Language»). Flash-плагін встановлювати небажано. Часовий пояс змінюється в системі і повинен відповідати геолокації VPN сервера (враховуючи також літній/зимовий час). «Відбиток шрифтів» має два різновиди:

• відтворення кількох символів Юнікоду в різних накресленнях та вимір розмірів отриманих символів;

• виявлення встановлених шрифтів за допомогою «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 ж 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 у разі встановлення та запуску плагіна Flash сайт зможе отримати доступ до всього списку шрифтів, встановлених у системі.

Додаток «CanvasBlocker» підміняє відбиток «Canvas» та частково «WebGL». Браузер Firefox дозволяє перевизначити значення рядків «Renderer» та «Vendor» для «API WebGL», проте в цілому відбиток «WebGL» залишається найбільш складним. Правдоподібна заміна всіх параметрів для «WebGL 2» може бути реалізована тільки при повноцінній емуляції відеокарти у віртуальній машині. На даний момент відомий один експериментальний проект з такою можливістю – модифікований VirtualBox від Д. Момота (Vektor T13), але його сумісність із «Whonix» поки що погано перевірена, і складно гарантувати стабільність, а також є проблеми із цифровими підписами драйверів. У звичайному «VirtualBox» функціональність «WebGL» буде залежати від того, включено чи 3D-прискорення графіки у віртуальній машині та чи встановлені «доповнення гостьовий ОС». І нарешті, заміна відбитка «AudioContext» виконується за допомогою «AudioContext Fingerprint Defender», також можна перемикати частоту дискретизації у налаштуваннях динаміків. Кінцева схема реалізації має вигляд, представлений на рисунку 3.1.

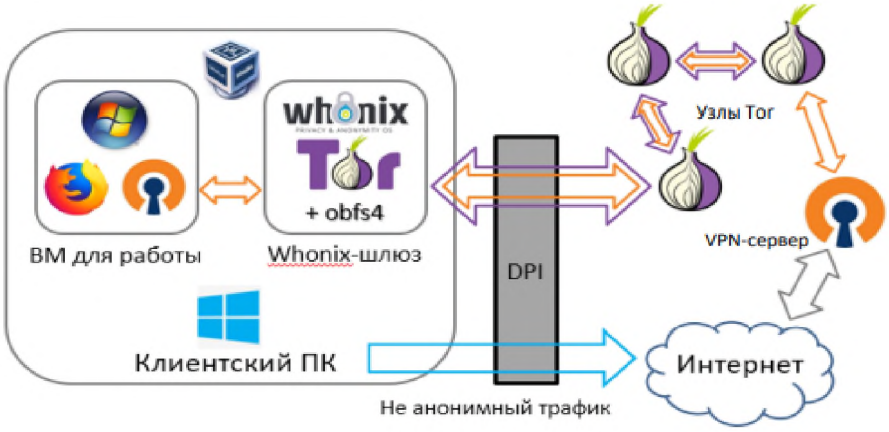

Рисунок 2.1 – Компоненти системи

Під позначенням DPI тут мається на увазі будь-яке обладнання аналізу та запису трафіку (у тому числі системи «СОРМ-3»), встановлене в інтернет провайдера. Схема не виключає можливості одночасного відвідування будь-

якого сайту з віртуальної машини та з основної системи, але навіть у цьому випадку з боку сайту було б дуже складно розпізнати, що відвідувач один і той же. Зауважимо, що за даної схеми немає необхідності маскувати трафік «OpenVPN», оскільки він знаходиться усередині каналу Tor з обфускацією. У той же час VPN забезпечить захист трафіку від можливого прослуховування на вихідних вузлах мережі Tor.

2.2. Налаштування серверу

2.2.1. Попередній етап

«VPS» («Virtual Private Server») – послуга, в рамках якої користувачеві надається так званий «віртуальний виділений сервер». В плані управління операційною системою вона здебільшого відповідає фізичному виділеному серверу. Зокрема, є root-доступ, власні IP-адреси, порти, правила фільтрування та таблиці маршрутизації. Власник VPS може видаляти, додавати, змінювати будь-які файли, включаючи файли в кореневій та інших службових директоріях, а також встановлювати власні програми або налаштовувати/змінювати будь-яке доступне йому прикладне програмне забезпечення [48]. Тип віртуалізації сервера може бути будь-яким, однак «Xen» та «KVM» (повна віртуалізація) вважаються більш надійними та зручними, ніж «OpenVZ» (загальне ядро ОС).

Відповідно, ми будемо використовувати VPS, щоб встановити та налаштувати на ньому VPN-сервер. Трафік між користувачем та VPN-сервером надійно зашифрований і тим самим захищений від прослуховування. Між сервером і кінцевим ресурсом трафік не шифрується засобами VPN, але можливо зашифрований протоколом TLS, якщо відвідуваний сайт працює безпечно з'єднання HTTPS. З цього випливає важливе зауваження: сервер, на

якому розміщується VPS, все ж таки здатний відстежувати історію підключень до зовнішнім ресурсам і навіть прослуховувати трафік незахищених з'єднань.

Для тестового запуску VPN у рамках даної роботи (і для особистого використання в подальшому) був орендований недорогий віртуальний сервер у «Провайдер VPS HostSailor». Операційна система – «Debian 9 x64», гіпервізор – «Xen», сервер розташований у Нідерландах. Для віддаленого доступу до сервера протоколу SSH використовувався клієнт «PuTTY», а також програма «WinSCP» для зручна робота з файлами на сервері.

Перш ніж приступати до установки VPN, слід убезпечити сервер від можливого несанкціонованого доступу. Авторизація за паролем – не найбезпечніший метод для SSH, тому насамперед був налаштовано вхід за сертифікатом «Ed25519», а парольну авторизацію вимкнено. «Ed25519» – це схема сигнатур еліптичної кривої, яка забезпечує кращий захист, ніж «ECDSA» і «RSA», і хорошу продуктивність через невелика довжина 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.

2.2.2. Встановлення та налаштування OpenVPN та Easy-RSA

Переконаємося, що підтримка «TUN/TAP» на VPS увімкнена, для цього в консолі введемо команду cat/dev/net/tun. Висновок «File descriptor in bad state» є нормальним. Якщо ж отримаємо «No such file or directory», то адаптер «TUN/TAP» не увімкнено [38]. Залежно від провайдера, потрібно включити цю функцію через панель керування сервером на сайті, або зробити запит до техпідтримці. На «Xen VPS» у Hostsailor адаптер був включений спочатку.

Для встановлення пакету «OpenVPN» у Debian» виконуємо команди:

«apt update»

«apt install openvpn»

Створимо папку для ключів і перейдемо до неї:

«mkdir /etc/openvpn/keys»

«cd/etc/openvpn/keys»

Усі операції зі створення ключів та сертифікатів можна виконати за допомогою утиліти «openssl», але простіше скористатися спеціально створеною для цього програмою «Easy-RSA», яка використовує openssl для виконання дій з ключами та сертифікатами. Раніше «Easy-RSA» постачалася разом з «OpenVPN», але тепер це окремий проект. Завантажуємо її, виймаємо та створюємо файл налаштувань з прикладеного зразка:

«wget https://github.com/OpenVPN/easy-rsa/archive/master.zip»

«unzip master.zip»

«cd /etc/openvpn/keys/easy-rsa-master/easyrsa3»

«cp vars.example vars»

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

#set_var EASYRSA_REQ_COUNTRY «US»

#set_var EASYRSA_REQ_PROVINCE «California»

#set_var EASYRSA_REQ_CITY «San Francisco»

#set_var EASYRSA_REQ_ORG «Copyleft Certificate Co»

#set_var EASYRSA_REQ_EMAIL «me@example.net»

#set_var EASYRSA_REQ_OU «My Organizational Unit»

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

#set_var EASYRSA_KEY_SIZE 2048

#set_var EASYRSA_DIGEST «sha256»

Щоб підвищити стійкість шифрування «RSA», збільшимо довжину ключів до найбільшою – замінимо «2048» на «4096», а «sha256» на «sha512». Однак, замість «RSA» можна використовувати більш сучасну криптографію на еліптичних кривих [49], що дасть експоненційне зростання криптостійкості при

меншою довжиною ключа. Наприклад, популярним сьогодні ключам «RSA» із довжиною 1024-2048 біт відповідає лише 160-224 бітний ключ «ECC». Крім високої надійності шифрування, це підвищує продуктивність. також у цьому випадку не потрібно генерувати файл ключа Діффі-Хеллмана. Вибір між «RSA» та еліптичними кривими необхідно зробити до початку роботи з «EasyRSA» для створення ключів. У файлі конфігурації vars нам знадобиться 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 СБУ викликали побоювання, що деякі, а можливо, й усі види криптографії на основі еліптичних кривих, які використовуються органами по стандартизації в США були навмисно ослаблені, щоб спростити для СБУ завдання їхнього злому. Доказів, що це можливо для кривих, що використовуються для підписання та обміну ключами, не існує, і деякі фахівці вважають це малоймовірним. У ході роботи спочатку було обрано менше поширена крива secp256k1, яку, зокрема, використовує система Bitcoin і яка була згенерована канадською компанією «Certicom», а не Національним інститутом стандартів та технології США (як інші криві). Передбачається, що ця крива надає менше можливостей приховати «Бекдор» [50]. На жаль, починаючи з версії «2.4.5 OpenVPN» не працює з цією кривою (точніше, вона не підтримується оновленою бібліотекою OpenSSL 1.1), тому довелося зупинитись на «secp521r1».

2.2.3. Генерація сертифікатів

Нам необхідно створити так звану «PKI» – інфраструктуру публічних ключів. В цілому, «PKI» грунтується на використанні криптосистеми з відкритим ключем та наявності посвідчувального центру. Ключі створюються

парами – закритий та відкритий. Для обміну з будь-ким захищеною інформацією ми обмінюємося відкритими ключами. В даному випадку сервер буде мати свій закритий ключ та відкриті ключі клієнтів. У клієнтів є свої закриті ключі та 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» наступний:

1. Ініціалізувати «PKI»;
2. Створити центр, що засвідчує – «Certificate Authority»;
3. Згенерувати сертифікати сервера;
4. Згенерувати сертифікати клієнта;
5. Створити файл параметрів Діффі-Хеллмана;
6. (опційно) Створити список відгуків сертифікатів;
7. (Посилення безпеки) Створити ключ автентифікації TLS.

Виконуємо команду ініціалізації:

./easyrsa init-pki

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

./easyrsa build-ca

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

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

./easyrsa gen-req server nopass

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

./easyrsa sign-req server server

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

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

./easyrsa gen-dh

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

./easyrsa gen-crl

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

cp pki/ca.crt /etc/openvpn/

cp pki/dh.pem /etc/openvpn/

cp pki/crl.pem /etc/openvpn/

cp pki/issued/server.crt /etc/openvpn/

cp pki/private/server.key /etc/openvpn/

cd /etc/openvpn

Додатково ми використовуємо механізм «HMAC» («hash-based message authentication code»), який служить для перевірки цілісності переданих даних, щоб унеможливити «атаки посередника». Для включення «HMAC» потрібно згенерувати спеціальний ключ і додати до файл конфігурації сервера директиву

«tls-auth», що вказує на даний ключ. Тоді сервер додаватиме підпис «HMAC» до всіх пакетів. рукостискання SSL/TLS. Будь-який UDP-пакет, який не має правильного підпису, може бути відкинуто без подальшої обробки. «HMAC-підпис», встановлювана директивою «tls-auth», забезпечує підвищений рівень безпеки на додаток до механізмів протоколу «SSL/TLS». Це може захистити від:

• DoS-атак або флуда на UDP-порт OpenVPN.

• Сканування портів з метою визначення прослуховуваних сервером UDP-портів.

• Уразливості, пов'язані з переповненням буфера в реалізації SSL/TLS.

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

Згенеруємо ключ:

«openvpn --genkey --secret ta.key»

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

Тепер за допомогою «WinSCP» змінимо права доступу до файлів: «ca.crt», «crl.pem», «dh.pem», «server.crt» – виставляємо для всіх 0644». На файлах «server.key» та «ta.key» повинні мати рацію «0600». На даному етапі сервер вже готовий до роботи, але необхідно ще створити ключі клієнтів та правильні файли конфігурації. Переходимо знову до папки «EasyRSA», створюємо та 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 підключення до VPN. У цьому випадку для підключення достатньо мати закритий ключ. Ім'я «client_name» – довільне, наприклад «home_pc». Тепер, коли всі ключі створені, конфігуруємо та запускаємо сервер. У папці / etc /openvpn створюємо файл «server.conf» (або замінюємо існуючий). Вміст використаного файлу наведено у додатку Б.

2.2.4. Додаткове налаштування та запуск сервера

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

«server=185.208.208.141»

«server=146.185.176.36»

«interface=tun0»

У цьому випадку тут вказані адреси використаних «DNS» від «OpenNIC», а також мережний інтерфейс «TUN», запити з якого оброблятиме «DNSmasq». У системному файлі /etc/resolv.conf також слід вказати аналогічні адреси «DNS і видалити звідти адреси «Google DNS», якщо вони були за замовчуванням.

Для перенаправлення трафіку з мережі «VPN» у зовнішній інтернет зазвичай використовуються механізми «NAT» та «IP forwarding». До файлу /etc/sysctl.conf додаємо (або розкоментуємо наявні) рядки:

«net.ipv4.ip_forward = 1»

«net.ipv6.conf.all.forwarding=1»

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

«iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 185.141.27.70»

«iptables -A INPUT -i eth0 -p icmp -j DROP»

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

Перезапуск «DNSMasq», запуск та перевірка працездатності «OpenVPN»:

systemctl restart dnsmasq»

systemctl start openvpn@server»

systemctl status openvpn@server»

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

2.3. Налаштування робочого місця

На клієнтський ПК встановлюється «VirtualBox», образи двох віртуальних машин «Whonix» завантажуються з офіційного сайту та імпортуються в «VirtualBox». У схемі використовується тільки «Whonix-Gateway», але доцільно завантажити і «Whonix-Workstation» для тих випадків, коли важливіше підвищена захищеність, ніж зручність та непомітність. Створюється ще одна віртуальна машина, в якій встановлюється Windows (переважний варіант – заздалегідь створити образ ВМ із встановленою системою та іншим програмним забезпеченням, а потім імпортувати його у клієнта відразу у готовому вигляді). Застосовується «Destroy Windows Spying» для видалення засобів збору телеметрії. У Налаштування віртуальної машини вказується внутрішня мережа «Whonix». Також рекомендується виставити число ядер процесора більше одного, цей параметр доступний через браузер (властивість «navigator.hardware Concurrency»), а одне ядро дуже явно вказує на наявність ВМ. У мережних налаштуваннях самої системи слід встановити параметри для підключення до «Whonix-Gateway»:

«IP-адреса – 10.152.152.50»

«Маска підмережі – 255.255.192.0»

«Шлюз - 10.152.152.10»

«DNS – 10.152.152.10»

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

«DisableNetwork 0»

«UseBridges 1»

«ClientTransportPlugin obfs2, obfs3, obfs4 exec /usr/bin/obfs4proxy»

«bridge obfs4 <адреса моста> # 2–3» адреси, кожна в окремому рядку

«ExcludeNodes {ru}, {??} # ?? » – вузли з невідомою геолокацією

У ході тестування було використано такі адреси мостів (на момент написання вони залишаються актуальними):

bridge obfs4 194.135.88.138:443
9F0BC3AA3CC72F17DC7789D7ABC7A763038F82CB
cert=lINVQVt8EQS5q9DWz3S+RHLosgiRVXueHlMfY3qtas1qHhGXvg7MOu6jE
CDZ0mbrS7tQLA iat-mode=0 bridge obfs4 185.79.93.126:59815
1594A9B832D4E0BD946A5988B364F1687814EC5D
cert=3DlWyDr4IwpZlxQbDX+7obB/EZr+eQavtnFbqaQsLym01MgIIsXPIl5E3ftp4I
LYK/G+OQ iat-mode=0 bridge obfs4 144.76.182.167:43981
77644CB35D66304974B84855A580155053365935
cert=yI120MhitxPLUcJFhDgspTy+sHOm4VlSAXLegRjYsu9qEd2yR59YNq3tvDnk
RiGY/+rQFQ iat-mode=0

У систему встановлюється OpenVPN-клієнт та браузер Firefox. Файл конфігурації для клієнта наведено в додатку В (деякі параметри OpenVPN для сервера та клієнта запозичені у сервісу «RootVPN»). При відключеному VPN весь трафік йде через Tor, що дозволяє відвідувати onion сайти в Firefox (спочатку необхідно в «about:config» відключити параметр «network.dns.block DotOnion»). Важливо: не слід встановлювати Tor Browser у цій машині, оскільки це призведе до ланцюжка «Tor через Tor» – вбудований Tor-клієнт браузера працюватиме через Tor-шлюз. Це не тільки знижує швидкодію, але й потенційно небезпечно через можливе появи самоперетинного маршруту та

скорочення ефективної довжини ланцюжки до одного-двох вузлів. Якщо потрібно використовувати Tor Browser, можна запустити його в системі або всередині «Whonix-Workstation».

Firefox встановлює набір додатків, згаданих у розділі 3, та застосовуються необхідні налаштування. Повний список можливих параметрів Зміни досить великий і немає єдиного правильного варіанти. «Білий список шрифтів» застосовується так: на одному із сайтів (наприклад, «BrowserLeaks») виявляємо список шрифтів, що розпізнаються в поточної конфігурації. Створюємо рядковий параметр «font.system.whitelist» на сторінку про: config» у Firefox. Вміст параметра заповнюємо отриманим список шрифтів. Тепер «відбиток шрифтів» буде змінюватися при видаленні деяких шрифтів зі списку. Зазначимо, що різні сайти перевіряють наявність різного набору шрифтів, тому видалення (або додавання до системи) нема кого шрифт не гарантує зміну отриманого списку на конкретному сайті. Параметр «WebGL Renderer» під «VirtualBox» містить слова «Software Adapter», це видає наявність віртуалізації, тому потрібно підмінити рядок значенням, взятим із будь-якого реального ПК. 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 движка браузера може бути виявлена за непрямим ознакам, тому бажано замінювати лише версію браузера. У доповнення «CanvasBlocker» рекомендується вибрати режим «fake at input», так як він складніший для виявлення. Системний годинник слідує періодично синхронізувати. Крім того, у Firefox 60 точність таймера знижена до 2 мс замовчуванням і до 100 мс у режимі «ResistFingerprinting».

Очищення даних («cookies», «Local Storage» та ін) відбувається при перезапуску Firefox, а також при використанні функції «Забути» або ручному видаленні даних для конкретного сайту (у Firefox 63 розробники планують спростити цю процедуру). Крім того, додаток «Firefox Multi-Account

Containers» дозволяє відкрити той самий сайт у декількох ізольованих вкладках, кожна з яких не має доступу до інших вкладок.

2.4. Перевірка отриманої збірки

2.4.1. Перевірені фактори та використані веб-сайти

Необхідно переконатися, що заміна всіх цифрових відбитків надійно працює, а відвідувані сайти не розпізнають наявність засобів анонімізації. У віртуальній машині з Windows було виконано підключення до настроєного VPN через «Whonix-Gateway», використаний Firefox 60 (остання стабільна версія на момент тестування). При роботі не було помічено проблем з підключенням OpenVPN за протоколом TCP через ланцюжок Tor та «obfs4». Вартовий пояс у системі було змінено до запуску браузера.

Для перевірки VPN щодо «невиявлення» використовувалися наступні інтернет-ресурси:

«https://2ip.ua/privacy» – визначає наявність VPN або проксі-сервера за характерним особливостям. 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.ua»: відмінність мови браузера, неповна заміна «User-agent», наявність IP у «чорних списках». Додатково відображає різні дані про браузер і виводить деякі рекомендації щодо підвищення безпеки.

«http://witch.valdikss.org.ru/» – визначає операційну систему по специфічним особливостям 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, дозволяє перевірити відсутність витоків (бажано повторити тест кілька разів). Основні сайти для визначення цифрових відбитків:

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

«https://audiofingerprint.openwpm.com/» – відбиток «AudioContext API».

«https://browserprint.info» – комплексний відбиток за рядом параметрів, включаючи шрифти, Canvas», AudioContext», розмір екрану та інші.

«https://panopticlick.eff.org/» – один із перших сайтів, які демонстрували технологію цифрового відбитка браузера, має подібність до «BrowserPrint», але набір параметрів трохи менший.

2.4.2. Дані про основну систему без анонімізації

Цифрові відбитки «Canvas», «WebGL», «AudioContext» з основної системи мають значення, оскільки у віртуальній машині вони будуть іншими навіть без застосування додаткових засобів для їхньої заміни [52]. Завдання – переконатися у наявності можливості змінювати їх багаторазово.

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

Метод проверки	Результат
Заголовки HTTP proxy	нет
Открытые порты HTTP proxy	нет
Открытые порты web proxy	нет
Открытые порты VPN	нет
Подозрительное название хоста	нет
Разница во временных зонах (браузера и IP)	IP: 2018-05-29 07:56 (Europe/Amsterdam) браузер: 2018-05-29 7:56
Принадлежность IP к сети Tor	нет
Режим браузера Turbo	нет
Принадлежность IP хостинг провайдеру	нет
Определение web proxy (JS метод)	нет
Утечка IP через Flash	нет
Определение туннеля (двусторонний пинг)	высокая анонимизация (не можем проверить)
Утечка DNS	нет данных об используемых DNS
VPN fingerprint	нет
Утечка IP через WebRTC	нет

Рисунок 2.2 – Перевірка на сайті «2ip.ua»

Важливо, що цей ресурс не зміг визначити DNS-адреси та факт приладдя IP до хостинг-провайдера «HostSailor». Це є недоліком сайту, а не гідністю VPN-сервера. Наприклад, сайт ipqualityscore.com впізнала IP-адресу як належить «HostSailor» і відповідно привласнила йому статус «підозрілого». Імовірність такого розпізнавання існує при використання практично будь-яких VPN-сервісів та VPS-хостингів, проте вона значно нижче, ніж адрес мережі Tor.

Для наочного порівняння наведемо результат цієї перевірки для VPN провайдера «ProtonVPN» (в режимі безкоштовного доступу):

Метод проверки	Результат	
Заголовки HTTP proxy	нет	👍
Открытые порты HTTP proxy	нет	👍
Открытые порты web proxy	нет	👍
Открытые порты VPN	500/udp, IPSec	👎
Подозрительное название хоста	нет	👍
Разница во временных зонах (браузера и IP)	IP: 2018-04-10 10:17 (Asia/Tokyo) браузер: 2018-04-10 8:17	👎
Принадлежность IP к сети Tor	нет	👍
Режим браузера Turbo	нет	👍
Принадлежность IP хостинг провайдеру	нет	👍
Определение web proxy (JS метод)	нет	👍
Утечка IP через Flash	нет	👍
Определение туннеля (двусторонний пинг)	обнаружен	👎
Утечка DNS	нет данных об используемых DNS	👍
VPN fingerprint	MTU 1365	👎
Утечка IP через WebRTC	нет	👍

Рисунок 2.3 – Приклад незадовільного результату

Очевидно, що тут не було виставлено відповідного часового поясу, проти решти трьох параметрів залежить саме від налаштувань сервера. Тестування на сайті «Whoer» показало, що витік реального IP через «WebRTC» не відбувається, але є витік внутрішньомережевої адреси (10.8.0.2), яка побічно свідчить про наявність VPN. Після включення до uBlock відповідної опції («Prevent WebRTC from leaking local IP addresses») даний витік блокується. Альтернативний спосіб: встановити параметр «media.peerconnection.ice.proxy_only = true» у конфігурації Firefox. Результат аналогічний до дії uBlock. Після цього даний сайт не виявляє жодних ознак використання анонімайзера:

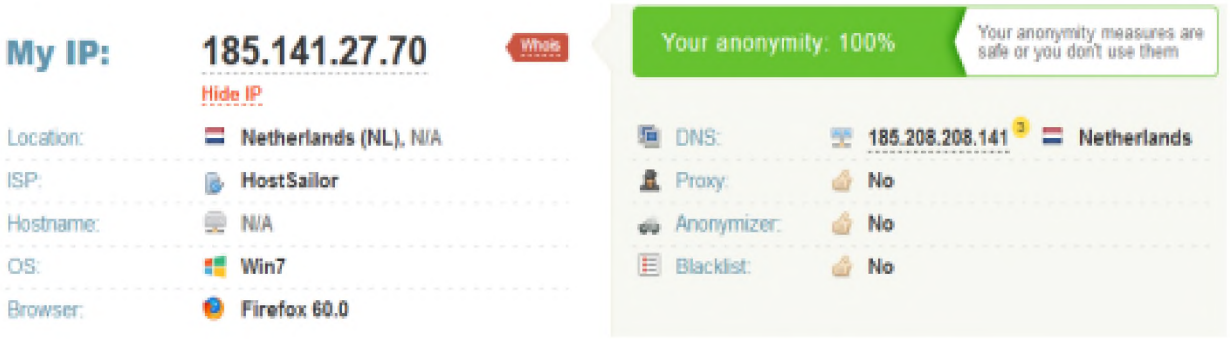

Рисунок 2.4 – Тест на сайті «Whoer.net»

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

```
First seen    = 2018/06/05 14:54:39
Last update   = 2018/06/05 14:57:15
Total flows   = 6
Detected OS   = Windows 7 or 8
HTTP software = Firefox 10.x or newer (ID seems legit)
MTU           = 1500
Network link  = Ethernet or modem
Language      = English
Distance      = 7

PTR test      = Probably home user
Fingerprint and OS match. No proxy detected (this test
No OpenVPN detected.
```

Рисунок 2.5 – Відповідь сайту «witch.valdikss.org»

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

IP	HOSTNAME	ISP	COUNTRY
146.185.176.36		RIPE-ERX-146-185-0-0	NL
82.196.9.45		Digital Ocean, Inc.	NL
185.208.208.141		Hostio Solutions B.V.	NL

Рисунок 2.6 – Перевірка адрес DNS

Один із варіантів цифрового відбитка браузера наведено нижче.

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

Рисунок 2.7 – Цифровий відбиток браузера з «Panopticlick.eff.org

Відбиток «Canvas» на сайті «BrowserLeaks» має такий формат:

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

Рисунок 2.8 – Випадковий «Canvas Fingerprint» з «CanvasBlocker»

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

1)

Signature	✓ 5BEB984A
Uniqueness	100% (0 of 258561 user agents have the same signature)

2)

Signature	✓ B305455D
Uniqueness	99.97% (88 of 258561 user agents have the same signature)

3)

Signature	✓ A4E1854E
Uniqueness	× False (Tor Browser signature)

Рисунок 2.9 – Відбіитки «HTML5 Canvas»

1– Відбиток без використання заміни

2 – Випадковий відбиток при увімкненому «CanvasBlocker»

3 – Статична заміна з опцією «ResistFingerprinting»

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

Network Filters Detection :	
HTTP Proxy	✓ not detected
Tor Browser Detection :	
TOR Relay IP	✓ not detected
Tor Browser Ports	✓ not detected
HTML5 Canvas Protection	✓ not detected
WebGL Blocking (NoScript)	✓ not detected
CSS Fonts Protection	✓ not detected
Adblock Detection :	
AB Type	! Adblock for Mozilla Firefox

Рисунок 2.10 – Перевірка на сайті «BrowserLeaks»

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

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

Рисунок 2.11 – Вихідний відбиток «WebGL у «VirtualBox»

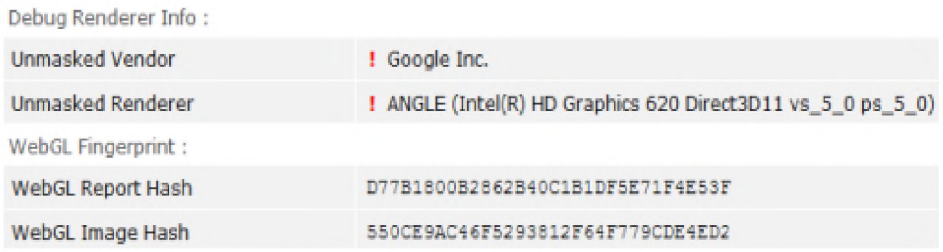

Рисунок 2.12 – Відбиток після підміни

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

Відбитки шрифтів:

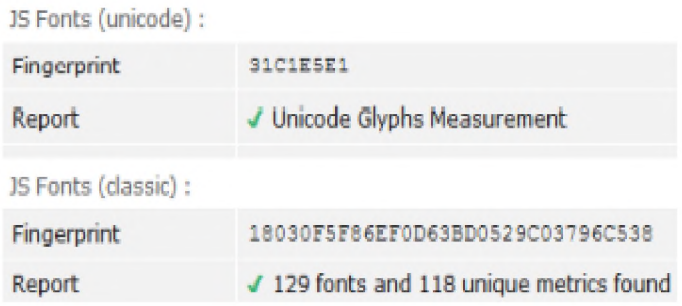

Рисунок 2.13 – Відбиток шрифтів до підміни

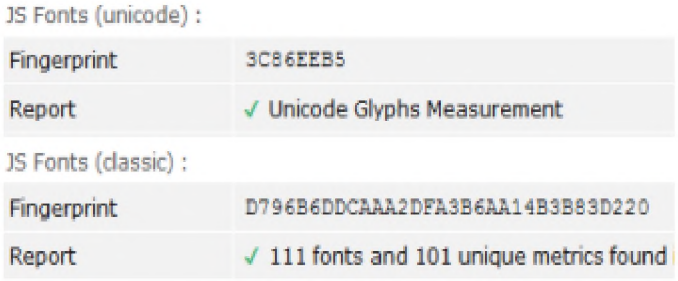

Рисунок 2.14 – Відбиток шрифтів після підміни

Приклади «Audio Fingerprint» були отримані на сайті «vektort13.pro» через більш компактне уявлення, ніж на «openwpm.com».

Рисунок 2.15 – Вихідні відбитки «AudioContext»

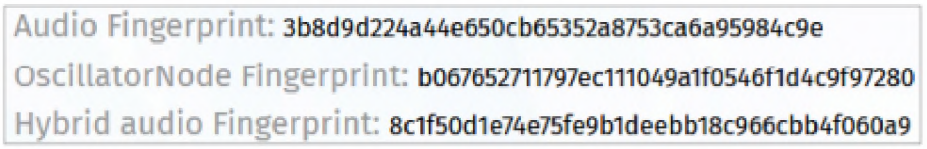

Рисунок 2.16 – Випадкові відбитки «AudioContext»

У ході тестування було підтверджено можливість зміни цифрових відбитків необмежену кількість разів («Canvas», «WebGl Image», «Audio Fingerprint») або, як мінімум, неодноразової заміни (шрифти, «User-agent», дозвіл екрана, «WebGL Render», «ClientRects» та ін.) [52].

2.5. Висновки до розділу 2

У спеціальній частині розроблено готове середовище користувача в якому забезпечується:

- захист від виявлення відвідуваними сайтами будь-якої інформації про вихідну систему та браузер, які використовуються для неанонімної активності;

- шифрування трафіку, що прокладається через обладнання провайдера, включаючи DPI систему, COPM-3 та інші;

- реалізована можливість неодноразової зміни цифрових відбитків;

- виключена можливості витоку реального IP в анонімному браузері;

- організовано захист від виявлення використання засобів анонімізації на відвідуваних сайтах;

- організовано невизначеність для систем аналізу трафіку щодо присутності VPN або Tor.

Запропонована конфігурація програмного забезпечення виявляється ефективною у протидії різним сучасним методам відстеження, забезпечуючи високий рівень захисту та функціональності. Важливим елементом цієї конфігурації є надійна ізоляція анонімного браузера від неанонімної системи. Це не тільки ускладнює можливість відстеження користувача через веб-додатки та рекламні мережі, але і гарантує, що інформація про користувача не переходить між анонімним та звичайним браузерами.

Крім того, конфігурація забезпечує захист від розкриття реальних даних про систему, що є критичним аспектом забезпечення анонімності. Використання ефективних методів шифрування та блокування витоків інформації дозволяє уникнути можливих атак та зберегти конфіденційні дані.

Також важливо підкреслити успішність налаштування OpenVPN щодо маскування. Це забезпечує додатковий шар захисту, роблячи важчим виявлення і слідування за інтернет-з'єднанням користувача.

Проте, варто враховувати деякі обмеження та нюанси. Підключення VPN через Tor, хоч і можливе, але менш надійне з точки зору анонімності, порівняно з використанням лише Tor. Крім того, зауважимо, що операційні системи типу Windows, зазвичай, не рекомендується для анонімної роботи, і можливо, бажано розглядати спеціальні Linux-дистрибутиви, які забезпечують вищий рівень анонімності та безпеки. Ці обмеження слід враховувати при виборі оптимального рішення для конкретних потреб користувача.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Запропоновано підхід до створення і впровадження методів протидії відстеженню та ідентифікації користувача задля забезпечення інформаційної безпеки підприємства при роботі з інтернет ресурсами.

Метою даного розділу є обґрунтування економічної доцільності розробки і впровадження методів протидії відстеженню та ідентифікації користувача, зокрема, і політики безпеки інформації загалом. Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрати на придбання і налагодження складових системи анонімізації або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проєктування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на створення і впровадження структурної схеми методів протидії відстеженню та ідентифікації користувача задля забезпечення інформаційної безпеки підприємства при роботі з інтернет ресурсами визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації, до яких належать наступні:

$t_{тз}$ – тривалість складання технічного завдання, $t_{тз}$=15;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо, $t_в$=20;

$t_м$ – тривалість програмування за готовою блок-схемою, $t_м$=25;

$t_р$ – тривалість опрацювання програми на ПК, $t_м$=40;

$t_д$ – тривалість підготовки технічної документації, $t_д$=10.

Отже,

$$t = t_{тз} + t_в + t_м + t_р + t_д = 15 + 20 + 25 + 40 + 10 = 110 \text{ годин.} \quad (3.1)$$

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}. \quad (3.2)$$

$$К_{рп} = З_{зп} + З_{мч} = 22000 + 844{,}8 = 22844{,}8 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 110 * 200 = 22000 \text{ грн.}, \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, 200 грн./годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t * С_{мч} = 110 * 7{,}68 = 844{,}8 \text{ грн.}, \quad (3.4)$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P_e \cdot t \cdot C_e + \frac{Ф_{перв} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} \quad (3.5)$$

де: P_e – встановлена потужність ПК;

t – трудомісткість створення моделі;

C_e – енерговитрати;

$Ф_{перв}$ – первісна вартість ПК на початок року;

$Н_а$ –річна норма амортизації на ПК;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення;

$F_р$ –річний фонд робочого часу (за 40-годинного робочого тижня).

Первісна вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$\text{Смч} = 0{,}8 \cdot 4 \cdot 1{,}68 + \frac{9100*0{,}30}{1920} + \frac{8400*0{,}2}{1920} = 5{,}38 + 1{,}42 + 0{,}88 = 7{,}68 \text{ грн} \quad (3.6)$$

Для реалізації запропонованого підходу може бути використано стандартне апаратне забезпечення, яке вже наявне на підприємстві, тому капітальні витрати не виникають.

Витрати на налагодження системи анонімізації становитимуть 2500 грн.

Вирішення певних технічних завдань потребує залучення аутсорсингових організації, вартість послуг котрих складає 15000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$\begin{aligned} К &= К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = \\ &= 22844{,}8 + 15000 + 2500 = 40344{,}8 \text{ грн.} \end{aligned} \quad (3.7)$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи анонімізації.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи анонімізації складають:

$$С = С_{в} + С_{к} + С_{ак}, грн. \quad (3.8)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи анонімізації ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$Ск = Сн + Са + Сз + Сел + Со + Стос, грн. \quad (3.9)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 8000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$Сз = Зосн + Здод, грн. \quad (3.10)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 20500 грн. Додаткова заробітна плата – 5% від основної заробітної плати.

Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки.

Отже,

$$С_З = (20500 * 12 + 20500 * 12 * 0{,}05) * 0{,}2 = 51660 \text{ грн.} \quad (3.11)$$

Ставка ЄСВ для всіх категорій платників з 01.01.2024 р. складає 22%.

$$С_{єв} = 51660 * 0{,}22 = 11365{,}2 \text{ грн.} \quad (3.12)$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Сел), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Це, \text{грн.}, \quad (3.13)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

$F_р$ – річний фонд робочого часу системи анонімізації ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0{,}9 * 1920 * 1{,}68 = 2903{,}04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи анонімізації визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 40344,8 *0,02 = 806,9 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 8000 + 51660 + 11365{,}2 + 2903{,}04 + 806{,}9 = 74735{,}14 \text{ грн.} \quad (3.14)$$

Витрати, викликані активністю користувачів системи анонімізації ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів.

За статистичними даними активність користувачів складає 26%. Тому, отримуємо:

$$С_{ак} = 40344{,}8 * 0{,}26 = 10489{,}65 \text{ грн.} \quad (3.15)$$

Таким чином, річні поточні витрати на функціонування системи анонімізації складають:

$$С = 74735{,}14 + 10489{,}65 = 85224{,}79 \text{ грн.} \quad (3.16)$$

3.3 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 18000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 16500 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 15 осіб;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1200 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 5000 грн.;

I – число атакованих сегментів корпоративної мережі, 2;

N – середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.17)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок втрати анонімності:

$$Пп = \frac{\Sigma Зс}{F} * tn \quad (3.18)$$

$$Пп = \frac{16500 * 15}{176} * 4 = 5626 \text{ грн.},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.19)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$Пви = \frac{Σ3c}{F} * tви \quad (3.20)$$

$$Пви = \frac{16500 * 15}{176} * 6 = 8437{,}5 \text{ грн.},$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв = \frac{Σ3o}{F} * tв \quad (3.21)$$

$$Ппв = \frac{18000 * 1}{176} * 2 = 204{,}55 \text{ грн.},$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$Пв = 8437{,}5 + 204{,}55 + 5000 = 13642{,}05 \text{ грн.} \quad (3.22)$$

Втрати від зниження очікуваного обсягу прибутків за час простою анонімізації визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} * (tn + tв + tви) \quad (3.23)$$

$$V = \frac{1200000}{2080} * (4 + 2 + 6) = 6923 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U = 5625+13642,05 +6923=26190,05 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = Σi \cdot Σn \cdot U \quad (3.24)$$

$$B = Σ2 \cdot Σ10 \cdot 26190{,}05 = 523801 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи анонімізації

Загальний ефект від впровадження системи анонімізації задля інформаційної безпеки визначається з урахуванням ризиків порушення згідно наступної формули:

$$E = \text{В} \cdot R - C \text{ грн.}, \quad (3.25)$$

де В – загальний збиток від атаки у разі перехоплення інформації, грн.;

R – вірогідність успішної реалізації загрози (25%);

С – щорічні витрати на експлуатацію системи анонімізації.

Загальний ефект від впровадження системи анонімізації визначається з урахуванням ризиків порушення інформаційної безпеки, отже було розраховано:

$$\text{Е} = 523801 * 0{,}25 - 85224{,}79 = 45725{,}46 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності системи анонімізації

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій ($\text{Т}_\text{о}$).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи анонімізації:

$$\text{ROSI} = \frac{\text{Е}}{\text{К}} \text{, частки одиниці,} \quad (3.26)$$

де Е – загальний ефект від впровадження системи анонімізації грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$\text{ROSI} = 45725{,}46 \,/\, 40344{,}8 \;=\; 1{,}13 \text{ частки одиниці}$$

Проєкт визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{\text{деп}} - N_{\text{інф}})/100), \tag{3.27}$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1{,}13 > (6 - 5)/100 \;=\; 1{,}13 > 0{,}01.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$\text{T0} = \frac{\text{K}}{\text{E}} = \frac{1}{\text{ROSI}} \text{ ,,} \tag{3.28}$$

$$T_0 = \; 1 \,/\, 1{,}13 \;=\; 0{,}88 \text{ року } (10{,}5 \text{ місяців}).$$

3.6 Висновок до розділу 3

Отже, згідно з наведеними розрахунками можливо зробити висновок, що обґрунтування підходу до створення і впровадження методів протидії відстеженню та ідентифікації користувача задля забезпечення інформаційної безпеки підприємства при роботі з інтернет ресурсами є економічно доцільним.

Капітальні витрати, які складають 40344,8 грн., дозволяють отримати ефект величиною 45725,46 грн. Відповідно до отриманих значень показників економічної ефективності можна зазначити, що такий підхід дозволить отримувати 1,13 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт

повернення інвестицій ROSI складає 1,13 грн.). Термін окупності при цьому складатиме 10,5 місяців.

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об'єктів прав інтелектуальної власності) та кількістю об'єктів прав інтелектуальної власності, право на авторство яких може бути порушеним.

ВИСНОВКИ

У ході дослідження було здійснено аналіз сучасних методів ідентифікації користувачів та відстеження їхньої активності в Інтернеті. Це саме по собі було одним із завдань даної роботи – збір та аналіз розрізнених фактів із найрізноманітніших джерел з метою систематизувати цю інформацію та перейти від неофіційного обговорення "анонімності" до наукового дослідження. Були виконані етапи аналітичного огляду, проектування та експериментів. У результаті була отримана конфігурація програмного комплекту, що поєднує ряд позитивних аспектів. Значною мірою була підтверджена початкова гіпотеза у тому, що високий рівень захисту досягається без шкоди функціональності браузера.

Спроектована система має і очевидні недоліки, найбільш істотна – високі системні вимоги. Віртуальна машина з Windows займає значний обсяг місця на жорсткому диску та в оперативної 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 нестачу пам'яті в системі. В результаті, швидкодія віртуальної машини – незадовільне. Далеко не кожен користувач матиме досить потужний ПК із великим запасом оперативної пам'яті. Використовується ланцюжок «VPN через Tor», при всіх його перевагах, може бути визнана анонімною лише за умови, що клієнту вдалося зберегти анонімність при реєстрації та особливо при оплаті VPN-сервісу або VPS-хостингу. Для цього, очевидно, він уже повинен мати надійний інструментом анонімізації - отже, такий клієнт може просто не потребуватиме додаткових заходів захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анонімна поведінка [Електронний ресурс]. Режим доступу: URL: http://hiddengate.i2p.xyz/wiki/Анонімна поведінка (дата звернення: 18.10.2022).

2. Безсонова Є.Є., Зікратов І.А., Росков В.Ю. Аналіз способів ідентифікації користувача в мережі Інтернет. *Науково-технічний вісник інформаційних технологій, механіки та оптики*. 2012. № 6 (82). С. 21- 33.

3. Васильєв В. Browser Fingerprint – анонімна ідентифікація браузерів [Електронний ресурс]. Режим доступу: URL: https://habr.com/company/oleg-bunin/blog/321294/.

4. Визначаємо користувачів VPN (та їх налаштування) та проксі з боку сайту [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/216295/.

5. Встановлення OpenVPN на CentOS 7 [Електронний ресурс]. Режим доступу: URL: https://secfall.com/anonimnost-v-internete-svoimi-rukami-ustanovka-i-nastroyka-vpn servera/.

6. Встановлення та налаштування SoftEther VPN Server [Електронний ресурс]. Режим доступу: URL: https://secfall.com/ustanovka-i-nastroyka-soft-etther-vpn/.

7. Глущенко О. Чек-лист перевірки анонімності серфінгу[Електронний ресурс]. Режим доступу: URL: https://habr.com/post/263557/.

8. Голованов В. ООН зарахувала шифрування та анонімність в Інтернеті до прав людини [Електронний ресурс]. Режим доступу: URL: https://habr.com/aricle/356760/

9. Гленн Грінвальд. Чому важлива недоторканність приватного життя: TED Talk [Електронний ресурс]. Режим доступу: URL: https://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript.

10. Фінгерпринтінг браузера. Як відстежують користувачів у Мережі [Електронний ресурс].

11. Завантажити онлайновий сервіс, що є віртуально неможливим до блоку [Електронний ресурс]. Режим доступу: URL: https://www.propublica.org/article /meet-the-online-tracking-device-that-is-virtually impossible-to-block.

12. Кирилін Д.А. Глибоко ешелонована анонімність [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/147792/.

13. Козлюк А. Ви маєте право на анонімність. [Електронний ресурс]. Режим доступу: URL: https://habr.com/company/digitalrightscenter/blog/329050.

14. Анонімність та безпека в Інтернеті., [Електронний ресурс]. URL: https://www.6262.com.ua/news/3425371/anonimnist-v-interneti-pid-cas-vijni-dobirka-sposobiv-ta-servisiv,

15. Кричевський В. Думки про ідеальну анонімність: Блог компанії Whoer.net [Електронний ресурс]. Режим доступу: URL: https://vctr.media/ua/pravo-zalyshytysya-v-tini-yak-pidpryyemczi-mytczi-ta-aktyvisty-vykorystovuyut-anonimnist-162191/

16. Лопаніцин А. Анонімності немає [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/254217/.

17. Макаренко Г. Freedom House перевів Україну в розряд країн з невільним інтернетом: Суспільство [Електронний ресурс]. Режим доступу: URL: https://babel.ua/news/70409-freedom-house-v-ukrajini-panuye-chastkova-svoboda-v-interneti .

18. Методи анонімності у мережі. [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/204266/.

19. Що таке мережа Tor та як вона працює [Електронний ресурс]. Режим доступу: URL: https://exbase.io/uk/wiki/shho-take-merezha-tor .

20. У Firefox виявлено 0-day вразливість, що використовується для атак на користувачів Tor [Електронний ресурс]. Режим доступу: URL: https://habr.com/companies/eset/articles/316524/

21. Обережніше з копіпастом: фінгерпринтінг тексту недрукованими символами [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/352950.

22. Організація роботи на ОС Whonix/Runion [Електронний ресурс]. Режим доступу: URL: https://lwplxqzvmgu43uff.onion.rip/viewtopic.php?id=11369.

23. Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2022). *Тези доповідей на VII Всеукраїнській науково-практичній конференції: 23-25 листопада 2022 р., м. Дніпро* / Укладачі Іванченко О.В., Вашерук О. В. Дніпро, Дніпровський національний університет імені Олеся Гончара, Кременчук: Видавництво «НОВАБУК». 2022. 212 с.

24. Петренко С. Чому приватність важлива, навіть якщо вам нема чого приховувати [Електронний ресурс]. Режим доступу: URL: https://blognot.co/011002.

25. Попередження криптографії на основі еліптичних кривих: Шифрування VPN [Електронний ресурс]. Режим доступу: URL: https://privateinternetaccess.com/pages/vpn encryption#ecc_warning.

26. Порівняння протоколів VPN/vpnMentor [Електронний ресурс]. Режим доступу: URL: https://ua.vpnmentor.com/blog/порівняння-протоколів-vpn-pptp-vs-l2tp-vs-openvpn-vs sstp vs-ikev2/.

27. Проект SAFE. Базові засади інформаційної безпеки [Електронний ресурс]. Режим доступу: URL: https://www.simplilearn.com/top-cyber-security-projects-article

28. Райтман М.А. Мистецтво легального, анонімного та безпечного доступу до ресурсів Інтернет. Х., 2017. 624 с.

29. Рекомендовані налаштування безпеки для Firefox/cryptopunks [Електронний ресурс]. Режим доступу: URL: https://cryptopunks.org/article/firefox -secure-tweak.

30. Савчук І. Технологія Port knocking [Електронний ресурс]. Режим доступу: URL: http://blogerator.org/page/pozadi-zakrytyh-dverej-port-knocking-bezopasnost-dostupa knockd zaschita-ssh-1.

31. Сагайдак С., Вовк С. Протидія відстеженню та ідентифікації користувачів інтернету. *VII Всеукраїнська науково-практична конференція «ПЕРСПЕКТИВНІ НАПРЯМКИ СУЧАСНОЇ ЕЛЕКТРОНІКИ, ІНФОРМАЦІЙНИХ ТА КОМП'ЮТЕРНИХ СИСТЕМ» MEICS-2021 23-25 листопада 2022 р., Дніпро, Україна.* Дніпро, 2022. С. 19-21.

32. Самозахист від стеження [Електронний ресурс]. Режим доступу: URL: https://ssd.eff.org/ua

33. Створюємо OpenVPN-сервер. Анонімно орендуємо VPS: Захист інформації [Електронний ресурс]. Режим доступу: URL: https://lwplxqzvmgu43uff.onion.rip/viewtopic.php?id=14778

34. Робимо «шпигунську флешку» із захищеною ОС Tails [Електронний ресурс]. Режим доступу: URL: https://www.nexus.ua/anonimnaya-operatsionnaya-sistema-tails

35. Віртуальні приватні мережі нового покоління. [Електронний ресурс] URL: https://freehost.com.ua/ukr/faq/articles/vps-hosting-freehostua-zseredini/

36. Цатурян Т.Ш. Огляд методів розпізнавання відвідувачів веб-ресурсів. *Молодіжний науково-технічний вісник.* 2014. №1. С. 17-23.

37. Що таке VPS, принцип роботи: Технічна документація [Електронний ресурс]. Режим доступу: URL: https://freehost.com.ua/ukr/faq/wiki/vps-vds-chto-eto/.

38. Що таке атаки перетину та підтвердження [Електронний ресурс]. Режим доступу: URL: https://www.pgpru.com/faq/anonimnostjobschievo prosy#h37444-7.

39. Юнусов Т. Tor та нові альтернативи в галузі забезпечення анонімності [Електронний ресурс]. Режим доступу: URL: https://habr.com/articles/357186/

40. Як зберегти анонімність у мережі: повне керівництво [Електронний ресурс]. Режим доступу: URL: cryptoworld.su/як-зберегти-анонімність-в-мережі-повно/

41. Anonymity Bibliography [Electronic resource]. Access mode: URL: https://www.freehaven.net/anonbib/full/date.html.

42. Cao Y., Li S., Wijmans E. (Cross-) Browser Fingerprinting via OS and Hardware Level Features [Electronic resource]. Access mode: URL: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf

43. Do not confuse Anonymity with Pseudonymity: DoNot [Electronic resource]. Access mode: URL:https://www.whonix.org/wiki/DoNot

44. Efros A. Трішки анонімний [Електронний ресурс]. Режим доступу: URL: https://habr.com/post/191448/

45. Fitzmaurice F. OpenVPN with Modern Cryptography [Electronic resource]. Access mode: URL: https://www.maths.tcd.ie/~fionn/misc/ec_vpn.php

46. Norte J.C. Advanced Tor Browser Fingerprinting: Security[Electronic resource]. Access mode: URL: http://jcarlosnorte.com/security/ 2016/03/06/advanced-tor browser-fingerprinting.html.

47. Positive Technologies. Виявлено спосіб деанонімізації користувачів за допомогою "звукових відбитків" [Electronic resource]. Access mode: URL: https://www.researchgate.net/figure/Operational-steps-of-the-deanonymization-attack-against-a-user-of-an-anonymization_fig3_315971174

48. Positive Technologies. У мережі Tor виявлено 110 активних вузлів, що відстежують [Electronic resource]. Access mode: URL: https://tb-manual.torproject.org/uk/troubleshooting/

49. Rutkowska J. Software compartmentalization vs. physical separation [Electronic resource]. Access mode: URL: https://invisiblethingslab.com /resources/2014/Software_compartmentalization_vs_physic l_sep aration.pdf

50. Saini K. Squid Proxy Server 3.1: Beginner's Guide. Packt Publishing Ltd, 2011. 308 p.

51. Things NOT to Do [Electronic resource]. Access mode: URL: https://www.whonix.org/wiki/DoNot

52. Timpanaro J.P., Chrisment I., Festor O. Monitoring the I2P network. France, 2011. C. 5-7.

53. Tor (The Onion Router) – як стати анонімним в інтернеті / Нові інформаційні технології, лютий 2013. URL: https://technari.com.ua/ua/services/about-company/articles/anonymous/.

54. Tor Network Status/TorStatus [Electronic resource]. Access mode: URL: https://torstatus.blutmagie.de/#Stats

55. Tor: Pluggable Transports: Documentation [Electronic resource]. Access mode: URL: https://www.torproject.org/docs/pluggable-transports.html.enю

№	Формат	Найменування	Кількість листів	Примітки

Додаток А. Відомість матеріалів дипломної роботи

Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	43	
6	А4	Спеціальна частина	28	
7	А4	Економічний розділ	11	
8	А4	Висновки	1	
9	А4	Список використаних джерел	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	2	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	1	
16		Матеріали дипломної роботи на оптичному носії		Оптичний диск

Додаток Б. Вміст конфігураційного файлу сервера OpenVPN

```
port 443
proto tcp
dev tun
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
topology subnet
max-clients 200
ca ca.crt
cert server.crt
key server.key
dh none
tls-crypt tc.key
crl-verify crl.pem
mssfix 0
client-to-client
push "dhcp-option DNS 10.8.0.1"
ping 10
ping-restart 120
push "ping 10"
push "ping-restart 120"
persist-tun
cipher AES-256-GCM
tls-version-min 1.2
ncp-ciphers AES-256-GCM:AES-256-CBC
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-
SHA256:TLS-ECDHEECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
remote-cert-tls client
```

```
tls-server
status-version 2
script-security 2
sndbuf 393216
rcvbuf 393216
reneg-sec 2592000
hash-size 1024 1024
verb 3
mute 3
replay-window 128
compress
log /dev/null
```

Додаток В. Вміст конфігураційного файлу кліенту OpenVPN

```
client
dev tun
dev-type tun
remote 185.141.27.70 443 tcp
nobind
persist-tun
cipher AES-256-GCM
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256:TLS-ECDHEECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
verb 4
mute 10
mssfix 0
ping 10
ping-restart 120
hand-window 70
server-poll-timeout 4
reneg-sec 2592000
sndbuf 393216
rcvbuf 393216
remote-cert-tls server
tls-client
compress
block-outside-dns
script-security 2
auth-nocache
<ca>
# -----CERTIFICATE-----
```

```
</ca>
<tls-crypt>
# OpenVPN static key
</tls-crypt>
<cert>
# -----CERTIFICATE-----
</cert>
<key>
# -----PRIVATE KEY-----
</key>
```

Додаток Г. Установки конфігурації браузера Firefox

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

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

browser.safebrowsing.enabled = false

browser.safebrowsing.downloads.enabled = false

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

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

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

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

dom.battery.enabled = false – не відстежувати рівень заряду батареї.

dom.network.enabled = false – не визначати параметри з'єднання з мережею (При цьому передається тип з'єднання).

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

geo.enabled = false - відключення геолокації.

media.navigator.enabled = false

media.navigator.video.enabled = false - відключення взаємодії з мікрофоном та камерою.

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

webgl.disable-extensions = true

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

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

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

dom.webaudio.enabled = false - відключення AudioContext API (на даний момент на даний момент вже існують доповнення для боротьби з Audio fingerprinting).

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

Додаток Ґ. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 92 б. (« відмінно »).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

Додаток Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 125м-22-3
Скорохода Максима Сергійовича на тему: «Методи протидії відстеженню та ідентифікації користувачів інтернету»

Кваліфікаційна робота магістра представлена пояснювальною запискою на 107 с., містить 16 рис., 1 табл., 6 додатків, 55 джерел.

Метою кваліфікаційної роботи є забезпечення анонімності користувача під час роботи в мережі Інтернет. Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека».

Для досягнення поставленої мети в кваліфікаційній роботі проаналізовано сучасні методи забезпечення анонімності в Інтернет, фактори, за якими можливо відстеження користувача під час роботи в мережі та шляхи витоку даних, що призводять до порушення анонімності.

У спеціальній частині була спроектована система для шифрування трафіку, можливості зміни цифрових відбитків і захисту від витоку реального IP. Запропонована конфігурація програмного забезпечення ефективно протистоїть методам відстеження, зокрема завдяки надійній ізоляції анонімного браузера від звичайної системи.

В економічному розділі визначено капітальні витрати на програмні розробки, їх економічну доцільність доведено.

Практичне значення роботи полягає у розв'язанні проблем анонімності в Інтернеті та протидії цензурі та відстеженню.

Результати проведених у кваліфікаційній роботі досліджень можуть бути використані при розробці анонімної системи для протидії відстеженню або для забезпечення безпеки.

Наукова новизна дослідження полягає у розробці імплементації комплексних заходів забезпечення анонімності в Інтернеті.

В якості недоліків слід відзначити наступне: недотримання графіка проведення розробки, нечіткість окремих висновків і визначень.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, що висуваються до кваліфікаційної роботи магістра та заслуговує на оцінку « 85 / добре », а її автор Скороход М.С., присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
д.т.н., доц. каф. БІТ Сафаров О.О.

Керівник спеціальної частини,
Ас. каф. БІТ Мілінчук Ю.А.