ПОРІВНЯННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ТА ПРИВАТНОСТІ В ІНТЕРНЕТІ

Новік Т.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток цифрових технологій призвів до суттєвого збільшення обсягів персональних даних, що передаються та обробляються в мережі Інтернет. Сучасні онлайн-сервіси активно використовують інформацію про користувачів для персоналізації, аналітики та таргетованої реклами. Разом із цим зростає і кількість ризиків, пов'язаних із витоком конфіденційної інформації, відстеженням активності та втручанням у приватність користувача [1, 2].

Очікується, що глобальний ринок VPN-сервісів досягне $151,92 млрд у 2030 році, що підтверджує зростання попиту на технології цифрової приватності. Подальший розвиток засобів захисту приватності вимагає як технічного удосконалення інструментів, так і підвищення цифрової грамотності користувачів.

Метою доповіді є аналіз ефективності сучасних інструментів забезпечення анонімності в Інтернеті шляхом порівняння режимів підключення (без захисту, VPN, Tor) та оцінки їх впливу на IP-ідентифікацію, геолокацію, швидкість доступу та унікальність браузерного відбитка.

Значна частина інтернет-користувачів не усвідомлює масштаби збору цифрових слідів — IP-адреси, файлів cookies, інформації про браузер, мовні налаштування, часовий пояс тощо. За даними дослідження AmIUnique, до 81% мобільних браузерних відбитків є унікальними, що робить можливим точне відстеження поведінки окремих користувачів [3].

Анонімність та приватність в Інтернеті є взаємопов'язаними, проте не тотожними поняттями. Анонімність передбачає неможливість однозначної ідентифікації користувача, тоді як приватність стосується контролю над тим, які дані збираються та передаються третім сторонам. Важливою складовою забезпечення приватності є анонімізація даних, що передбачає вилучення ідентифікуючих характеристик таким чином, щоб особу неможливо було встановити навіть шляхом кореляції наборів даних [4].

Незважаючи на наявність технологій захисту, сучасні інструменти трекінгу дозволяють визначати поведінку користувачів високою точністю. Основні загрози включають:

- трекинг активності для рекламних цілей;
- cookies, що дозволяють повторну ідентифікацію;
- IP-ідентифікацію, яка дає змогу оцінити геолокацію;
- browser fingerprinting, який формує унікальний «цифровий профіль» пристрою.

Для мінімізації ризиків застосовуються VPN, мережа Tor, проксі-сервери та захищені месенджери. За даними GlobalStats, понад 54% користувачів не

використовують VPN, що свідчить про низьку цифрову культуру захисту приватності [5].

Порівняння режимів підключення за параметрами анонімності представлено в таблиці 1.

Таблиця 1 – Порівняння режимів підключення за параметрами анонімності.

Режим	**Без захисту**	**VPN**	**Tor**
IP-адреса	188.163.51.123	190.2.147.62	107.189.30.86
Локація	Ukraine	Netherlands	Luxembourg
Провайдер	Kyivstar PJSC	WorldStream LATAM	Luxembourg
Fingerprint унікальність (%)	unique among 4267710	VPN не змінює відбиток	unique among the 4267664
Статус збору даних (що вдалося отримати, а що ні)	Отримано реальні дані пристрою та користувача	Отримано реальні дані пристрою (VPN їх не приховує)	Реальні дані приховано (отримано лише підмінені уніфіковані дані)

Можна побачити, що мережа Tor забезпечує більший рівень анонімності, оскільки одночасно змінює IP та низку технічних параметрів браузера, проте це супроводжується суттєвим зниженням швидкості з'єднання. Варто зазначити, що висока анонімність завжди знижує швидкість інтернету через багаторазове шифрування трафіку.

У майбутньому знадобляться VPN нового покоління, які не лише змінюють IP-адресу, а й повністю маскують відбиток браузера. Так у VPN можна вбудувати функцію антидетекту, яка автоматично підмінятиме дані про пристрій користувача за окрему плату або додаткову функцію.

Список літератури

1. Computer Emergency Response Team of Ukraine Щодо обстановки в сфері кібер на 23-24 лютого 2024 року https://cert.gov.ua/article/6277822 (дата звернення 04.09.2025)

2. Голубничий, Д. Ю., Сєвєрінов, О. В., Коломійцев, О. В., Місюра, О. М., Третяк, В. Ф., Власов, А. В., & Крук, Б. М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

3. P. Laperdrix, W. Rudametkin and B. Baudry, "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 878-894, doi: 10.1109/SP.2016.57.

4. Трибух А. О. «Дослідження архітектурних підходів до забезпечення приватності конфіденційних даних у хмарному середовищі» — пояснювальна записка до магістерської роботи, ХНУРЕ, 2024.

5. NordVPN 2025 VPN Usage Statistics https://www.security.org/vpn/statistics/ (дата звернення 04.09.2025)