НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧА В КОНТЕКСТІ КІБЕРБЕЗПЕКИ ВЕББРАУЗЕРІВ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Москаленко Олексій Іванович

Керівник: доктор філософії
Слатвінська Валерія Миколаївна

Рецензент: к.т.н., доцент
Ахмаметьева Ганна Валеріївна

Одеса - 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Москаленко Олексія Івановича

1. Тема роботи: «Методологія забезпечення анонімності користувача в контексті кібербезпеки веббраузерів»
Керівник роботи: доктор філософії Валерія Миколаївна Слатвінська
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «27» травня 2025 року
3. Дата видачі завдання «16» вересня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області та пошук науково технічної інформації за темою роботи	Вересень жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота над другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	12.06.2025	

Здобувач _____Москаленко О.І._____
(підпис) (прізвище та ініціали)_

Керівник роботи _____Слатвінська В.М._____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему "Методологія забезпечення анонімності користувача в контексті кібербезпеки веббраузерів" на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 15 рисунків, 3 таблиці. 1 Додаток А. 24 літературних джерел. Робота виконана на 50 сторінках загального тексту і 39 сторінках основного тексту.

Метою є аналіз механізмів забезпечення анонімності у веб-браузерах, систематизація інструментів захисту та розробка рекомендацій для мінімізації ризиків профілювання користувачів. Досліджено вразливості браузерів, методи збору даних та технології захисту, такі як VPN, проксі-сервери та мережа Tor. Реалізовано метод зміни HTTP-заголовків і маскування ідентифікаторів за допомогою Selenium. Розроблено рекомендації щодо захисту від Browser Fingerprinting та налаштування браузера для приватності.

Результати роботи можуть бути використані при розробці нових стандартів конфіденційності в браузерах, створенні навчальних матеріалів з захисту приватності та впровадженні принципів privacy by design у веб-розробці.

Можливими напрямками подальших досліджень є вдосконалення методів протидії технікам ідентифікації користувачів через браузер

АНОНІМНІСТЬ, БРАУЗЕР, VPN, TOR, ПРОКСІ-СЕРВЕР, BROWSER FINGERPRINTING, HTTP-ЗАГОЛОВКИ, USER-AGENT, ЗАХИСТ ДАНИХ.

ABSTRACT

The qualification work titled "Methodology for Ensuring User Anonymity in the Context of Web Browser Cybersecurity" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, includes 15 figures, 3 tables, and 1 Appendix A. It references 24 literary sources. The work is presented in 50 pages of total text, with 39 pages of main text.

The aim of the work is to analyze mechanisms for ensuring anonymity in web browsers, systematize protection tools, and develop recommendations for minimizing the risks of user profiling. The research examines browser vulnerabilities, data collection methods, and protection technologies such as VPN, proxy servers, and the Tor network. A method for changing HTTP headers and masking identifiers using Selenium has been implemented. Recommendations have been developed for protecting against Browser Fingerprinting and configuring browsers for privacy.

The results of this work can be used in the development of new privacy standards for browsers, creating educational materials on privacy protection, and implementing privacy-by-design principles in web development.

Potential areas for future research include improving methods for countering user identification techniques through browsers.

ANONYMITY, BROWSER, VPN, TOR, PROXY SERVER, BROWSER FINGERPRINTING, HTTP HEADERS, USER-AGENT, DATA PROTECTION.

ЗМІСТ

ВСТУП

У даній роботі буде висвітлена проблема анонімності в мережі, яка має аспекти, що охоплюють технічні, соціальні та правові виміри. З одного боку, користувачі прагнуть зберегти контроль над своїми персональними даними та цифровою ідентичністю, з іншого - комерційні структури та державні органи активно розвивають інструменти профілювання та відстеження активності в Інтернеті. Для вирішення цієї проблеми у роботі буде створена багаторівнева система методологій забезпечення анонімності, яка дозволить мінімізувати або повністю усунути цифровий слід користувача, зберігаючи при цьому високий рівень зручності.

Мета дослідження полягає у комплексному аналізі методологій забезпечення анонімності користувача у веб-браузерах та розробці практичних технічних рішень для ефективного маскування цифрового сліду з акцентом на автоматизацію зміни ідентифікаційних параметрів браузера.

Завдання дослідження:

1. Провести теоретичний аналіз вразливостей сучасних браузерів щодо збереження анонімності та дослідити архітектурні недоліки, які уможливлюють відстеження користувачів.
2. Здійснити порівняльний аналіз ефективності існуючих інструментів анонімізації, зокрема VPN-сервісів, Tor-мережі та спеціалізованих розширень.
3. Розробити практичний інструментарій для автоматизованої зміни HTTP-заголовків та інших ідентифікаційних параметрів браузера.
4. Сформувати комплексний підхід до забезпечення анонімності, орієнтований на практичне застосування з оптимальним балансом між рівнем захисту та зручністю користування.

Об’єкт дослідження - методи та технології забезпечення анонімності користувача в контексті кібербезпеки веб-браузерів, зокрема механізми збору та

аналізу даних при веб-серфінгу, технології відстеження через цифрові відбитки браузера та системи захисту особистих даних у мережі Інтернет.

Предмет дослідження - комплексна методологія забезпечення анонімності користувача в контексті кібербезпеки веб-браузерів, зокрема через автоматизовану зміну HTTP-заголовків та інших ідентифікаційних параметрів.

Актуальність дослідження підтверджується динамікою законодавчих змін, зокрема впровадженням аналітичних систем відстеження діяльності користувачів[2], та розривом між правовими ініціативами та технологічними можливостями відстеження, що робить розробку ефективних інструментів анонімізації особливо важливою.

Практична значимість роботи полягає у створенні алгоритмів та програмних рішень, здатних автоматизувати процес зміни цифрових ідентифікаторів користувача, пропонуючи просту альтернативу Tor Browser із мінімальною втратою рівня анонімності. Результати дослідження можуть стати основою для:

1. Розробки нових стандартів конфіденційності в браузерах;
2. Створення навчальних матеріалів у сфері кібербезпеки;
3. Оптимізації архітектури веб-додатків з урахуванням принципів privacy by design;[18]
4. Практичного застосування користувачами, які потребують підвищеного рівня приватності без значних обмежень у зручності.

Основні висновки бакалаврської роботи були опубліковані у тезах «Використання Python для анонімізації веб-запитів» на науковій конференції «V Міжнародній науково-практичній конференції «Кібербезпека в сучасному світі: актуальні виклики[1], що свідчить про їхню апробацію та наукову значимість

1. ТЕОРЕТИЧНІ ОСНОВИ АНОНІМНОСТІ ТА БЕЗПЕКИ В ІНТЕРНЕТІ

1.1 Концепція анонімності в контексті кібербезпеки

Анонімність - це здатність людини або групи осіб приховувати свою справжню особистість чи характеристики, які могли б сприяти їхній ідентифікації. Тобто треті особи не повинні мати можливості пов'язати дії користувача з його реальними даними - іменем, адресою проживання, контактною інформацією тощо.

Анонімність створює парадокс, з одного боку, захищає певні групи, з іншого - ускладнює боротьбу з кіберзлочинністю. Вирішення цього парадоксу вимагає балансу між технічними рішеннями в шифруванні та правовими нормами в регулюванні збору данних.

Сама анонімність рідко буває абсолютною і тісно переплітається з поняттями конфіденційності та псевдонімності.[3]

1. Конфіденційність - це право вирішувати хто матиме доступ до інформації про вас.Наприклад коли ми надсилаємо приватне повідомлення другу в месенджері, ми не ховаємо свою особу, але обмежуємо коло тих хто може побачити це спілкування.
2. Псевдонімність - це використання постійного альтер-его замість справжнього імені. Це створення онлайн персони - можливо, блогер чи гравець - де треба підтримуватицю ідентичність роками. Люди знають вас як Персону але не знають, хто ви насправді.

Всі ці концепції перетинаються та доповнюють одна одну. Наприклад, журналіст-розслідувач може використовувати псевдонім для публікацій (псевдонімність), захищати свої джерела від розкриття (конфіденційність) і час від часу збирати інформацію, не розкриваючи своєї присутності (анонімність).

1.1.1 Значення та класифікація анонімності

Анонімність відіграє важливу роль у забезпеченні прав і безпеки користувачів. Вона має кілька ключових аспектів:

1. Свобода висловлювань. Анонімність дозволяє відкрито обговорювати чутливі питання без страху переслідувань, що є особливо важливим для дисидентів, викривачів корупції та вразливих груп. Водночас вона створює ризики безвідповідальної поведінки, дезінформації та токсичного контенту.[2]
2. Захист персональних даних. Відсутність публічної прив'язки до особистої інформації зменшує ймовірність цілеспрямованих атак, доксингу та соціальної інженерії.
3. Приватність і цифрова безпека. Обмеження збору персональних даних допомагає зменшити вплив цифрового стеження такого як таргетована реклама та алгоритми формування рекомендацых у ленті Фейсбуку, телеграма та інших соціальних мереж.

Як я вже повторював раніше анонімність особливо важлива в «Свобода висловлювань» для таких певних груп як:

1. Журналісти, які працюють у країнах з авторитарними режимами і потребують захищених каналів комунікації для збору та передачі інформації
2. Правозахисники, яким необхідно захищати конфіденційність своїх джерел та власну безпеку
3. Дослідники, що працюють із соціально чутливими темами та потребують неупередженого збору даних

Анонімність - це не просто технічне поняття, а складний соціально-психологічний конструкт. Її можна розглядати як своєрідний «щит» що захищає особистість людини в інтернет просторі від небажаного зовнішнього втручання, спостереження та контролю.

1.2 Уразливості веб-браузерів, які можуть розкрити особистість користувача

Навіть при відсутності прямого введеня персональних даних в інтернеті таких як платіжна інформація або логіни, є багато технічних параметрів які дозволяють ідентифікувати особу. В цьому підрозділі я буду розглядати ключові механізми браузерів які і формують так званий цифровий слід користувачів

1.2.1 IP-адреса як інструмент геолокації

Почнемо з найпростішого - IP-адреса є унікальним ідентифікатором пристрою в мережі, який використовується для передачі даних. Вона розкриває географічне положення користувача особливо при підключені до Wi-fi [10] бо провайдери часто прив’язують Ip-адреи до регионів, міст тощо, це дозволяє легко відстежити активність користувача. Для мінімізації ризиків ми розглянемо технології маскування, такі як VPN, проксі або Tor.

1.2.2 User-Agent: технічний профіль браузера

Абсолютно кожен браузер автоматично передає серверам ряд технічних даних у заголовку User-Agent, включаючи версію ОС, тип браузера та його налаштування. Версію операційної системи (Windows 10).

1. Тип і версію браузера (Chrome 90).
2. Архітектуру процесора (64-біт).

Ця інформація може бути частиною унікального цифрового профілю. Рідкісні комбінації, як-от нестандартні ОС чи застарілі версії браузерів, роблять вас менш схожими на інших користувачів.

1.2.3 Cookies та скрипти відстеження

Файли cookies зберігають данні авторизації, часто використовуються рекламними мережами для збору інформації про поведінку користувача. Наприклад, трекери фіксують переглянуті сторінки або пошук в інтернеті, час перебування на сайті та вподобання. Ці дані будуть формувати таргетовані реклами.

1.2.4 Браузерний відбиток (Browser Fingerprinting)

Цей метод ідентифікації базується на унікальній комбінації параметрів браузера: розширень [12],встановлених шрифтів, роздільності екрана, часового поясу тощо. На відміну від cookies, відбиток генерується динамічно і не залишає даних на пристрої. Зменшити унікальність можна за допомогою спеціалізованих браузерів (наприклад, Tor) або ручного обмеження налаштувань.

На рисунку 1.1 зображено схему, що ілюструє процес цифрової ідентифікації користувача в інтернеті.

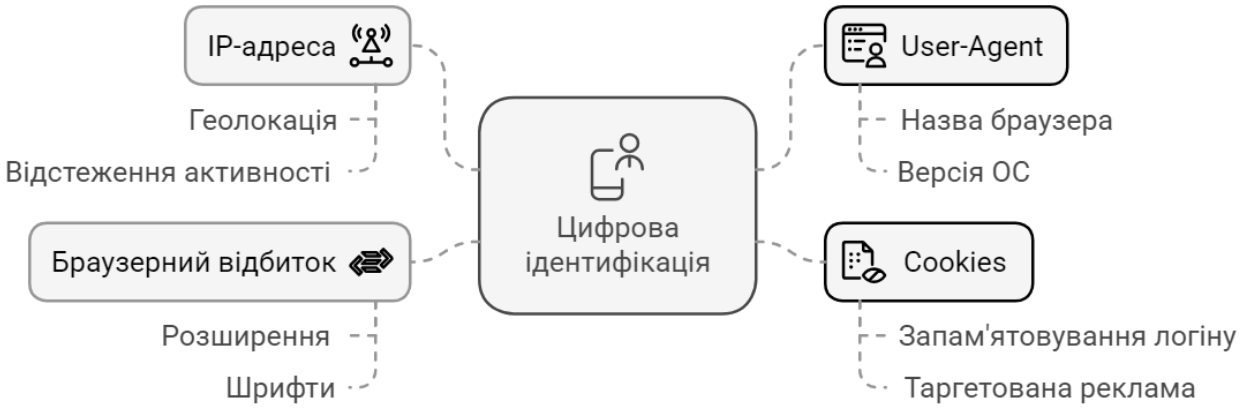

Рисунок 1.1 - Методи збору даних для цифрової ідентифікації

1.3. Методи збору даних про користувача

Збір даних про користувача є ключовим етапом у багатьох системах, які спрямовані на персоналізацію послуг, аналіз аудиторії або надання цільової підтримки. Існує кілька методів збору даних, які можна поділити на активні та пасивні. У цьому підрозділі ми зосередимося на активних методах, зокрема на заповненні полів, коли користувач самостійно вводить свої дані, наприклад, під час участі в акціях (як-от знижки в піцерії) або при отриманні гуманітарної допомоги (наприклад, "допомога від ООН").

1.3.1 Метод збору інформаціїї через онлайн-анкети

Активний збір даних через заповнення полів має ризики шахрайства та зловживання інформацією. Наприклад, зловмисники створюють фальшиві форми, що імітують програми на кшталт "допомоги від ООН", і поширюють їх через месенджери (Viber, Telegram) або email, обіцяючи фінансову підтримку. Користувачі, які заповнили такі анкети, можуть зіткнутися з шахрайством: через кілька тижнів їм телефонують із невідомих номерів, пропонуючи кредити чи "акційні" товари, або навіть погрожують. Дані часто продаються на чорному ринку для цільових шахрайських схем. Особливо вразливі люди похилого віку, які не завжди можуть розпізнати шахрайську форму, що підриває довіру до легітимних гуманітарних програм.

Нижче приведений основний вигляд анкети яку заповнюють люди:

1. Ім’я, прізвище та дату народження;
2. Склад сім’ї (кількість дітей, їхній вік);
3. Адресу проживання або тимчасового перебування;
4. Контактні дані (телефон, електронна пошта);
5. Соціальний статус (наприклад, чи є особа біженцем, чи має інвалідність);

1.3.2 Веб-аналітика (Google Analytics)

Веб-аналітика, зокрема Google Analytics, є одним із найпоширеніших пасивних методів автоматичного збору даних про поведінку користувачів на вебсайтах. Цей інструмент вбудовується на сайт за допомогою JavaScript-коду і автоматично фіксує широкий спектр інформації без необхідності активної участі користувача

Google Analytics відстежує:

1. Шляхи навігації: які сторінки відвідує користувач і в якому порядку; Тривалість перебування: скільки часу користувач проводить на кожній сторінці;
2. Джерела трафіку: звідки прийшов користувач (органічний пошук, платна реклама соціальні мережі, прямі переходи, тощо);
3. Дії користувача: кліки, заповнення форм, покупки та інші взаємодії з контентом.

Крім того, Google Analytics автоматично збирає демографічні дані [24] (вік, стать, країна) та технічну інформацію (тип пристрою, операційна система, браузер) через інтеграцію з cookies та обліковими записами Google. Це дозволяє створювати детальні звіти про аудиторію, ефективність сайту та рекламних кампаній.

На рисунку 1.2 представлено звіт Google Analytics, який демонструє загальну кількість сесій (11,368,561), середню тривалість сесії (333 секунди), розподіл трафіку за джерелами, популярні сторінки, географію користувачів та типи пристроїв.

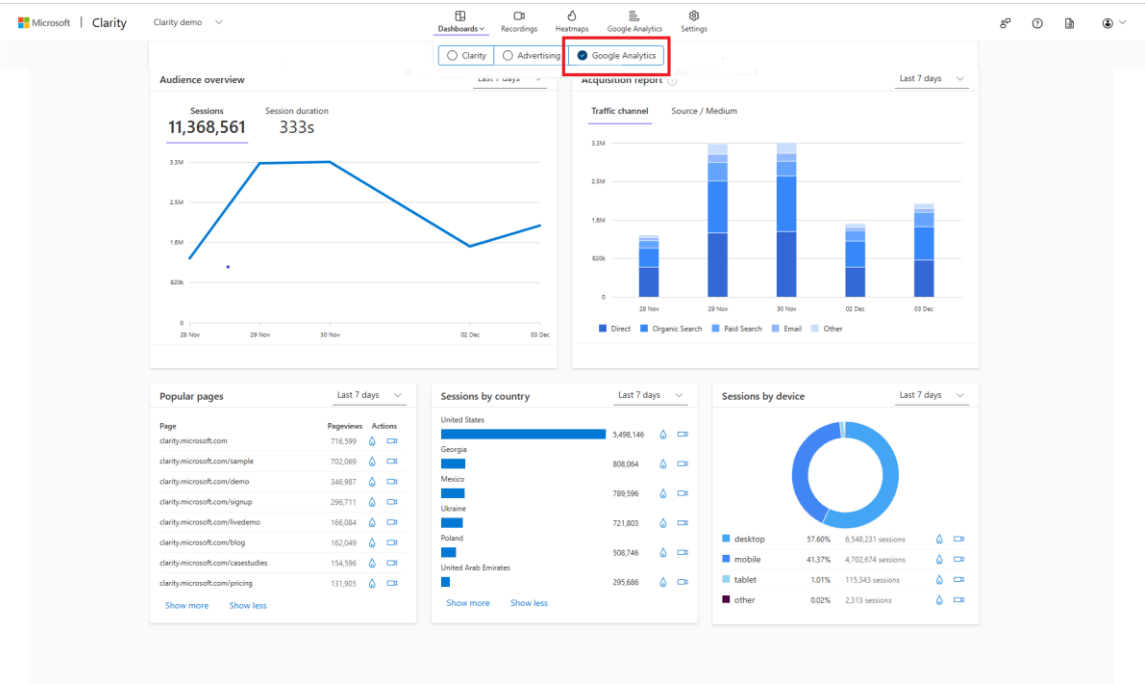

Рисунок 1.2 - інформація та звіт з Google Analytics

1.3.3 Більш шкідливі методи збору інформаціїї

1. Фішинг через підроблені точки Wi-Fi (Evil Twin)

Як працює: Хакер створює фальшиву Wi-Fi точку доступу з назвою, схожою на легітимну (наприклад, "CoffeeShop_Free" замість "CoffeeShop_WiFi"). Користувач підключається, а весь його трафік проходить через зловмисника.

Що можна зібрати: Незахищені паролі, відвідані сайти, cookies сесій.

Цікава деталь: Простота - достатньо портативного роутера чи ноутбука з програмою типу Aircrack-ng. Користувач навіть не підозрює, що його дані перехоплюють.

Інструменти: Kali Linux, WiFi Pineapple.

2. Соціальна інженерія через "загублений" USB-накопичувач

Як працює: На флешку записується файл (наприклад, "Зарплата_2025.xls.exe") з трояном. Її "випадково" залишають у людному місці. Цікавість змушує людину підключити флешку до комп’ютера.

Що можна зібрати: Доступ до файлів, паролі, віддалене керування пристроєм.

Цікава деталь: Метод спирається на людську природу, а не на складні технології. Ефективність досягає 60-70% - люди не можуть встояти перед спокусою зазирнути.

Інструменти: Простий скрипт (наприклад, через Metasploit) + флешка за $5.

3. Аналіз метаданих із фото чи документів

Як працює: Користувач ділиться фотографією в соцмережах чи месенджерах. Хакер завантажує файл і витягує метадані (EXIF) - геотег, модель камери, дату зйомки.

Що можна зібрати: Точне місце перебування, звички, тип пристрою.

Цікава деталь: Не потрібні складні інструменти - достатньо ExifTool чи навіть онлайн-сервісів. Люди часто не знають, що їхні фото "говорять".

Інструменти: ExifTool, будь-який HEX-редактор.

1.4. Загрози приватності користувачів

Алгоритми які збирають дані з різних джерел такі як соціальні мережі, історії пошуку, покупки в інтернеті - створюють точний портрет кожної людини в інтернеті, вони довзоляють:

1. Оцінити психологічні характеристики: вподобання, страхи, слабкості.
2. Дізнатися фінансові звички: скільки людина витрачає, яку картку використовує.
3. Зібрати біометричні дані: відбитки пальців, голос, фотографії з соцмереж.

У цього можуть бути як психологічні наслідки так і фінансові:

1. Маніпуляція споживчою поведінкою: Якщо часто шукаєте дитячі товари, алгоритми почнуть показувати вам рекламу з високими цінами, орієнтуючись на вашу материнську інтуїцію. Додатково, служби доставки можуть підвищити ціни для користувачів, які часто роблять замовлення вночі.
2. Політичний вплив**:** У час виборів профілювання може використовуватися для персоналізованої агітації. Наприклад, молодим людям показують

рекламу екологічних ініціатив, а старшим - повідомлення про соціальні гарантії.

3. Інформаційний купол: Користувачеві показують лише ту інформацію, яку він хоче побачити, приховуючи альтернативні погляди. Це створює ілюзію "правильного" консенсусу, навіть якщо він є тільки в межах цієї бульбашки.
4. Продаж даних: Додатки для відстеження фізичної активності можуть продавати ваші дані страхових компаній. Наприклад, низька активність може призвести до підвищених тарифів на медичне страхування.

Компанії можуть передавати дані стороннім організаціям, таким як маркетингові агенції чи страхові компанії. Як результат, вас можуть турбувати дзвінки від рекламодавців або страхових агентів, які пропонуватимуть свої товари чи послуги. Більше того, якщо ваші дані будуть продані без вашої згоди, це може спричинити фішингові атаки або навіть крадіжку вашої особистої інформації.

1.4.1 Витоки даних

Витоки даних можуть відбуватись через слабкий захист з боку компаній[2] або навіть через внутрішні загрози, коли співробітники продають дані конкурентам або шахраям. Як наслідок, ваші особисті дані можуть потрапити до зловмисників. Реальні наслідки витоків даних:

1. Фінансові втрати: Використання даних карток для покупок у "чорному" інтернеті або створення фальшивих кредитних історій.
2. Крадіжка особистості: Шахраї можуть створювати фальшиві профілі, використовувати ваші фото для реклами заборонених товарів, або навіть відкрити рахунки на ваше ім'я для відмивання грошей.
3. Фізична небезпека: Витік адреси може призвести до пограбувань. Наприклад, якщо зловмисники знають ваш час перебування вдома, вони можуть організувати пограбування.

2. МЕТОДИ ТА ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ

2.1 Virtual Private Network - принцип роботи

Один з основних методів забезпечення анонімності є - використання VPN (Virtual Private Network). У цьому підрозділі детально розглянемо принципи роботи VPN, проаналізуємо популярні сервіси, а також з'ясуємо, на що звертати увагу під час вибору VPN-провайдера.

Як працює VPN: покроковий процес [5]

1. Ініціація з'єднання
    1) Користувач запускає VPN-клієнт: Ви встановлюєте програму VPN (наприклад, NordVPN, ExpressVPN) на своєму пристрої (комп'ютері, телефоні тощо) і обираєте сервер, до якого хочете підключитися (наприклад, у США чи Німеччині).
    2) Автентифікація: Ваш пристрій надсилає запит на сервер VPN. Ви вводите свої облікові дані (якщо потрібно), і сервер перевіряє, чи маєте ви доступ до послуги.
2. Встановлення тунелю
    1) Тунель: VPN створює так званий "тунель" - захищений канал між вашим пристроєм і сервером VPN. Цей тунель ізолює ваш трафік від зовнішнього світу.
    2) Протоколи тунелювання: Для цього використовуються спеціальні протоколи, наприклад:
        1. OpenVPN: Відкритий код, надійний, широко використовується.
        2. IPSec/IKEv2: Швидкий і безпечний, популярний на мобільних пристроях.
        3. WireGuard: Сучасний, легкий і швидкий.

Як це відбувається?: Ваш пристрій і сервер домовляються про параметри тунелю (наприклад, який протокол і ключі шифрування використовувати).

3. Шифрування даних

1. Шифрування в дії: Перед відправкою трафік (наприклад, запит до сайту google.com) шифрується на вашому пристрої за допомогою алгоритму, наприклад AES-256 (Advanced Encryption Standard із ключем 256 біт).

- Приклад шифрування:

1. Без шифрування (без VPN): Ваше повідомлення «Вікіпедія» відправляється через інтернет у чистому вигляді як текст. Якщо (наприклад, хакер у громадському Wi-Fi) "підслухає" ваше з'єднання, він легко побачить, що саме ви написали.
2. З VPN: Перед відправкою ваше повідомлення "Вікіпедя" перетворюється на зашифрований набір символів, наприклад, "Xy7kP9mQw2...". Це виглядає як випадковий набір букв і цифр, який ніхто не зрозуміє без спеціального ключа. VPN-сервер, до якого ви підключені, має цей ключ і може розшифрувати повідомлення назад у "Вікіпедя а потім передати його на сайт. Усі, хто намагатиметься перехопити дані між вами і VPN-сервером, побачать лише незрозумілий код

2. Ключі шифрування: У процесі шифрування ваш пристрій і сервер обмінюються ключами (зазвичай за допомогою асиметричного шифрування, як RSA), щоб потім використовувати симетричне шифрування (наприклад, AES) для швидкості.

4. Передача даних через тунель

1. Ваш зашифрований запит (наприклад, "Xy7kP9mQw2...") надсилається через тунель до сервера VPN. Зовні видно лише, що ваш пристрій спілкується з IP-адресою сервера VPN, але що саме передається - невідомо
2. Ваш інтернет-провайдер (ISP) бачить лише зашифрований трафік і адресу VPN-сервера, а не кінцевий пункт призначення (наприклад, google.com).

5. Розшифрування на сервері VPN
    1. Сервер VPN отримує ваш зашифрований запит ("Xy7kP9mQw2..."), розшифровує його за допомогою спільного ключа і бачить оригінальний запит ("Вікіпедя» або відвідування google.com).
    2. Потім сервер перенаправляє цей запит до кінцевого пункту призначення (наприклад, до серверів Google).
6. Отримання відповіді
    1. Кінцевий сервер (наприклад, Google) надсилає відповідь (наприклад, сторінку пошуку) назад до сервера VPN.
    2. Сервер VPN знову шифрує цю відповідь і відправляє її через тунель назад до вашого пристрою.
7. Розшифрування на вашому пристрої
    1. Ваш VPN-клієнт отримує зашифровану відповідь, розшифровує її і передає до вашого браузера чи програми. Ви бачите результат - наприклад, сторінку Google.

Повний цикл: приклад

1. Ви хочете відвідати сайт www.example.com..
2. VPN-клієнт шифрує запит: "GET www.example.com." → "Kj9pLm2x...".
3. Зашифрований запит іде через тунель до сервера VPN у Лондоні.
4. Сервер у Лондоні розшифровує "Kj9pLm2x..." → "GET www.example.com." і надсилає його до www.example.com.
5. Сайт повертає сторінку (наприклад, HTML-код) до сервера VPN.
6. Сервер шифрує відповідь і відправляє назад: "Qw7nBx9..." → ваш пристрій.
7. Ваш пристрій розшифровує "Qw7nBx9..." і показує сайт у браузері.

На рисунку 2.1 узагальнено покроковий процес встановлення та функціонування VPN-з'єднання: від запуску VPN-клієнта користувачем і створення зашифрованого тунелю до передачі, розшифрування та отримання даних. Схема ілюструє, як саме дані шифруються, передаються через VPN-сервер і повертаються у зворотному напрямку, забезпечуючи конфіденційність і анонімність користувача в мережі.

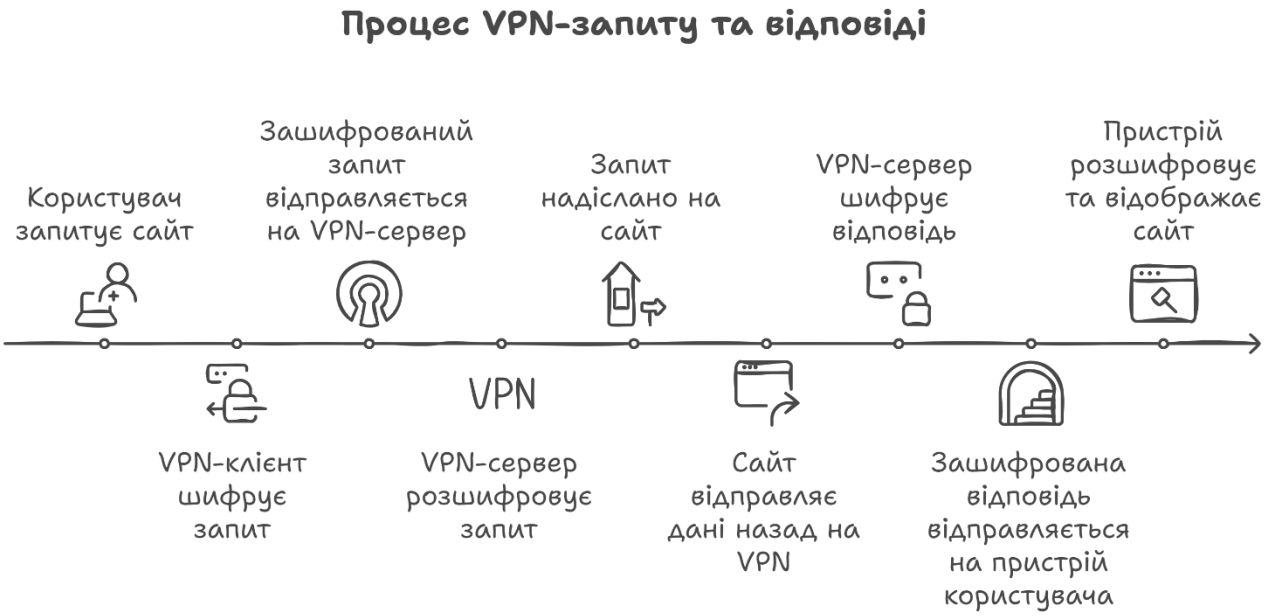

Рисунок 2.1 - Процес з`єднання з VPN-сервісом

VPN працює як посередник, який шифрує ваш трафік, приховує вашу IP-адресу і перенаправляє запити через захищений тунель. Це забезпечує конфіденційність і безпеку, але ефективність залежить від протоколу, алгоритму шифрування (наприклад, AES-256). [5]

2.1.1 Переваги й недоліки VPN

Ця технологія пропонує низку переваг, які роблять її затребуваною як серед всіх користувачів, перейдемо до переваг:

1. Захист конфіденційності: VPN приховує вашу реальну IP-адресу, замінюючи її адресою сервера VPN. Це ускладнює відстеження вашої активності в Інтернеті третіми сторонами, такими як провайдери чи рекламодавці.
2. Шифрування даних: VPN шифрує ваш інтернет-трафік, що робить його недоступним для перехоплення, наприклад, у громадських Wi-Fi-мережах, де ризик атак вищий.

3. Обхід географічних обмежень: Ви можете отримати доступ до контенту, заблокованого у вашому регіоні, підключившись до сервера в іншій країні.
4. Захист від стеження: VPN може допомогти уникнути моніторингу з боку урядів чи корпорацій, особливо в країнах із високим рівнем цензури.
5. Простота використання: Більшість сучасних VPN-сервісів мають зручні інтерфейси, що робить їх доступними навіть для новачків.

Незважаючи на численні переваги, використання VPN не позбавлене певних обмежень і ризиків, серед них можна перечислити:

1. Залежність від провайдера VPN: Якщо VPN-сервіс веде журнали активності (logs), ваша анонімність може бути під загрозою. Довіра до постачальника є ключовою.
2. Зниження швидкості: Шифрування та маршрутизація через віддалений сервер часто уповільнюють з'єднання, що може впливати на перегляд відео чи онлайн-ігри.
3. Не повна анонімність: VPN не захищає від усіх методів відстеження, наприклад, від cookies, цифрових відбитків (fingerprinting) або витоків даних через DNS.
4. Юридичні ризики: У деяких країнах використання VPN для обходу обмежень може бути незаконним, що створює потенційні проблеми для користувача.
5. Вартість: Якісні VPN-сервіси зазвичай платні, і безкоштовні альтернативи часто мають обмеження або менш надійні.

2.1.2 Порівняльний аналіз популярних VPN-сервісів

В цьому підрозділі переглянемо одні з найпопулярніших VPN-сервісів: NordVPN, ExpressVPN, ProtonVPN. Кожен із них обіцяє "швидкість, безпеку і безліч серверів у різних країнах". Розглянемо кілька найвідоміших:

1. NordVPN - це один із найбільших провайдерів VPN із широким вибором серверів і відмінною політикою конфіденційності.

Таблиця 2.1 - Огляд серверів Nord-VPN

Категорія	Опис
Кількість серверів	5000+ (у 60+ країнах)
Переваги	Перевірена політика "no-logs" з офіційними аудитами
	Зручні застосунки для різних ОС
	Широка географія серверів
Недоліки	Можливі перевантаження серверів
	Помітне падіння швидкості на завантажених серверах
Особливості	Один з найбільших провайдерів на ринку
	Висока надійність послуг

2. ExpressVPN - преміум-сервіс із високою швидкістю та простотою використання, ідеальний для вимогливих користувачів.

Таблиця 2.2 - Огляд серверів ExpressVPN

Категорія	Опис
Кількість серверів	Знання кількість
Основні переваги	Стабільно висока швидкість
	Прості у використанні клієнт
	Платформа дозволяє пристрій
Основні недоліки	Висока ціна порівняно з конкурентами
Особливості	Преміум-сервіс з акцентом на якість швидкості

3. ProtonVPN - швейцарський VPN з акцентом на конфіденційність і безкоштовною версією для базових потреб.

Таблиця 2.3 - Огляд серверів ProtonVPN

Категорія	Опис
Кількість серверів	Помірна кількість
Основні переваги	Розташування в Швейцарії
	Прозора політика конфіденційності
	Надійність безкоштовної версії
Основні недоліки	Обмежена кількість у безкоштовній версії
	Обмежена кількість серверів у базовому плані
Особливості	Особливий акцент на приватності та безпеці

2.1.3 Основні критерії вибору VPN-сервісу

1. Швидкість і мережа серверів - Для користувачів, які завантажують великі файли або переглядають потокове відео, важливими є висока швидкість з’єднання та широка мережа серверів. Наявність великої кількості серверів у різних країнах забезпечує стабільність і гнучкість підключення, що підтверджується відгуками користувачів.

2. Функціональні можливості - При виборі VPN варто звернути увагу на додаткові функції, які підвищують безпеку та зручність:

1. Kill Switch: автоматично припиняє доступ до інтернету у разі збою VPN-з’єднання, запобігаючи витоку даних.
2. Подвійний VPN: спрямовує трафік через два сервери для посиленого захисту.
3. Блокування реклами та шкідливих сайтів: захищає від зловмисного програмного забезпечення та відстеження рекламними мережами.

3. Безплатні VPN-сервіси - Безкоштовні VPN часто мають обмеження швидкості, кількості серверів і можуть збирати дані користувачів для продажу

третім сторонам. Для тих, хто цінує анонімність і безпеку, доцільніше обрати платний сервіс із вищим рівнем надійності та конфіденційності.

2.1.4 Юрисдикція та політика збереження логів

Юрисдикція - це країна, у якій зареєстрований VPN-провайдер і де він веде основну діяльність. Чому це важливо?

1. Закони про захист приватності: Наприклад, Швейцарія або Панама мають більш лояльне законодавство у сфері збереження даних.
2. Міжнародні угоди: Деякі країни входять до розвідувальних об'єднань (Five Eyes, Nine Eyes, Fourteen Eyes), що може означати спільний обмін даними між державними органами.

Політика збереження логів (no-logs policy) означає, що VPN-оператор офіційно заявляє, що не записує дані про ваші відвідування сайтів, IP-адреси чи тривалість сесій. Але не всі сервіси однаково чесні в цьому питанні, тож варто звертати увагу на репутацію компанії й те, чи проходила вона аудит незалежних фахівців.

VPN - це один із найдієвіших інструментів, коли йдеться про захист приватності та доступ до заблокованого контенту. Але, щоб отримати максимум користі, важливо обирати надійного провайдера, розуміти принципи роботи VPN і враховувати його обмеження. У наступних розділах ми розглянемо, як VPN порівнюється з іншими методами (проксі, Tor), а також навчимося правильно налаштовувати ці інструменти, щоб максимально приховати свою особистість під час вебсерфінгу.

2.2 Використання проксі-серверів

Проксі-сервери є інструментом для приховування реальної IP-адреси та забезпечення певного рівня анонімності [6] але не повної. Вони використовуються для обходу регіональних обмежень, підвищення конфіденційності та кешування

даних для оптимізації мережевого трафіку. На відміну від VPN, проксі застосовуються переважно для окремих застосунків або протоколів і не шифрують увесь трафік на рівні операційної системи.

2.2.1 Види проксі-серверів

1. HTTP/HTTPS-проксі - Проксі, який працює тільки з веб-трафіком, тобто з тим, що ви робите в браузері (відкриваєте сайти, наприклад).

Особливості:

1. HTTP: Просто передає ваші запити до сайтів без шифрування. Хтось може перехопити дані.
2. HTTPS: Використовує SSL/TLS (шифрування), тому з’єднання безпечніше - ваші дані складніше "підглянути".

Для чого: Перегляд веб-сторінок, обхід блокувань сайтів. HTTPS-проксі краще для безпеки.

2. SOCKS-проксі - Проксі, який працює "глибше" в мережі і може передавати не тільки веб-трафік, а й будь-які інші дані (наприклад, з ігор, торрентів, пошти).

Особливості:

1. SOCKS4: Базова версія, без шифрування.
2. SOCKS5: Сучасніша, підтримує шифрування і автентифікацію (логін/пароль), що робить її безпечнішою.

Для чого: Універсальний інструмент для анонімності в різних програмах, наприклад, для P2P-завантажень чи онлайн-ігор.

3. Анонімні проксі - Проксі, який замінює вашу IP-адресу на свою, щоб сайт не бачив, хто ви насправді.

1. Особливості: Не передає вашу реальну IP-адресу, але рівень анонімності залежить від типу (наприклад, "високоанонімні" ще й приховують, що ви використовуєте проксі).
2. Для чого: Базовий захист приватності, обхід геоблокувань.

4. Прозорі (transparent) проксі - Проксі, який не ховає вашу IP-адресу і не намагається зробити вас анонімним.

1. Особливості: Використовується не для приватності, а для інших цілей - наприклад, щоб прискорити завантаження сайтів (кешування) або контролювати трафік (фільтрація).
2. Для чого: Часто застосовується в школах, офісах чи публічних мережах для управління доступом.

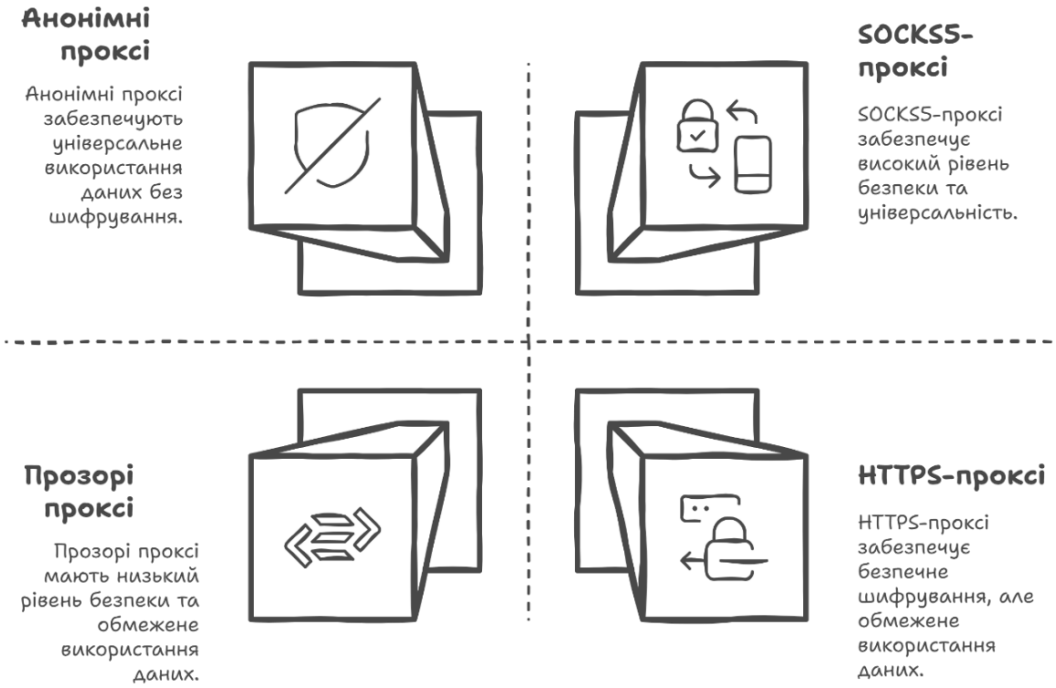

Рисунок 2.2 - Класифікація проксі-серверів

2.2.2 Налаштування проксі-серверів

Для використання проксі необхідно налаштувати відповідні параметри у браузері, операційній системі або застосунку.

1. Налаштування у браузері:
    1. Потрібно перейти у «Розширення» та завантажити ProxySite.
    2. Вибираємо країну та тиснемо «Підключення».

3. Якщо сервер потребує автентифікації, вводяться логін та пароль. Зазвичай це admin - admin

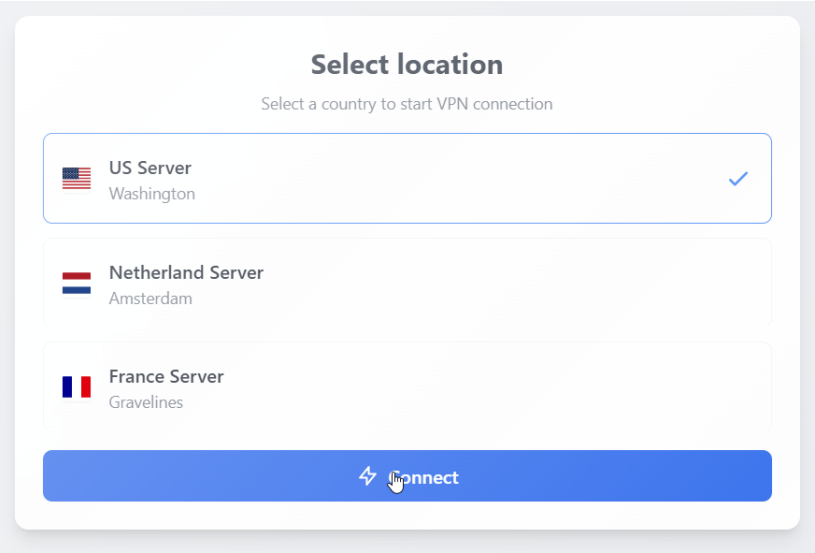

Рисунок 2.3 - Налаштування проксі в браузері

2. Налаштування в операційній системі:
    1. Потрібно зайти на сайт Proxy-sale.com та по ціні «2 долари в місяць» придбати ip-адресу проксі з портом.
    2. У Windows проксі налаштовується через "Параметри мережі та Інтернету" вводимо данні які ми придбали:

Рисунок 2.4 - Налаштування проксі у Windows

2.2.3 Ризики використання проксі-серверів

Проксі-сервери мають деякі ризики при використанні, такі як:

1. Нестабільність безкоштовних сервісів - багато відкритих проксі мають обмежений ресурс, що впливає на швидкість і надійність з'єднання.

2. Вразливість до перехоплення трафіку - якщо проксі не використовує шифрування (крім HTTPS і SOCKS5), передані дані можуть бути перехоплені зловмисниками.
3. Компрометація проксі-сервера - адміністратори проксі можуть вести журнали активності користувачів, що створює ризик витоку конфіденційної інформації.

Проксі-сервери є ефективним рішенням для швидкої зміни IP-адреси або обходу мережевих обмежень, однак у питаннях захисту даних вони значно менш дієві ніж VPN-сервіси, які забезпечують як мінімум шифрування трафіку.

2.3. Технологія Tor: особливості анонімізації трафіку

Загальний принцип роботи Tor Tor (The Onion Router) - це децентралізована мережа, яка забезпечує анонімність користувачів завдяки переспрямуванню трафіку через випадковий ланцюг серверів (вузлів) [4]. Кожен вузол знає лише попередню та наступну ланку маршруту, що ускладнює відстеження кінцевого відправника та одержувача даних.

Багаторівневе шифрування Tor використовує багатошарове шифрування: кожен вузол розшифровує лише один шар даних, розкриваючи адресу наступного вузла. Це забезпечує конфіденційність, оскільки жоден вузол (крім кінцевого) не має повної інформації про маршрут та вміст переданих даних.

2.3.1 Типи вузлів у мережі Tor та маршрути

1. Вхідні вузли (Entry Nodes): приймають трафік від користувача, їхні IP-адреси можуть бути відомі провайдеру.
2. Проміжні вузли (Middle Nodes): передають трафік між вузлами, не знаючи джерела чи призначення.
3. Вихідні вузли (Exit Nodes): передають дані на цільовий сервер, їхні IP-адреси видимі, що може створювати ризик перехоплення незашифрованого трафіку.

Динамічна зміна маршрутів Tor генерує новий ланцюг вузлів для кожного сеансу, що ускладнює аналіз трафіку. Наприклад:

1. Сеанс 1: Вхідний → Проміжний A → Вихідний X
2. Сеанс 2: Вхідний → Проміжний B → Вихідний Y

На рисунку 2.5 зображено динаміку зміни маршрутів Tor через нові вузли для кожного сеансу, що показує, як трафік передається від клієнта до вебсервера через вхідні, проміжні та вихідні вузли.

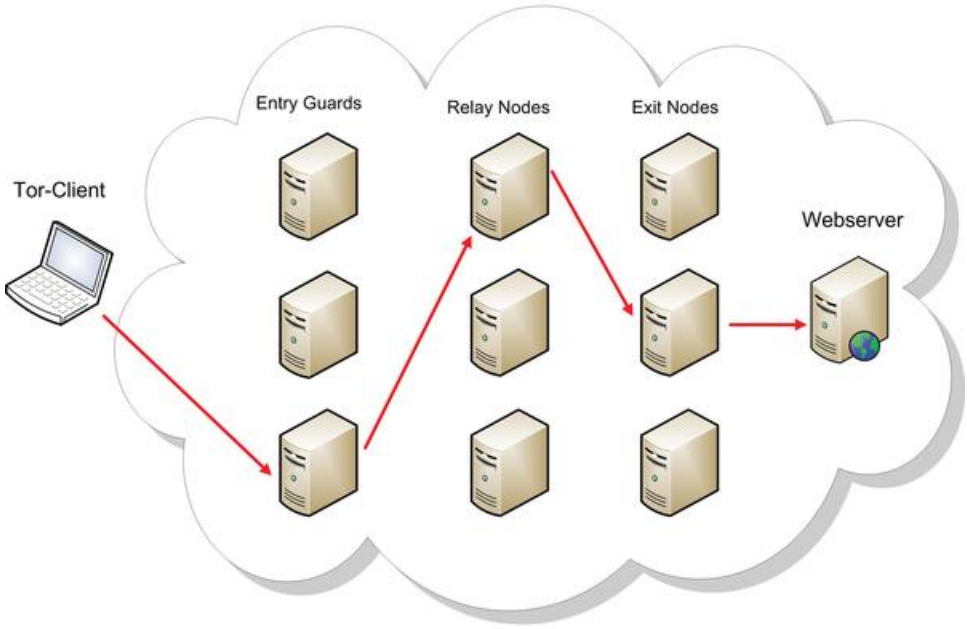

Рисунок 2.5 - Схема маршрутизації трафіку в мережі Tor

2.3.2. Переваги та недоліки технології

Tor забезпечує високий рівень анонімності, приховуючи IP-адресу користувача за допомогою багаторівневого шифрування та випадкових маршрутів трафіку. Крім того, Tor є кросплатформним рішенням, доступним для Windows, macOS, Linux та Android.

Через складний механізм переспрямування ця технологія має обмеження, швидкість з'єднання буде значно нижчою ніж у звичайних мережах. Вихідні вузли потенційно можуть становити загрозу безпеці, якщо передані дані не захищені

шифруванням HTTPS. Деякі сайти блокують підключення з відомих вихідних вузлів Tor, що ускладнює доступ до певних сервісів.

2.3.3 Практичні рекомендації

1. Використовувати офіційний Tor Browser: змінені версії можуть мати вразливості.
2. Відмовитися від плагінів: вони можуть розкрити реальний IP.
3. Завжди перевіряти HTTPS: захистить дані від вихідного вузла до сервера.
4. Не вводити особисті дані: анонімність зникає при розкритті особистої інформації.
5. Оновлювати браузер: для виправлення вразливостей.
6. Комбінувати з VPN: приховує факт використання Tor від провайдера.

2.4. Зміна HTTP-заголовків та маскування браузера

Перейдемо до практичної частини моєї роботи - одного з ключових методів підвищення анонімності користувача є модифікація HTTP-заголовків, зокрема заголовка User-Agent, що вказує на тип браузера, його версію, операційну систему та інші параметри[21]. Зміна або підробка цього заголовка ускладнює створення точного профілю користувача на основі даних про пристрій і тип програмного забезпечення.

User-Agent виступає ідентифікатором, оскільки браузери за замовчуванням надсилають рядок, який включає назву браузера, версію, а також інформацію про операційну систему. Аналітичні сервіси та трекери використовують ці дані для визначення типу пристрою, його налаштувань, а також для точного профілювання користувача.

Причини зміни User-Agent:

1. Приховування реальних характеристик пристрою. Імітація інших пристроїв (наприклад, мобільних).

2. Обхід обмежень доступу на сайтах, наприклад, мобільні версії чи боти

Підробка User-Agent дає можливість досягнути таких результатів:

1. Складно створити точний профіль користувача на основі типу пристрою та програмного забезпечення.
2. Важливо для обмеження доступу, обходу таргетованої реклами та виявлення бот-скриптів.

2.4.1. Практична реалізація: зміна User-Agent у Selenium

У межах практичної частини роботи було реалізовано зміну заголовка User-Agent з використанням бібліотеки Selenium [8]. Основною метою було динамічне формування та встановлення заголовка, що дозволяє підвищити рівень анонімності користувача під час автоматизованої взаємодії з вебресурсами.

По-перше потрібно встановити бібліотеки:

```
pip install selenium webdriver-manager
```

У коді створюються два списки. Списки комбінуються для динамічної генерації унікальних заголовків User-Agent

os_list - список можливих операційних систем та пристроїв (Windows, macOS, Android, iPhone), які використовуються для формування заголовка User-Agent.

```
os_list = [
    "Windows NT 10.0; Win64; x64",
    "Macintosh; Intel Mac OS X 10_15_7",
    "X11; Linux x86_64",
    "Linux; Android 10; SM-G973F",
    "iPhone; CPU iPhone OS 14_0 like Mac OS X"
]
```

Рисунок 2.6 - Показ функції os_list

chrome_versions - список версій браузера Chrome, що дозволяє створювати різні варіанти User-Agent.

```
chrome_versions = [
    "122.0.6261.128",
    "121.0.6167.140",
    "120.0.6099.224",
    "119.0.6045.200",
    "118.0.5993.89"
]
```

Рисунок 2.7 - Показ функії chrome_versions

Далі функція generate_random_user_agent() генерує випадковий заголовок User-Agent. Вона використовує функцію choice(), щоб випадковим чином вибрати операційну систему з списку os_list.

1. Випадковим чином вибирає версію браузера Chrome з chrome_versions.
2. Формує рядок User-Agent у форматі браузера Mozilla з вибраними операційною системою та версією Chrome

```
def generate_random_user_agent():
    os = choice(os_list)
    version = choice(chrome_versions)
    return f"Mozilla/5.0 ({os}) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/{version} Safari/537.36"
```

Рисунок 2.8 - Показ функції generate_random_user_agent()

Інша частина коду яка буде показана нижче - налаштовує браузер Chrome за допомогою Selenium, використовуючи об'єкт Options()

```
options = Options()
custom_user_agent = generate_random_user_agent()

options.add_argument(f'user-agent={custom_user_agent}')
options.add_argument('--disable-gpu')
options.add_argument('--disable-webgl')
options.add_argument('--disable-webrtc')
options.add_argument('--disable-background-networking')
options.add_argument('--disable-client-side-phishing-detection')
options.add_argument('--disable-sync')
options.add_argument('--disable-translate')
options.add_argument('--disable-default-apps')
options.add_argument('--disable-popup-blocking')
options.add_argument('--disable-features=AudioServiceOutOfProcess,WebRtcHideLocalIpsWithMdns')
options.add_argument('--disable-blink-features=AutomationControlled')
```

Рисунок 2.9 - Налаштування браузера з об`єкту Options()

1. user-agent={custom_user_agent} - змінює HTTP-заголовок User-Agent, дозволяючи імітувати різні пристрої та браузери. Це ускладнює трекінг користувача та створення цифрового відбитка.
2. --disable-gpu - вимикає апаратне прискорення графіки, що зменшує можливість ідентифікації через графічний процесор.
3. --disable-webgl - вимикає WebGL (веб-графіку), яка часто використовується для побудови відбитку пристрою.
4. --disable-webrtc - блокує WebRTC, який може розкрити реальну IP-адресу навіть при використанні VPN або проксі.
5. --disable-background-networking - відключає фонові мережеві з'єднання браузера, які можуть автоматично надсилати дані без відома користувача.
6. --disable-client-side-phishing-detection - вимикає клієнтське виявлення фішингу від Google, зменшуючи взаємодію з серверами.
7. --disable-sync - блокує синхронізацію з обліковим записом Google, щоб уникнути передачі особистих даних.
8. --disable-translate - вимикає автоматичний переклад сторінок, який може працювати через зовнішні сервіси.
9. --disable-default-apps - забороняє завантаження стандартних додатків Chrome, які можуть впливати на ідентифікацію.
10. --disable-popup-blocking - відключає блокування спливаючих вікон, щоб уникнути виявлення автоматизованої поведінки.
11. --disable-features=AudioServiceOutOfProcess,WebRtcHideLocalIpsWithMdns - блокує окремі вбудовані функції, що можуть передавати технічні дані про систему.
12. --disable-blink-features=AutomationControlled - приховує той факт, що браузер керується програмно. Важливо для обходу систем виявлення ботів, оскільки приховується navigator.webdriver
13. excludeSwitches=['enable-automation'] - прибирає вказівку, що Chrome запущений у режимі автоматизації. Це знижує ризик блокування з боку сайтів.

14. useAutomationExtension=False - вимикає вбудоване розширення автоматизації Chrome, яке може видати, що браузер працює через Selenium.

Далі була зроблена частина коду яка перевіряє результат на практиці. На Рисунку 2.10 буде показана частина коду яка відповідає за перевірку.[21]

```
try:
    driver.get("https://www.whatismybrowser.com/detect/what-is-my-user-agent/")
    wait = WebDriverWait(driver, 10)
    detected_value = wait.until(EC.presence_of_element_located((By.ID, "detected_value")))
    displayed_user_agent = detected_value.text
    print(f"Встановлений User-Agent: {custom_user_agent}")
    print(f"Визначений User-Agent: {displayed_user_agent}")
    print("✅ User-Agent успішно змінено!" if custom_user_agent in displayed_user_agent else
```

Рисунок 2.10 - Код для перевірки виконання програми

1. Після встановлення нових параметрів браузера через Selenium, браузер направляється на сайт whatismybrowser.com, щоб перевірити, чи змінився User-Agent.
2. За допомогою WebDriverWait я чекаю поки сторінка завантажиться і елемент, що містить значення User-Agent, стане доступним.
3. Після отримання цього значення я порівняв його з встановленим User-Agent. Якщо вони збігаються, скрипт виводить підтвердження про успішну зміну.

Результат отримання інформації з сайту:

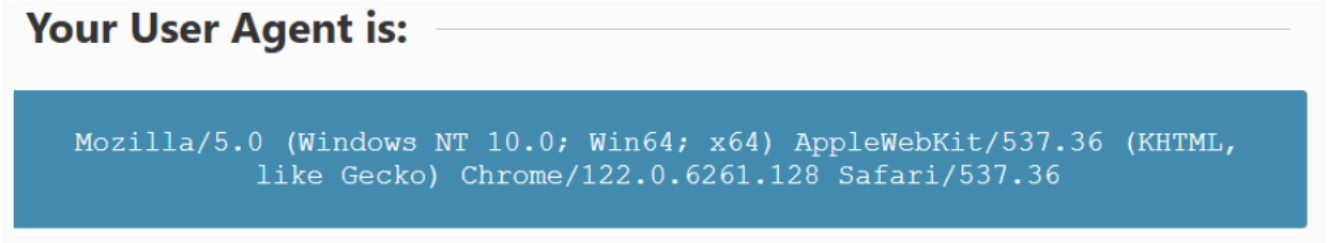

Рисунок 2.11 - Отримання результату з сайта “whatismybrowser.com»

Результат отримання інформації з терміналу виконання коду.

```
DevTools listening on ws://127.0.0.1:64774/devtools/browser/927926c1-394a-4c16-9a87-c3a76628dc7c
[10260:14668:0409/192704.684:ERROR:interface_endpoint_client.cc(725)] Message 0 rejected by interface blink.mojom.WidgetHost
Встановлений User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.128 Safari/537.36
Визначений User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.128 Safari/537.36
✅ User-Agent успішно змінено!
```

Рисунок 2.12 - Отримання результату з терміналу для порівняння

Це дозволяє підтвердити, що зміни, які ви внесли в заголовок User-Agent, були успішно застосовані

У рамках практичної частини було реалізовано автоматизований підхід до зміни HTTP-заголовка User-Agent з використанням Selenium. На Рисунку 2.13 буде показаний повний цикл роботи скрипта.

Рисунок 2.13 Демонастрація повного циклу виконання скрипту.

Увесь реалізований скрипт можна подивитися у “Додаток А”. Результат виконання коду підтвердив правильну зміну заголовка - сайт визначив саме той User-Agent, який був згенерований і встановлений у скрипті. Це свідчить про успішну модифікацію HTTP-запиту на рівні браузера.

Переваги:

1. Динамічна зміна User-Agent при кожному запуску ускладнює ідентифікацію пристрою та підвищує рівень анонімності.
2. Емуляція різних типів пристроїв і браузерів дозволяє обходити обмеження деяких сайтів, які блокують доступ для певних клієнтів.
3. Гнучкість реалізації: списки браузерів і операційних систем легко редагуються або доповнюються під конкретні задачі.

2.5. Browser Fingerprinting та методи захисту

Browser Fingerprinting - це метод ідентифікації користувачів [20] на основі унікальних параметрів їхнього браузера та пристрою. Він дозволяє сайтам збирати специфічні дані навіть без використання cookies. Сайти використовують набір характеристик, які рідко змінюються або унікальні для кожного користувача. До таких параметрів належать:

1. User-Agent - дані про браузер, ОС та їхні версії.
2. Роздільна здатність екрану - розмір екрану та вікна браузера.
3. Встановлені шрифти - різні ОС мають унікальні списки шрифтів.
4. Мовні налаштування - мова інтерфейсу браузера та локалізація.
5. Canvas Fingerprinting - сайт змушує браузер малювати невидиме зображення, аналізуючи дрібні відмінності у його відтворенні.
6. WebGL Fingerprinting - збір даних про відеокарту, оскільки навіть однакові моделі можуть відтворювати графіку з невеликими варіаціями.

Комбінація цих параметрів дозволить створити майже унікальний «відбиток» пристрою, який можна використовувати для відстеження користувачів навіть після очищення кешу чи зміни IP-адреси.

Оскільки fingerprinting використовує набір різних технологій, повністю приховати свою активність складно. Однак є ефективні методи мінімізації ризиків:

1. Використання Tor Browser - Tor уніфікує налаштування браузера для всіх користувачів, роблячи їхні «відбитки» однаковими. Крім того, він блокує JavaScript та WebGL, які часто застосовуються для fingerprinting.
2. Розширення для браузера
    1. uBlock Origin - блокує рекламу, скрипти та трекери.
    2. Privacy Badger - аналізує активність веб-сайтів та блокує ті, що намагаються відстежувати користувача.
    3. NoScript (Firefox) / ScriptBlock (Chrome) - забороняють виконання шкідливих скриптів.

4. HTTPS Everywhere - примусово використовує зашифровані HTTPS-з'єднання для захисту трафіку.

3. Зміна налаштувань браузера (реалізовано у практичній частині Див. 2.4) - деякі браузери мають вбудовані функції для блокування fingerprinting.
4. Використання віртуальних машин або браузерів у режимі "пісочниці" - Це дозволяє запускати браузер у середовищі, яке не залишає унікальних слідів на основному пристрої.

Тож Browser Fingerprinting - це новітній інструмент відстеження, який дозволяє сайтам ідентифікувати користувачів без традиційних трекерів.

3. ПРАКТИЧНІ ПІДХОДИ ТА РЕКОМЕНДАЦІЇ ЩОДО АНОНІМНОСТІ

3.1 Використання неідентифікованих SIM-карт у веббраузерах в цілях анонімності

Після розгляду основних інструментів для забезпечення анонімності у межах веббраузерів, вони не гарантують повну конфіденційність якщо залишаються інші відкриті канали ідентифікації користувача такі як SIM-карти які можуть бути використані для верифікації акаунтів[3], надсилання повідомлень або доступу до мобільного інтернету. Тому наступний розділ присвячено методам підвищення анонімності поза межами браузера, зокрема через використання неідентифікованих SIM-карток та анонімних платіжних засобів, таких як криптовалюти

Можливість використання неідентифікованих SIM-карток значно варіюється залежно від країни:

1. В Україні з 2022 року діє Закон "Про електронні комунікації", що вимагає надання паспортних даних при купівлі SIM-карток.
2. Польща: Туристам доступні передплачені SIM-картки без обов'язкової ідентифікації.
3. Естонія: Існує можливість придбання незареєстрованих карток.
4. Велика Британія: Відсутні суворі вимоги до верифікації особи покупця.

Ці відмінності створюють можливості для отримання SIM-карток, не прив'язаних до реальної особистості користувача, що є першим кроком до анонімної присутності в мережі.

3.1.1 Методи отримання анонімних SIM-карток

Існує кілька поширених способів отримання неідентифікованих SIM-карток:

1. Придбання за кордоном: Купівля карток у країнах з ліберальним законодавством (Польща, країни Балтії).
2. Туристичні SIM-картки: Часто продаються в аеропортах та туристичних зонах без суворої перевірки документів.

3. Віртуальні номери: Сервіси на кшталт Hushed або TextNow надають віртуальні телефонні номери для отримання SMS, що позбавляє необхідності мати фізичну SIM-картку.

3.1.2. Стратегії використання для створення анонімних акаунтів

Основна цінність неідентифікованих SIM-карток - можливість створення та верифікації "липових" акаунтів у соціальних мережах та месенджерах. Ось ефективні стратегії використання:

1. Ізольовані: Одна SIM-картка - один сервіс. Наприклад, одна картка використовується лише для Telegram, інша - лише для Twitter.
2. Комбінування з VPN: Реєстрація акаунта через VPN з IP-адресою тієї країни, де була придбана SIM-картка, значно ускладнює відстеження.
3. Регулярна ротація: Періодична зміна SIM-карток (наприклад, раз на місяць) мінімізує накопичення поведінкових патернів.
4. Одноразове використання: Для особливо чутливих операцій SIM-картка використовується тільки для первинної верифікації акаунта, після чого знищується.

Нижче буде наведено приклад всіх дій для забезспечення анонімності у рамках використання липових Sim-карт

1. Придбання SIM-картки в Польщі без ідентифікації.
2. Активація картки в публічному місці (не вдома/на роботі).
3. Підключення до інтернету через VPN з польським IP.
4. Реєстрація акаунта в соціальній мережі з верифікацією через SMS.
5. Зберігання SIM-картки в безпечному місці або знищення після одноразового використання.

3.1.3 Ризики та заходи безпеки

При використанні анонімних SIM-карток слід враховувати такі ризики:

1. Аналіз метаданих: Час активації, частота використання та інші метадані можуть видати користувача.
2. Геолокація: Підключення до стільникових веж розкриває фізичне місцезнаходження.
3. IMEI пристрою: Використання одного пристрою для різних SIM-карток створює зв'язок між ними.

3.2 Криптовалюти як інструмент анонімності у вебпросторі

Після використання технічних методів ддя забезпечення анонімності, потрібно забезпечити собі фінансову анонімність яка також важлива у контексті використання веббраузерами. Звичайні способи оплати, такі як банківські картки чи електронні гаманці, напряму пов’язані з особою користувача. Тому неофіційним елементом транзакцій є криптовалюти[23].

Криптовалюти забезпечують різний рівень приватності:

1. Біткоїн надає псевдонімність: транзакції відкриті для перегляду, але не містять імен. Проте зв'язки між адресами можуть бути відновлені.
2. Monero є повністю анонімною валютою: приховує відправника, отримувача та суму транзакції.

3.2.1 Застосування криптовалют у контексті анонімності веббраузера

Застосування криптовалюти разом з інструментами веб-анонімності дозволяє:

1. Анонімно придбати VPN, проксі-сервіси або доступ до Tor-міст.
2. Сплачувати за віртуальні приватні сервери (VPS) для хостингу власних анонімізуючих рішень.
3. Купувати облікові записи або SIM-картки, не залишаючи слідів у традиційних платіжних системах.

3.2.2 Приклад інтеграції криптовалюти в ланцюг анонімності

Розглянемо покрокову схему використання криптовалюти в рамках захищеного інтернет-сценарію:

1. Вхід в інтернет через VPN + Tor для маскування IP-адреси.
2. Відвідування P2P-обмінника.
3. Купівля біткоїна за готівку або анонімним методом.
4. Обмін біткоїна на Monero через DEX.
5. Оплата хостингу для свого VPN або проксі з використанням Monero.
6. Збереження залишку в холодному гаманці (офлайн) для майбутніх платежів.

Щоб уникнути деанонімізації, навіть з відкритими криптовалютами варто створювати нову адресу для кожної транзакції та не використовувати той самий гаманець у відкритій мережі без VPN/Tor.

3.3 Комплексний гайд із забезпечення анонімності в інтернеті

Цей підрозділ об'єднує всі ключові техніки, розглянуті раніше, у практичний посібник для користувачів, які прагнуть мінімізувати цифрові сліди. Початковим кроком є створення незалежної інфраструктури, яка не прив'язана до вашої особистості. Для цього:

1. SIM-картка без ідентифікації. Її можна придбати в країнах із м’яким регулюванням, як-от Польща чи Велика Британія. Активувати картку варто в публічному місці, подалі від вашої домівки.
2. Криптовалюта як платіжний інструмент. Купівля біткоїнів за готівку через P2P-платформи або крипто-банкомати - перший крок. Далі для підвищення приватності монети краще обміняти на Monero і зберігати в холодному (офлайн) гаманці.

Перейдемо до покрокової інструкції для забезпечення анонімності в мережі

1) Підключення VPN - вибрати для підключення надійний VPN-сервіс з політикою "no-logs". Для максимального рівня анонімності рекомендується

оплачувати VPN через криптовалюту, зокрема Monero. Увімкнути функцію Kill Switch в налаштуваннях VPN, щоб запобігти витокам даних у разі розриву з'єднання.

2) Імплементація зміни HTTP-заголовків - Після підключення VPN налаштувати зміну HTTP-заголовків для браузера. Використовувати спеціальні скрипти, щоб динамічно змінювати значення таких заголовків, як User-Agent та інші (див. Додаток А для коду).

3) Встановлення захисних розширень для браузера - Для посилення захисту у браузері потрібно встановити наступні розширення:

1. uBlock Origin - блокує рекламу, трекери та шкідливі скрипти.
2. Privacy Badger - автоматично виявляє та блокує поведінкові трекери.
3. HTTPS Everywhere - змушує використовувати зашифровані з’єднання, де це можливо.
4. NoScript - дозволяє контролювати, які скрипти можуть виконуватися на веб-сторінках, що запобігає виконанню небажаних JavaScript-кодів.

3.3.1 Захист від деанонімізації та підтримка безпеки

1. Регулярна перевірка - Періодично перевіряти відбитки з Browser Fingerprint на сайтах типу AmIUnique або Panopticlick. Тестувати VPN на витоки, використовуючи сервіси ipleak.net або browserleaks.com. Регулярно переглядати HTTP-заголовки через інструменти розробників у браузері.
2. Оновлення інструментів та змінення стратегій - Для збереження високого рівня анонімності оновлювати Tor Browser, VPN-клієнти та розширення на регулярній основі. Також періодично замінювати SIM-картки і криптогаманці для підвищення рівня анонімності.
3. У разі виявлення деанонімізації треба вжити такі заходи як:
    1. Змінити SIM-картку та криптогаманці.
    2. Створити нові облікові записи через інший Tor-ланцюг
    3. Видалити всі дані, пов'язані з попередньою інфраструктурою.

ВИСНОВКИ

У результаті проведеного дослідження методології забезпечення анонімності користувача в контексті кібербезпеки веббраузерів були визначені ключові вектори сучасних загроз приватності та розроблено комплексний підхід до захисту особистих даних під час вебсерфінгу з акцентом на практичні інструменти автоматизованої зміни ідентифікаційних параметрів браузера.

Аналіз теоретичних основ показав, що базові механізми захисту, вбудовані у сучасні браузери, є суттєво недостатніми: більшість сайтів використовують приховані механізми збору даних та передають унікальні ідентифікатори навіть у режимі "інкогніто". Це підтверджує необхідність розробки спеціалізованих рішень для забезпечення справжньої анонімності.

У роботі було досліджено та порівняно ефективність ключових інструментів забезпечення анонімності:

1. VPN-сервіси визнано основним інструментом базового захисту, ефективність якого критично залежить від політики збереження логів та юрисдикції провайдера.
2. Tor Browser забезпечує високий рівень анонімності завдяки багаторівневій маршрутизації, але має суттєві обмеження у швидкості та зручності користування, що робить його менш практичним для щоденного використання.
3. Методи протидії browser fingerprinting (цифровому відбитку браузера) визнано критичним компонентом анонімізації, який часто недооцінюється користувачами.

Практична частина роботи була сфокусована на розробці автоматизованого Python-скрипта на основі Selenium для динамічної зміни HTTP-заголовків, User-Agent[14] та інших ідентифікаційних параметрів браузера. У результаті тестування було доведено, що такий підхід дозволяє значно ускладнити відстеження користувача без необхідності повного переходу на Tor Browser.

Важливим практичним результатом роботи стала розробка комплексного підходу до забезпечення анонімності, який включає:

1. пріоритетне використання VPN у поєднанні з розробленим скриптом зміни HTTP-заголовків як ефективну альтернативу Tor Browser для більшості сценаріїв користування;
2. інтеграцію спеціалізованих браузерних розширень для блокування fingerprinting (NoScript, uBlock Origin, Privacy Badger);
3. методику використання неідентифікованих SIM-карт та криптовалют для анонімної реєстрації облікових записів та здійснення платежів;
4. опціональне застосування Tor для ситуацій, що вимагають максимального рівня анонімності.

Експериментальним шляхом було підтверджено, що для ефективного захисту необхідно впливати не на окремі параметри, а на цілу сукупність характеристик браузера, формуючи постійно змінюваний цифровий профіль користувача.

Забезпечення анонімності у веббраузерах - це динамічний процес що вимагає комбінування різних технологій з акцентом на автоматизацію зміни ідентифікаційних параметрів. Запропонований підхід дозволяє досягти високого рівня анонімності без суттєвої втрати в зручності і швидкості роботи[3], на відміну від традиційних рішень на базі Tor. Результати дослідження формують практичну методологію забезпечення анонімності в цифровому середовищі та можуть бути використані як для індивідуального захисту користувачів, так і для подальших наукових розробок у сфері кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Москаленко О.І. Використання Python для анонімізації веб-запитів. // 2024. // V Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики. С. 195-197. URL: https://is.gd/g0nghi
2. Oleksii Lishchuk. Як зберегти анонімність в Інтернеті у 2025 році // Acer Blog. 2025. URL: https://blog.acer.com/ua/discussion/2526/yak-zberegti-anonimnist-v-interneti-u-2025-roci [Електронний ресурс].
3. Хто і як стежить за вами в інтернеті і що з цим робити // Радіо Свобода. 2019. URL:https://www.radiosvoboda.org/a/internet-surveillance/30111147.html [Електронний ресурс].
4. Як забезпечити анонімність в інтернеті? // Ganjaseeds. н.д. URL: https://ganjaseeds.com.ua/ua/articles/ensure-anonymity-Internet-ua/ [Електронний ресурс; дата доступу: 19.05.2025].
5. Tor 101: How Tor Works and its Risks to the Enterprise // Unit 42. 2022. URL: https://unit42.paloaltonetworks.com/tor-traffic-enterprise-networks/ [Електронний ресурс].
6. How Does A VPN Work? // Fortinet. н.д. URL: https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work [Електронний ресурс; дата доступу: 19.05.2025].
7. Buckbee M. What is a Proxy Server and How Does it Work? // Varonis. 2022. URL: https://www.varonis.com/blog/what-is-a-proxy-server [Електронний ресурс].
8. Awati R., Chai W., Ferguson K. What is HTTP and how does it work? // TechTarget. 2023. URL:https://www.techtarget.com/whatis/definition/HTTP-Hypertext-Transfer-Protocol [Електронний ресурс].
9. Muthukadan B. Selenium with Python // ReadTheDocs. 2024. URL: https://selenium-python.readthedocs.io [Електронний ресурс].
10. Відстеження анонімності через IP-адресу: Як уникнути? // Mindscope. 2024. URL:https://mindscope.biz.ua/vidstezhennya-anonimnosti-cherez-ip-adresu-yak-unyknuty/ [Електронний ресурс].

11. Chea E. Browser fingerprinting explained // Fingerprint. 2024. URL: https://fingerprint.com/blog/browser-fingerprinting-techniques/ [Електронний ресурс].
12. Що таке браузерне фінгерпринтинг та як він працює? // Seon.io. 2023. URL: https://seon.io/resources/browser-fingerprinting/ [Електронний ресурс].
13. Даттон С. Що таке флаги Chrome? // Developer Chrome. 2023. URL: https://developer.chrome.com/docs/web-platform/chrome-flags?hl=ua [Електронний ресурс].
14. Selenium Python Tutorial (with Example) // BrowserStack. 2024. URL: https://www.browserstack.com/guide/python-selenium-to-run-web-automation-test [Електронний ресурс].
15. Moraneus. Посібник з використання Python Selenium // Medium. 2024. URL: https://medium.com/@moraneus/guide-to-using-python-selenium-873342d5fdad [Електронний ресурс].
16. Using HTTP cookies // MDN Web Docs. 2025. URL: https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies [Електронний ресурс].
17. Longe T. Website click tracking - Best tools & methods explained // UXCam. 2025. URL: https://uxcam.com/blog/website-click-tracking/ [Електронний ресурс].
18. Protect your data with site isolation // Google Chrome Enterprise Help. 2020. URL: https://support.google.com/chrome/a/answer/7581529?hl=en [Електронний ресурс].
19. Disable-Firefox-Telemetry-and-Data-Collection // GitHub. 2017. URL: https://github.com/K3V1991/Disable-Firefox-Telemetry-and-Data-Collection [Електронний ресурс].
20. How to use uBlock Origin to block Javascript by default // UTCC Blog. 2018. URL: https://utcc.utoronto.ca/~cks/space/blog/web/UBlockJavascriptBlocking [Електронний ресурс].
21. What is my User Agent? // WhatIsMyBrowser.com. 2024. URL: https://www.whatismybrowser.com/detect/what-is-my-user-agent/ [Електронний ресурс].

22. User-Agent // Mozilla Developer Network. 2025. URL: https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/User-Agent [Електронний ресурс].
23. Anonymous Browsers: Tracking // HackYourMom. 2023. URL: https://hackyourmom.com/en/kibervijna/oglyad-anonimnyh-brauzeriv-dlya-pryvatnogo-serfingu/ [Електронний ресурс].
24. Shreya. Technologies and Methods Websites Use to Track its Users // CookieLawInfo. 2021. URL: https://www.cookielawinfo.com/technologies-and-methods-websites-use-to-track-its-users/ [Електронний ресурс].
25. Website tracking guide // Contentsquare. 2024. URL: https://contentsquare.com/guides/website-tracking/ [Електронний ресурс].

ДОДАТОК А

Програмна реалізація зміни User-Agent у Selenium - У цьому додатку наведено код, який реалізує зміну HTTP-заголовка User-Agent за допомогою бібліотеки Selenium Python. Даний код дозволяє динамічно генерувати та встановлювати різні User-Agent для браузера Chrome, що ускладнює відстеження користувача.

А.1 Повний код програми:

```
from selenium import webdriver
from selenium.webdriver.chrome.options import Options
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC
from random import choice

os_list = [
    "Windows NT 10.0; Win64; x64",
    "Macintosh; Intel Mac OS X 10_15_7",
    "X11; Linux x86_64",
    "Linux; Android 10; SM-G973F",
    "iPhone; CPU iPhone OS 14_0 like Mac OS X"
]
chrome_versions = [
    "122.0.6261.128",
    "121.0.6167.140",
    "120.0.6099.224",
    "119.0.6045.200",
    "118.0.5993.89"
]

def generate_random_user_agent():
    os = choice(os_list)
    version = choice(chrome_versions)
```

```
    return f"Mozilla/5.0 ({os}) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/{version} Safari/537.36"

options = Options()
custom_user_agent = generate_random_user_agent()

options.add_argument(f'user-agent={custom_user_agent}')
options.add_argument('--disable-gpu')
options.add_argument('--disable-webgl')
options.add_argument('--disable-webrtc')
options.add_argument('--disable-background-networking')
options.add_argument('--disable-client-side-phishing-
detection')
options.add_argument('--disable-sync')
options.add_argument('--disable-translate')
options.add_argument('--disable-default-apps')
options.add_argument('--disable-popup-blocking')
options.add_argument('--disable-
features=AudioServiceOutOfProcess,WebRtcHideLocalIpsWithMdns')
options.add_argument('--disable-blink-
features=AutomationControlled')

options.add_experimental_option('excludeSwitches',     ['enable-
automation'])
options.add_experimental_option('useAutomationExtension', False)

driver = webdriver.Chrome(options=options)

try:
     driver.get("https://www.whatismybrowser.com/detect/what-is-
my-user-agent/")
    wait = WebDriverWait(driver, 10)
                                  detected_value                =
wait.until(EC.presence_of_element_located((By.ID,
"detected_value")))
```

```
    displayed_user_agent = detected_value.text
    print(f"Встановлений User-Agent: {custom_user_agent}")
    print(f"Визначений User-Agent: {displayed_user_agent}")
    print("User-Agent успішно змінено!" if custom_user_agent in displayed_user_agent else "User-Agent не було змінено належним чином")

    driver.get("https://uk.wikipedia.org/wiki/Україна")
    input("Натисніть Enter для закриття браузера...")

except Exception as e:
    print(f"Виникла помилка: {e}")
finally:
    driver.quit()
```