УДК 004.45
DOI https://doi.org/10.32782/2663-5941/2024.5.1/21

Завгородній В.В.
Державний університет інфраструктури та технологій

Завгородня Г.А.
Державний університет інфраструктури та технологій

Васильєв С.В.
Державний університет інфраструктури та технологій

Прусов В.О.
Державний університет інфраструктури та технологій

РОЗРОБКА МЕТОДОЛОГІЇ ДЛЯ АНОНІМНОСТІ КОРИСТУВАЧІВ ТА ПРОТИДІЇ ВІДСТЕЖЕННЮ ОНЛАЙН

Робота присвячена розробці рішення для забезпечення анонімності користувачів, зокрема тих, хто не володіє технічними знаннями, але має потребу приховати свою особу в Інтернеті. Вихідна система передбачає, що інтернет-провайдер має доступ до ідентифікації користувача, а робоча станція (найімовірніше, ОС Windows) використовується для повсякденних завдань.

У роботі було проведено низку ключових етапів, що включали збір та аналіз сучасної теоретичної інформації, вивчення наявних рішень-аналогів, проектування практичного рішення та серію експериментів для оцінки його ефективності. Основною метою дослідження було розробити комплекс програмного забезпечення, що забезпечує високий рівень анонімності користувачів в Інтернеті та захист від різних методів відстеження й ідентифікації.

У роботі було запропоновано використання схеми «VPN через Tor» для ефективного маскування користувацького трафіку. Така конфігурація дозволяє видавати VPN-адресу замість Tor, що робить трафік менш підозрілим для зовнішніх систем. Замість стандартного Tor Browser пропонується використовувати модифікований Firefox з відповідними налаштуваннями для анонімності. Chromium-браузери відхиляються, оскільки Firefox має ширший спектр конфіденційних налаштувань, таких як протидія фінгерпринтингу та можливість налаштування приватних даних.

У результаті роботи було підібрано, налаштовано і протестовано програмний комплекс, який найбільш ефективно вирішує поставлені завдання. Основні функціональні можливості системи включають приховування та підміну даних користувача, шифрування та обфускацію трафіку, маскування використання засобів анонімізації, ізоляцію веб-браузера від основної операційної системи, а також захист від витоків реальних даних.

Для посилення захисту запропоновано використовувати віртуальні машини з ОС Windows, що забезпечує додатковий рівень ізоляції від можливих атак та витоків даних. Для анонімізації трафіку через Tor рекомендується використовувати Whonix-Gateway з протоколом obfs4, який забезпечує протидію аналізу DPI.

Ключові слова: *інформаційна безпека, анонімність, захист від відстеження, шифрування, Інтернет.*

Постановка проблеми. Проблема анонімності в Інтернеті існувала з самого початку його створення, але набула особливої актуальності в 2013 році після викриттів Едварда Сноудена. Він оприлюднив інформацію про програми глобального стеження, зокрема систему PRISM, що продемонструвало безпрецедентне втручання у приватне життя громадян.

На сьогоднішній день розробка та використання програмних засобів для анонімності та захисту відстеження в Інтернеті є актуальною проблемою. Попри популярність VPN-сервісів і анонімайзерів, багато з них мають суттєві недоліки.

1. Комплексність забезпечення анонімності – багато сервісів вирішують завдання частково. Навіть у мережі TOR, яка вважається безпечною, траплялися випадки ідентифікації користувачів. VPN-провайдери можуть зберігати історію дій та передавати її державним службам.

2. Зниження зручності – анонімізація може впливати на швидкість з'єднання та функціональність браузера. Деякі сайти блокують IP-адреси

TOR, а відключення JavaScript та Cookies може ускладнювати роботу.

3. Непомітність – використання анонімізуючих інструментів часто може привернути увагу. Більшість сервісів не забезпечують повної непомітності.

4. Складність використання – багато інструментів важко налаштовувати, що вимагає глибоких технічних знань. Це обмежує їх використання для звичайних користувачів.

Також існує проблема браку авторитетних наукових публікацій з цієї теми, особливо українськомовних. Інформація часто доступна на форумах і в анонімних мережах, що лише підкреслює актуальність проблеми анонімності в Інтернеті.

Аналіз останніх досліджень і публікацій. На перший погляд, дана тематика переважно висвітлюється на неофіційних інтернет-ресурсах, проте існує чимало наукових робіт, що досліджують вразливості анонімних мереж, методи ідентифікації пристроїв та розробку нових способів захисту від сучасних методів стеження.

Дослідження [1] аналізує можливі атаки в мережі Tor та демонструє одну з них. Статті [2–5] вивчають поведінку складних ланцюжків проксі-серверів та розглядають слабкі місця Tor, альтернативи та можливість використання Skype через цю мережу.

У публікації [6] представлено інструмент для випадкової заміни даних браузера з метою уникнення ідентифікації. У 2017 році дослідники зі США в статті [7] описали техніку точного розпізнавання комп'ютерів незалежно від браузера, рекомендувавши використовувати Tor Browser для протидії такому стеженню. У дослідженні приділено увагу методам фінгерпринтингу, зокрема WebGL.

Дослідження [8] аналізує сучасні методи відстеження в Інтернеті. Інтернет-ресурс The Free Haven пропонує велику колекцію статей на тему анонімності та шифрування. Зокрема, стаття [9] аналізує трафік мережі Tor, опублікована Військово-морською дослідною лабораторією США.

Роботи [10–12] охоплюють теми шифрування файлів, використання менеджерів паролів, захисту від вірусів, анонімних мереж та інше. Також детально розглядаються Tails і PGP. Стаття [13] у спрощеній формі пояснює роботу Tor, I2P, шифрування файлів та електронної пошти.

Наведені дослідження є важливими кроками на шляху до забезпечення анонімності, але питання повного захисту користувачів від сучасних загроз залишається актуальним.

Постановка завдання. Основна мета дослідження – оцінити можливість створення засобу анонімізації, який максимально поєднує надійність, зручність, непомітність та простоту налаштування. Оскільки ці якості часто конфліктують між собою (підвищення безпеки може знизити зручність), дослідження має визначити межі їх сумісності та способи реалізації. Планується проєктування програмного продукту для практичного використання.

Виклад основного матеріалу. Для забезпечення анонімності широкому колу користувачів (враховуючи, що потреба в ній може виникнути не лише у технічно підкованих осіб), виходимо з припущення, що вихідна система не є анонімною: інтернет-провайдер знає особу користувача, комп'ютер використовується для повсякденних завдань, і, ймовірно, працює під ОС Windows. Передбачається використання платних сервісів, таких як надійний VPN або VPS. Основні вимоги до рішення:

– приховати від сайтів усі дані, що стосуються вихідної системи та браузера;

– забезпечити шифрування трафіку для обходу моніторингових систем провайдера;

– надати можливість змінювати цифрові відбитки користувача;

– запобігти витоку реальної IP-адреси через анонімний браузер;

– маскувати використання засобів анонімізації від сайтів та систем аналізу трафіку;

– зробити рішення легким у встановленні та налаштуванні.

Не всі вимоги є критичними – наприклад, маскування VPN або Tor може бути опціональним, якщо провайдер їх не блокує. Крім того, не всі сайти виявляють анонімізаційні засоби або перевіряють правдоподібність цифрових відбитків. Однак розроблене рішення намагається максимально врахувати всі ці вимоги для ефективної анонімізації користувача.

З огляду на мету – максимально приховати факт використання засобів анонімізації – застосування Tor Browser є небажаним, оскільки його легко виявити, що може привернути небажану увагу. Для цього пропонується використовувати схему «VPN через Tor», яка забезпечує IP-адресу VPN-сервера на виході, що виглядає менш підозріло порівняно з адресами, пов’язаними з Tor. Використовувати Tor Browser в такій конфігурації складно, оскільки він налаштований виключно на передачу трафіку через мережу Tor і не підтримує інші проксі-налаштування. Крім того, Tor Browser має характерні цифрові відбитки, що також може викликати підозри.

Тому для нашої задачі більш доцільно використовувати звичайний Firefox із відповідними змінами в конфігурації, які дозволять підлаштувати браузер під потреби анонімної роботи. Браузери на основі Chromium не розглядаються, оскільки для анонімної діяльності зазвичай рекомендується саме Firefox. Це обумовлено як репутацією Mozilla, яка активно підтримує конфіденційність користувачів, так і широкими можливостями для налаштування браузера під специфічні вимоги анонімізації.

У таблиці 1 наведено основні установки конфігурації браузера Firefox для забезпечення анонімності та захисту від відстеження.

Ці параметри налаштовують Firefox для максимального приховування активності користувача та мінімізації витоків інформації, що може бути використано для відстеження.

Крім основних налаштувань, існує багато додаткових параметрів, що можуть підвищити рівень захисту. Головна мета цих налаштувань – запобігти витоку другорядних даних, зберігаючи функціональність браузера без змін. Наприклад, відключення телеметрії допомагає підвищити конфіденційність, а вимкнення WebRTC запобігає витоку реальної IP-адреси, але може свідчити про використання засобів анонімізації, чого краще уникати.

Таблиця 1

Основні установки конфігурації браузера Firefox для забезпечення анонімності та захисту від відстеження

Параметр	Значення	Опис	Примітки
privacy.resistFingerprinting	true	Включення захисту від відстеження через цифрові відбитки	Не рекомендується через ідентичність з відбитками Tor Browser
privacy.firstparty.isolate	true	Ізоляція контенту для запобігання відстеженню через Cookies	Може викликати проблеми на деяких сайтах
browser.safebrowsing.enabled	false	Вимкнення Safe Browsing для захисту від передачі даних на Google	Збільшує ризик зараження шкідливим ПЗ
browser.safebrowsing.downloads.enabled	false	Вимкнення Safe Browsing для завантажених файлів	
browser.safebrowsing.malware.enabled	false	Вимкнення захисту від шкідливих сайтів	
browser.search.suggest.enabled	false	Заборона передачі введеного тексту в пошукову систему без підтвердження	
dom.enable_performance	false	Вимкнення передачі даних про продуктивність завантаження сторінок	
network.dns.disablePrefetch	true	Вимкнення попередньої обробки DNS для посилань на сторінці	
dom.battery.enabled	false	Заборона відстеження рівня заряду батареї	
dom.network.enabled	false	Відключення передачі даних про тип мережевого підключення	
media.peerconnection.enabled	false	Відключення WebRTC для захисту від витоку IP-адреси	Альтернатива: опція в uBlock для запобігання витоку.
geo.enabled	false	Відключення геолокації	
media.navigator.enabled	false	Заборона доступу до мікрофона та камери	
media.navigator.streams.fake	true	Генерація фейкового аудіо та відеосигналу для підміни реальних даних	
webgl.disable-extensions	true	Обмеження функцій WebGL для захисту від передачі даних про систему	Можна повністю вимкнути WebGL
webgl.min_capability_mode	true	Зменшення функціональності WebGL для обмеження доступу до даних	
privacy.trackingprotection.enabled	true	Включення захисту від відстеження	Можна використовувати uBlock з додатковими фільтрами
general.useragent.override	<рядок>	Підміна User-agent для маскування браузера	Зручніше використовувати розширення для цієї задачі
dom.webaudio.enabled	false	Вимкнення AudioContext API для захисту від аудіо-відбитків	Можна використовувати доповнення для захисту
layout.css.visited_links_enabled	false	Вимкнення виділення відвіданих посилань для захисту від трекінгу	

Джерело: складено авторами

У налаштуваннях Firefox рекомендується активувати режим «Завжди працювати в приватному перегляді». Хоча цей режим не гарантує повної анонімності, він є ефективним для боротьби з Evercookie, оскільки всі збережені ідентифікатори автоматично видаляються після закриття браузера. Теоретично, можна відключити кеш та локальне сховище, але це може спричинити проблеми з роботою браузера. У вкладці «Приватність» варто заборонити cookies зі сторонніх сайтів, а в додаткових налаштуваннях – повністю відключити телеметрію. Головні моменти щодо налаштувань та розширень для анонімності у Firefox:

1. Протидія фінгерпринтингу: Firefox має вбудовані опції протидії «фінгерпринтінгу», які активуються через налаштування privacy. resistfingerprinting. Однак цей режим не використовується, оскільки деякі відбитки збігаються з Tor Browser, а також він змінює часовий пояс на UTC, що не підходить для нашого випадку.

2. Важливі браузерні доповнення:

– CanvasBlocker: блокує або заміняє відбиток Canvas fingerprint, генерує випадкові дані для кожної сторінки;

– NoScript: блокує виконання небезпечних компонентів JavaScript, Java, Flash, захищає від XSS-атак;

– uBlock Origin: блокує рекламу, відстежувальні елементи, може захистити від фінгерпринтінгу та витоків IP через WebRTC;

– Decentraleyes: захищає від відстеження через CDN, використовуючи локальні ресурси;

– Privacy Badger: блокує трекери та самонавчається;

– HTTPS Everywhere: примусово використовує HTTPS на сайтах, які це підтримують;

– Smart Referer: підміняє або блокує HTTP referer для захисту приватності;

– AudioContext Fingerprint Defender: спотворює відбитки AudioContext, додаючи випадковий шум;

– ScriptSafe: пропонує додаткові опції антивідстеження, зокрема захист буфера обміну та випадкові затримки між натисканнями клавіш;

– User-agent Switcher: дозволяє замінювати User-agent, зокрема через JavaScript.

Такі налаштування та доповнення сприяють покращенню приватності користувача, блокуванню відстежувальних елементів і забезпеченню анонімності в браузері Firefox.

Головні моменти про доповнення RAS та інтеграцію Tor у Firefox:

1. Доповнення RAS (Random Agent Spoofer):

– Призначення: інструмент для заміни профілю браузера (User-agent та інші параметри) з широкими можливостями;

– Функціонал: заміна роздільної здатності екрану, часового поясу, параметра window.name. Деякі налаштування керують вбудованими параметрами Firefox;

– Недоліки: немає опції Time Zone Spoofing у тестованій версії. Розробка припинена через складнощі міграції на новий стандарт Firefox WebExtension;

– Сумісність: несумісний із версіями Firefox 57 і вище.

2. Інтеграція Tor у Firefox:

– Проект Fusion: ініціатива щодо об'єднання Tor Browser і Firefox в єдиний браузер, який працюватиме в різних режимах;

– Мета: покращити боротьбу з фінгерпринтингом і спростити налаштування для користувачів;

– Проект Tor Uplift: продовження інтеграції функцій Tor у Firefox.

Все це посилить анонімність та конфіденційність користувачів, особливо після інтеграції нових функцій протидії фінгерпринтінгу.

Наступні кроки забезпечують надійний захист та ізоляцію від потенційних загроз і витоків даних.

1. Використання віртуальної машини (ВМ):

– для захисту від витоків та ізоляції браузера використовується Whonix, що складається з двох ВМ: одна є шлюзом в інтернет, інша виконує основні завдання. Можна підключати до шлюзу будь-яку ВМ, зокрема Windows;

– Windows 10 обрано для підвищення анонімності, оскільки виглядає звичніше, ніж Linux. З неї видаляються оновлення, що відправляють телеметрію.

2. Анонімізація трафіку через Whonix-Gateway:

– Tor використовується для анонімізації, але факт використання Tor маскується через VPN;

– використання VPN може бути як через комерційний VPN-сервіс, так і через власний сервер на VPS;

– для маскування трафіку застосовується протокол obfs4, який протидіє аналізу DPI.

3. Налаштування VPN-сервера:

– VPN використовує TCP-порт 443 і блокує зовнішні ICMP-запити;

– DNS-запити йдуть через VPN, із серверів OpenNIC, відповідних країні розташування VPS;

– використовується шифрування керуючого каналу та HMAC-аутентифікація.

4. Додаткові заходи безпеки:

– встановлюється програмне забезпечення для шифрування даних, видалення EXIF та безпечного обміну повідомленнями;

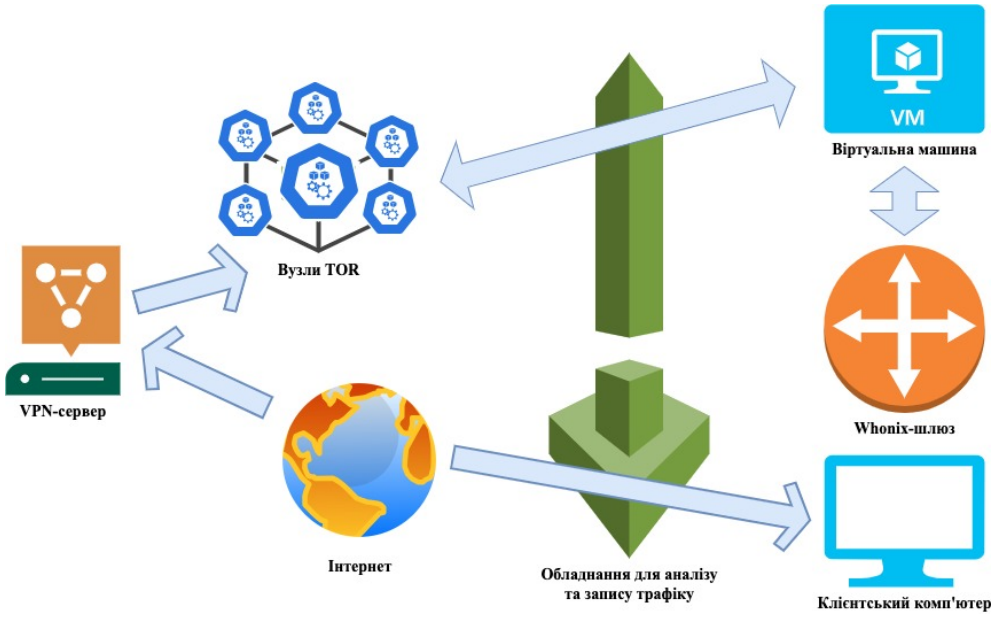

Рис. 1. Основні компоненти системи

Джерело: світлини зроблено авторами

– антивірус необов'язковий, оскільки ВМ ізольована від реальної системи та IP, а знімки стану ВМ можуть швидко відновити чисту копію.

Підсумкова схема реалізації наведена на рисунку 1:

– DPI (Deep Packet Inspection): обладнання для аналізу та запису трафіку, яке може включати системи СОРМ-3, встановлені у провайдера;

– відвідування сайтів: схема дозволяє одночасне відвідування сайтів як із віртуальної машини, так і з основної системи, але розпізнати, що це один і той самий користувач, буде дуже складно;

– обфускація OpenVPN: у даній схемі немає необхідності додатково маскувати OpenVPN, оскільки трафік проходить через Tor з обфускацією;

– захист трафіку: VPN забезпечує захист трафіку від можливого прослуховування на вихідних вузлах мережі Tor.

Така схема забезпечує високий рівень анонімності та захисту даних під час роботи в інтернеті.

Висновки. У ході роботи було проведено глибокий пошук інформації про сучасні методи ідентифікації користувачів та відстеження їхньої активності в Інтернеті. Одним із завдань було зібрати й систематизувати ці дані, що включало аналітичний огляд, проектування та експерименти. Результатом стало створення конфігурації програмного комплекту, який забезпечує високий рівень захисту без погіршення функціональності браузера.

Запропоноване у роботі рішення дозволяє ефективно захищати особисті дані користувача, шифрувати трафік, запобігати витоку IP-адрес та фінгерпринтів, а також забезпечує можливість гнучкого налаштування браузера для максимального рівня анонімності. Використання VPN через Tor гарантує надійну анонімність, навіть при використанні стандартних ОС, таких як Windows.

Таким чином, робота вносить значний вклад у розуміння і вирішення проблем анонімності в Інтернеті, протидії цензурі та боротьби із сучасними системами відстеження, що є надзвичайно актуальним в умовах зростаючого контролю за онлайн-активністю і загроз конфіденційності у цифрову еру.

Список літератури:

1. Karunanayake I., Ahmed N., Malaney R., Islam R., Jha S.K. De-Anonymisation Attacks on Tor: A Survey. *In IEEE Communications Surveys & Tutorials*. Vol. 23. No. 4. P. 2324-2350. 2021. DOI: https://doi.org/10.1109/COMST.2021.3093615

2. Alsabah M., Goldberg I. Performance and security improvements for TOR: A survey. *ACM Computing Surveys (CSUR)*. Vol. 49(2). P. 1-36. 2016. DOI: https://doi.org/10.1145/2946802

3. Saad Saleh, Junaid Qadir, Muhammad U. Ilyas. Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. *Journal of Network and Computer Applications*. Vol. 114. 2018. P. 1-28. DOI: https://doi.org/10.1016/j.jnca.2018.04.002

4. Cambiaso E., Vaccari I., Patti L., Aiello M. Darknet Security: A Categorization of Attacks to the Tor Network. *In ITASEC*. Vol. 2315. P. 1-12. 2019. URL: https://ceur-ws.org/Vol-2315/paper10.pdf

5. Basyoni L., Fetais N., Erbad A., Mohamed A., Guizani M. Traffic Analysis Attacks on Tor: A Survey. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. 2020. P. 183-188. DOI: https://doi.org/10.1109/ICIoT48696.2020.9089497

6. Nikiforakis N., Joosen W., Livshits B. PriVaricator: Deceiving Fingerprinters with Little White Lies. *In Proceedings of the 24th International Conference on World Wide Web (WWW '15). International World Wide Web Conferences Steering Committee*. P. 820-830. 2015. https://doi.org/10.1145/2736277.2741090

7. Cao Y., Li S., Wijmans E. (Cross-)Browser fingerprinting via OS and hardware level features. *In Proceedings 2017 Network and Distributed System Security Symposium. Internet Society.* 2017. URL: https://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf

8. Englehardt S., Narayanan A. Online Tracking: A 1-million-site Measurement and Analysis. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery*. P. 1388-1401. 2016. DOI: https://doi.org/10.1145/2976749.2978313

9. Jansen R., Juarez M., Galvez R., Elahi T., Diaz C. Inside Job: Applying Traffic Analysis to Measure Tor from Within. *Network and Distributed System Security Symposium.* 2018. DOI: https://doi.org/10.14722/ndss.2018.23279

10. Darir H., Borisov N., Dullerud G. DiProber: Estimating Relays Capacities in Underloaded Anonymous Communication Networks. *2024 American Control Conference (ACC)*. P. 462-467. 2024. DOI: https://doi.org/10.23919/ACC60939.2024.10644851

11. Mukhin V., Zavgorodnii V., Kornaga Y., Krysak I., Bazaliy M., Mukhin O. Program Code Protecting Mechanism Based on Obfuscation Tools. In: Zgurovsky, M., Pankratova, N. (eds) *System Analysis & Intelligent Computing*. *(SAIC). Studies in Computational Intelligence.* Vol. 1022. P. 407-419. 2022. DOI: https://doi.org/10.1007/978-3-030-94910-5_20

12. Mukhin V., Kornaga Y., Bazaliy M., Zavgorodnii V., Krysak I., Mukhin O. Obfuscation Code Technics Based on Neural Networks Mechanism. *IEEE 2nd International Conference on System Analysis & Intelligent Computing (SAIC)*. P. 1-6. 2020. DOI: https://doi.org/10.1109/SAIC51296.2020.9239247

13. Chao D., Xu D., Gao F., Zhang C., Zhang W., Zhu L. A Systematic Survey on Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization. *In IEEE Communications Surveys & Tutorials*. Vol. 26. No. 3. P. 1775-1829. 2024. DOI: https://doi.org/10.1109/COMST.2024.3350006

Zavgorodnii V.V., Zavgorodnya A.A., Vasiliev S.V., Prusov V.O. DEVELOPMENT OF A METHODOLOGY FOR USER ANONYMITY AND ANTI-TRACKING ONLINE

The work is devoted to the development of a solution to ensure the anonymity of users, in particular those who do not have technical knowledge, but need to hide their identity on the Internet. The source system assumes that the ISP has access to the user's identity, and the workstation (most likely a Windows OS) is used for day-to-day tasks.

A number of key stages were carried out in the work, including the collection and analysis of modern theoretical information, the study of existing analogue solutions, the design of a practical solution and a series of experiments to evaluate its effectiveness. The main goal of the research was to develop a set of software that ensures a high level of anonymity of users on the Internet and protection against various methods of tracking and identification.

The work proposed the use of the "VPN over Tor" scheme for effectively masking user traffic. This configuration allows the VPN address to be issued instead of Tor, making the traffic less suspicious to external systems. Instead of the standard Tor Browser, it is suggested to use a modified Firefox with appropriate settings for anonymity. Chromium browsers are rejected because Firefox has a wider range of privacy settings, such as anti-fingerprinting and the ability to configure private data.

As a result of the work, a software complex was selected, configured and tested, which most effectively solves the tasks. The main functionality of the system includes hiding and changing user data, encrypting and obfuscating traffic, masking the use of anonymizers, isolating the web browser from the main operating system, and protecting against real data leaks.

To strengthen protection, it is suggested to use virtual machines with Windows OS, which provides an additional level of isolation from possible attacks and data leaks. To anonymize traffic through Tor, it is recommended to use Whonix-Gateway with the obfs4 protocol, which provides protection against DPI analysis.

Key words: *information security, anonymity, protection from tracking, encryption, Internet.*