ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ ВИКОРИСТАННЯ ВІДБИТКУ БРАУЗЕРА ДЛЯ ЗАХОДІВ КІБЕРЗАХИСТУ

САМОЙЛОВ Станіслав Вадимович - к-т юрид. наук, начальник 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції (міжрегіональний територіальний підрозділ) Національної поліції України

ORCID ID 0009-0004-0057-1126

ШАРОНОВ Андрій Павлович - аспірант Одеського державного університету внутрішніх справ

ORCID ID 0009-0002-1761-9646

КРАЙНІЧУК (ШЕЛЕПАЛО) Галина Василівна - к-т фіз.-мат. наук, доцент кафедри захисту інформації Вінницького національного технічного університету

ORCID ID 0000-0002-6822-4858

УДК 343.98:004.056

DOI: https://doi.org/10.71404/NP.2026.1.6

У статті показано сучасний стан досліджень у сфері браузерного відбитку з точки зору кібербезпеки, конфіденційності та захисту. Систематизовано теоретичні підходи, експериментальні результати та практичні механізми захисту, опираючись на класичні та новітні наукові джерела. Описано нормативно-правову базу України, що регулює застосування технологій ідентифікації користувачів. Дано правове підґрунтя обробки даних, отриманих шляхом використання бібліотек відбитку браузера. Встановлено використання відбитку браузера, як інструменту комплексу організаційних заходів кіберзахисту та сумісність з національною системою кіберзахисту. Сформовано рекомендації для державних органів та приватного сектору щодо використання відбитків браузерів для кіберзахисту, виписано правові гарантії користувачам та наведено баланс між безпекою та приватністю в Україні.

Ключові слова: право; закон; відбиток браузера; метод; цифровий слід; захист; конфіденційність; атака; кібербезпека; кіберзагроза.

Вступ

Стрімке зростання кіберзагроз, поширення бот-мереж, фішингових атак, автоматизованих інструментів обходу автентифікації та використання анонімізаторів створюють потребу в нових, більш ефективних методах ідентифікації технічних параметрів користувацьких систем. У цьому контексті технологія відбитка браузера (browser fingerprinting) дозволяє отримувати унікальний або квазіунікальний набір параметрів клієнтського пристрою та стає важливим інструментом виявлення аномальної активності, протидії автоматизованим кіберзагрозам, а також підсилення автентифікаційних процесів.

За останніх декілька років дослідження у сфері browser fingerprinting активізувалися, а саме: зростає використання цієї технології для трекінгу, здійснюється розробка методів виявлення та захисту. За останнє десятиліття інтерес до веб-ідентифікації без використання кукі зріс. FingerprintJS – популярна у відкритих джерелах бібліотека JavaScript, яка збирає характеристики браузера і формує хеш-ідентифікатор. Її код доступний на GitHub, тому багато дослідників використовують її як референтну реалізацію або порівнювальний орієнтир.

Актуальність дослідження та наукове обґрунтування

У Законі України «Про основні засади забезпечення кібербезпеки України» (2017) підкреслюється необхідність використання сучасних технологій моніторингу та виявлення кіберінцидентів. Browser fingerprinting розглядається як ефективний інструмент:

- виявлення підміни пристрою,
- протидії ботам та скриптованим атакам,
- ідентифікації шкідливої поведінки у веб-системах.

Це особливо важливо для суб'єктів критичної інфраструктури, для яких закон зобов'язує застосовувати комплексні механізми захисту.

У чинному законодавстві України браузерний відбиток не є прямо визначеним видом даних. Проте, відповідно до Закону України «Про захист персональних даних» (2010), будь-які дані, що дають змогу ідентифікувати особу прямо або опосередковано, можуть вважатися персональними.

У воєнних умовах та умовах масових кібератак роль таких технологій зростає в рази. Попри глобальну увагу до проблеми fingerprinting (роботи Su & Kapravelos, FP-Radar, EssentialFP, CSS-Spy тощо), в Україні:

- недостатньо системних досліджень правового статусу fingerprinting,
- немає національних методичних рекомендацій,
- не розроблено офіційних стандартів кіберзахисту з використанням інструментів ідентифікації браузера.

Наукове обґрунтування можливостей, обмежень та правових меж застосування таких технологій є критично важливим для формування політик кіберзахисту на державному рівні, у бізнесі та в приватному секторі.

Україна декларує курс на приведення цифрової безпекової сфери до відповідності стандартам ЄС (GDPR, eIDAS, рекомендації ENISA) [16, 19, 20]. Browser fingerprinting уже розглядається в ЄС як високоризикова технологія, що потребує спеціальних правових процедур та може застосовуватися легально лише за умови належних гарантій приватності.

Наукове дослідження дозволить сформувати рекомендації для адаптації українського законодавства та узгодити підходи до законного використання технології під час кіберзахисту.

Таким чином, актуальність дослідження використання browser fingerprinting у кібербезпеці України зумовлена:

- різким зростанням кіберзагроз,
- правовою невизначеністю статусу таких даних,
- потребою в сучасних засобах кіберзахисту та аналітики,
- необхідністю гармонізації з європейськими нормами,
- відсутністю національних науково-методичних підходів.

Технологія відбитка браузера стає не лише інструментом технічного захисту, але й об'єктом важливих правових, етичних та нормативних досліджень, що робить її вкрай актуальною для сучасної науки в галузі кібербезпеки України.

У цій статті описано питання вивчення механізмів та принципів дії відбитку браузера, особливо з бібліотекою „FingerprintJS" з метою опису організаційно-правового нормативу для використання його в межах комплексу організаційних заходів кіберзахисту.

Постановка проблеми

Аналіз останніх трендів й викликів показує виникнення векторів зловживань через WebAssembly або Performance API, розподілені системи для виявлення fingerprinting (наприклад, федеративне навчання), що спричинює атаки, орієнтовані на розширення браузера. Найновіші дослідження виявляють стратегії відстеження та протидію цих зловживань. Важливо дати оцінку того, на скільки сучасні захисти браузерів є ефективними. Browser fingerprinting, як технологія, здатна забезпечити стабільний спосіб відстеження користувача, навіть без явної персональної інформації. Це створює низку правових питань:

- які режими правової обробки повинні застосовуватись,
- чи потрібна згода користувача,
- чи є такий тип даних частиною критичної інфраструктури безпеки веб-сервісів та інші.

Розв'язання цих та інших питань у правовому полі потребує наукового аналізу, методологічного опису та організаційно-правового обґрунтування. Українське законодавство (зокрема вимоги ДССЗЗІ та Доктрина інформаційної безпеки України) встановлює необхідність розроблення та впровадження сучасних технічних механізмів протидії кіберзагрозам.

Browser fingerprinting може стати:

- основою систем поведінкової аналітики,
- допоміжним механізмом багатофакторної аутентифікації,
- елементом систем виявлення вторгнень (IDS),
- технологією раннього попередження про підозрілу активність.

Стаття висвітлює огляд питання правової етики, регуляторні загрози і перспективи для майбутніх досліджень – з акцентом на баланс конфіденційності та безпеки в цілому.

Мета і завдання дослідження

Метою статті є висвітлення організаційно-правових аспектів з використанням механізмів та принципів дії відбитку браузера з бібліотекою „FingerprintJS", що дають змогу ефективно і з мінімальними витратами організувати його застосування з точки зору кібербезпеки, конфіденційності та захисту.

Завданнями цієї статті є:

- детальний огляд сучасних досліджень механізму та принципів дії технології відбитку браузера;
- огляд нормативно-правового підґрунтя України щодо розробки рекомендацій для державних органів та приватного сектору щодо використання та ризиків відбитків браузерів для заходів кіберзахисту.

Результати дослідження

Механізм та принципи дії технології відбитку браузера

Відбиток браузера утворюється шляхом збору низки параметрів, що відображають конфігурацію та поведінку браузера і пристрою користувача. Згідно з дослідженням Laperdrix та ін. [1-6], для успішної ідентифікації параметри повинні бути одночасно унікальними і стабільними, але достатньо інформативними, щоби відбиток відрізнявся між користувачами. До прикладу, багато відомих скриптів використовують заголовки HTTP (Accept, User-Agent, Connection), мовні налаштування, часовий пояс, роздільну здатність екрана, кольорову глибину, доступні плагіни, список встановлених шрифтів, наявність кукі, локального сховища, атрибути WebGL тощо. Залежно від реалізації, ці параметри збирає JavaScript або Flash-код, а потім надсилає на сервер у вигляді окремих значень або попередньо сформованого хеша [7].

Особливе місце посідає canvas-відбиток: скрипт створює прихований елемент «canvas», малює текст та геометричні фігури, перетворює це зображення в байтовий масив і обчислює контрольну суму. Відмінності в графічних бібліотеках, моделях відеокарт, операційній системі та шрифтах спричиняють малі відхилення в отриманому масиві, що утворює унікальний відбиток. Аналогічні прийоми застосовують для WebGL та аудіо API.

Після збору параметрів їх об'єднують у єдиний рядок і хешують за допомогою криптографічної або швидкої хеш-функції. Перша версія FingerprintJS використовувала алгоритм MurmurHash2, що формував 32-бітний ідентифікатор. На відміну від традиційних хешів, дослідники пропонували застосовувати нечітке хешування (fuzzy hashing). Такий метод розбиває дані на блоки, використовує rolling hash і дозволяє оцінити схожість двох відбитків за допомогою відстані редагування; завдяки цьому невеликі зміни в кількох параметрах не призводять до повного оновлення відбитка [8]. Саме нечіткі хеші застосовуються для виявлення схожих пристроїв або для стійкості відбитку до незначних змін версії браузера.

Зібрані на клієнті параметри часто передаються на сервер для подальшої обробки. У відкритій версії FingerprintJS обчислення відбитку виконувалося в браузері, що забезпечувало простоту, але знижувало точність і дозволяло зловмиснику підмінювати значення [9]. Комерційні сервіси виконують частину алгоритму на сервері, поєднуючи відбиток з додатковими даними (IP-адреса, часові патерни, HTTP-заголовки), що підвищує точність і дозволяє виявляти ботів. Наприклад, сервіс BotD обчислює понад 30 атрибутів, що збирає FingerprintJS, та додатково оцінює послідовність їх зміни в часі [5].

Нормативно-правове підґрунтя використання відбитку браузера

Нормативно-правова база України, що регулює застосування технологій ідентифікації користувачів пояснює, згідно із ЗУ «Про основні засади забезпечення кібербезпеки України» від 2017 року те, що базові механізми організації кіберзахисту для державних і приватних суб'єктів можуть використовувати browser fingerprinting, як інструмент виявлення несанкціонованого доступу, бот-діяльності, сесійних атак або діяльності обхідних інструментів. Для цього важливими є такі положення цього Закону зі ст. 4, що визначає об'єкти кібербезпеки та кіберзахисту, якими є інформаційні та комунікаційні системи, мережі, інформаційні ресурси, що мають важливе значення для життєдіяльності суспільства та держави, а також критична інформаційна інфраструктура, і встановлює, що порядок функціонування Національної телекомунікаційної мережі та інші питання кіберзахисту регулюються Кабміном та відповідальними органами. А це спричинює формування принципів кібербезпеки, що підкреслюють необхідність застосування сучасних технологій виявлення та протидії кіберзагрозам. Відповідно до ст. 9 цього Закону – обов'язок суб'єктів критичної інфраструктури забезпечувати комплексний кіберзахист, що включає моніторинг аномальної активності.

Browser fingerprinting може бути частиною таких систем, тому може активно виявляти кіберзагрози та може вправно документувати обхідні дані та сесійні атаки.

Відповідно до наказу ДССЗЗІ № 600 від 2017 р. «Про затвердження вимог з технічного захисту інформації» використання browser fingerprinting може бути інструментом комплексу організаційних заходів кіберзахисту. Впровадження заходів контролю доступу, моніторингу та журналювання є обов'язковим у захищених інформаційних системах. Browser fingerprinting відповідає цим вимогам, оскільки забезпечує:

- неперсоніфікований, але стабільний індикатор користувацької активності;
- виявлення аномалій, включно з підміною сесії, бот-атаками, використанням VPN/Tor/анонімізаторів,
- додатковий фактор ризик-орієнтованої аутентифікації, рекомендований міжнародними стандартами (NIST SP 800-63B).

Доктрина інформаційної безпеки України (Указ Президента №47/2017) визначає сумісність browser fingerprinting із національною системою кіберзахисту. У документі встановлено необхідність:

- впровадження сучасних систем аналізу трафіку;
- моніторингу кіберінцидентів;
- виявлення загроз у реальному часі.

Fingerprinting виконує роль низькорівневої поведеневої телеметрії, що дозволяє:

- виявляти шкідливу автоматизовану поведінку;
- фіксувати спроби обходу автентифікації;
- підсилювати інструменти threat intelligence.

Питання, чи є браузерний відбиток персональними даними в Європейському Союзі, однозначне (GDPR – так). В Україні використання browser fingerprinting потребує обґрунтованої правової підстави (згода користувача, безпекова необхідність, договірні зобов'язання). Це регламентується Законом України «Про захист персональних даних» від 2010 року, а саме: згідно зі ст. 2 персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. І це визначає персональні дані як інформацію, що дає можливість ідентифікувати фізичну особу.

Browser fingerprinting не містить даних ПІБ, але може забезпечувати унікальну ідентифікацію, а отже, підпадає під дію закону в контексті «опосередкованої ідентифікації». Наприклад, стаття 6 вимагає, щоб обробка таких даних була законною, пропорційною та мінімально необхідною, а стаття 8 – забезпечує право суб'єкта даних на інформацію щодо збору таких даних.

Основна вимога Закону України про «Про електронні довірчі послуги» від 2017 року – використання надійних засобів автентифікації. Відповідно до цього, browser fingerprinting може застосовуватися як:

- додатковий фактор у моделі risk-based authentication;
- механізм підтвердження цілісності клієнтського середовища;
- засіб виявлення заражених або модифікованих клієнтських пристроїв.

Проте, fingerprinting не може бути самостійною формою електронної ідентифікації чи підпису, оскільки не має юридично значимого статусу.

Основними ризиками, визначеними нормами українського законодавства є:

1) Порушення приватності. Враховуючи технологічну можливість унікальної ідентифікації, організація має забезпечити інформування та мінімізацію даних (ст. 6 та ст. 8 Закону України «Про захист персональних даних») на захист від автоматизованого рішення, яке має для нього правові наслідки.

2) Непрозора обробка поведінкових даних. Користувач має бути повідомлений про мету й обробку даних, а саме знати механізм автоматичної обробки персональних даних.

3) Загроза надмірного моніторингу. Використання fingerprinting має бути пропорційним до загроз (принцип пропорційності обробки).

4) Відповідальність за витік інформації. (У межах ст. 10 Повноваження державних органів у сфері захисту інформації в системах відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»). Витік зібраних відбитків може дозволити стороннім суб'єктам стежити за користувачем. А це, у свою чергу, тягне кримінальну відповідальність, що регулюється низкою статтей кримінального Кодексу, а саме: відповідно до ст.364 зловживання службовим становищем, до ст. 365 перевищення влади, до ст. 328 розголошення державної таємниці, до ст.367 недбалого ставлення, а також недотримання правил захисту іфнормації.

Організаційно-правові рекомендації

Формування відбитку – це процес збору множини атрибутів браузера й пристрою (HTTP-заголовки, JS-параметри, canvas/WebGL, шрифти, плагіни тощо). Надійний fingerprint потребує одночасної унікальності та стабільності компонентів, що об'єктивно показано в [7].

Класичне хешування (наприклад, MurmurHash2) перетворює всю сукупність даних у єдиний 32- або 128-бітовий код, але навіть невелика зміна вхідних даних призводить до нового хешу. Тому цей підхід дає високу унікальність (~90 %), але погано переносить оновлення.

Нечітке хешування або Locality-Sensitive Hashing дозволяє оцінити схожість відбитків; він ділить вхід на блоки та генерує підхеші, тож невеликі зміни не впливають на загальний ідентифікатор [8]. Для швидкого пошуку схожих відбитків можна застосовувати MinHash+LSH [13].

На практиці: у системі AIS JavaScript-бібліотека FingerprintJS використовується тільки для збору компонентів; обчислення нечіткого хешу здійснюється на бекенді (PHP). Параметри з різною стабільністю мають різні ваги; невеликі зміни (версія браузера, часовий пояс) не повинні створювати новий профіль.

Захист приватності – важливо не зберігати персональні дані, псевдонімізувати відбитки та використовувати їх лише для легітимних цілей (безпека, аналіз).

Актуальні тренди – дослідники розробляють анти-fingerprinting розширення, а стандартизатори (W3C [1]) працюють над зменшенням поверхні атаки та балансом між функціональністю і приватністю [1].

Зберігання та безпека даних – зберігаючи відбитки, необхідно враховувати вимоги законодавства (GDPR, ePrivacy) [18, 19] та правила безпеки:

- мінімізація даних, наприклад у [7] запропоновано не включати у fingerprint персональні дані (IP-адреси) та збирати лише технічні параметри;
- хешування та псевдонімізація, тобто замість збереження оригінальних атрибутів можна зберігати їх хеші. У практиках електронної пошти fuzzy-hashing дозволяє знаходити подібні повідомлення без зберігання їх тексту [14];
- оновлення та контроль версій. Потрібно фіксувати дату та час створення відбитка для відстеження змін;
- розмежування доступу, а саме: доступ до бази відбитків має бути обмежений, тому рекомендується зберігати хеші та допоміжні дані окремо.

На основі аналізу українського законодавства та міжнародної практики можна виокремити такі організаційно-правові рекомендації щодо впровадження FP-технологій:

1) Розробка локальних політик, а саме, політика приватності має містити розділ про browser fingerprinting, та необхідно визначити правову підставу для обробки (згода/ легітимний інтерес/ безпекова потреба).

2) Пропорційність застосування, тобто fingerprinting має використовуватись лише у випадках: виявлення ботів, захисту аутентифікаційних сесій, моніторингу ризикових транзакцій.

3) Захист даних, тобто використання хешування або псевдонімізації зібраних параметрів та обмеження зберігання fingerprint-ідентифікаторів.

4) Інтеграція в інцидент-менеджмент, мається на увазі, що fingerprinting має входити до системи журналювання та виявлення інцидентів згідно з вимогами ДССЗЗІ.

Сформуємо модель нормативно-правових рекомендацій щодо використання Browser Fingerprinting в Україні. Модель рекомендована для державних органів, суб'єктів критичної інфраструктури, комерційних структур, розробників веб-сервісів та провайдерів електронних послуг.

Модель нормативно-правових рекомендацій щодо використання Browser Fingerprinting в Україні грунтується на таких загальних принципах впровадження:

1) Законність обробки, а саме - застосовувати fingerprinting лише за умови відповідності, як мінімум:

- Закону України «Про захист персональних даних» (2010),
- Закону «Про основні засади забезпечення кібербезпеки України» (2017),
- Закону «Про інформацію» (1992),
- Закону «Про електронні довірчі послуги» (2017).

2) Пропорційність та мінімізація, тобто обсяг параметрів, що збираються, має бути мінімально необхідним для цілей кіберзахисту. Заборонити збір надлишкових даних (наприклад, характеристик, які не впливають на оцінку ризику).

3) Технічна безпека та криптографічний захист: чітко описане хешування або псевдонімізація fingerprint-ідентифікаторів, відповідно до вимог ДСТУ 4145-2002 і рекомендацій ДССЗЗІ.

4) Прозорість та повідомлення користувачів, тобто в політиці конфіденційності варто прямо вказати, що збираються дані клієнтського середовища, мету збору даних (наприклад, боротьба із шахрайством, виявлення ботів, безпека облікових записів) та тривалість зберігання зібраних даних.

5) Обмеження вторинного використання, а саме: заборонити використання fingerprint'ів для маркетингового трекінгу, якщо вони збиралися для цілей кіберзахисту.

Рекомендації для державних органів:

1) Розробити офіційні методичні рекомендації на рівні Мінцифри або Національного координаційного центру кібербезпеки (НКЦК) розробити документ, що регламентує:

- перелік допустимих параметрів браузера,

- цілі і правові режими обробки,
- критерії пропорційності,
- механізми аудиту систем.

2) Стандартизувати використання в критичній інфраструктурі, зокрема додати fingerprinting до переліку рекомендованих технологій у сферах:

- виявлення вторгнень (IDS),
- моніторингу веб-доступу,
- ризик-орієнтованої автентифікації.

3) Уніфікувати підходи до зберігання та обробки, тобто розробити стандарти для:

- часу зберігання fingerprint-даних,
- використання хеш-функцій,
- вимог до журналювання дій.

Рекомендації для приватного сектору:

1) Використання в ризик-орієнтованій аутентифікації: Fingerprinting має бути додатковим, а не основним фактором. Наприклад:

- виявлення входу з невідомого пристрою,
- оцінка ризику при платіжних операціях,
- аналіз підозрілої поведінки сесії.

2) Використання в антифрод-системах: інтеграція fingerprinting, наприклад, з:

- CAPTCHA,
- поведінковими моделями,
- ML-системами виявлення ботів.

3) Документування процесу обробки, а саме компаніям рекомендується вести, до прикладу:

- журнал операцій із fingerprint-даними,
- політики доступу,
- внутрішні процедури реагування на інциденти

Правові гарантії користувачам:

1) Право на доступ до інформації про обробку (ст. 8 Закону «Про захист персональних даних»).

2) Право на виправлення або видалення персональних даних (у межах технічно можливого).

3) Заборона профілювання користувача без явної згоди.

4) Встановлення термінів зберігання (наприклад, 90-180 днів для кіберзахисту).

Використання fingerprinting в Україні може бути легальним, якщо забезпечити баланс. Баланс між безпекою та приватністю сформовано в таблиці 1.

Таблиця 1. Баланс між безпекою та приватністю

Безпека	Приватність
Виявлення ботів та атак	Прозорість обробки
Захист акаунтів	Мінімізація параметрів
Контроль доступу	Хешування та псевдомінімізація
Розслідування інцидентів	Терміни зберігання та обмеження доступу

Висновки та перспективи подальших досліджень

Практичні застосування браузерних відбитків:

1) Безпека та боротьба із шахрайством – верифікація пристрою при авторизації та аналіз транзакцій для виявлення ботів або підозрілих дій.

2) Аналітика та персоналізація – ідентифікація повторних відвідувачів для накопичення анонімної статистики.

3) Цільова реклама та трекінг – створення профілів для рекламних мереж.

4) Вимірювання ефективності та обмеження відбитку браузера досліджена на унікальність, стабільність, продуктивність та прихильність до приватності.

Відбиток браузера є якісним інструментом, але його надійність не абсолютна. Відповідність одного відбитка одному пристрою не гарантується: однакові конфігурації утворюють однаковий відбиток, а часті оновлення програмного забезпечення або зміна обладнання можуть змінити результати. Водночас застосування нечітких хешів та комбінування кількох джерел даних (IP, час, поведінкові патерни) значно підвищує точність, що робить технологію привабливою для захисту від ботів та шахрайства.

Розробникам та законодавцям необхідно збалансувати користь (безпека, боротьба з ботами) і ризики (порушення приватності, можливість демографічного профілювання) та встановити чіткі обмеження щодо використання браузерного відбитку.

Організаційно-правове застосування browser fingerprinting в Україні цілком допустиме, якщо воно не суперечить основним законам у сфері кібербезпеки, приватності та інформаційного захисту. Fingerprinting може бути потужним елементом системи протидії кіберзагрозам за умови:

- прозорості обробки даних;
- забезпечення приватності користувачів;
- впровадження технічних та організаційних заходів захисту;
- чіткої відповідності законодавству України.

Browser fingerprinting є перспективним інструментом кіберзахисту в Україні, проте його використання має бути врегульоване через:

- розробку методичних рекомендацій**,**
- юридичні обмеження щодо приватності**,**
- чітке визначення правового режиму даних**,**
- інтеграцію з національною системою кібербезпеки**.**

За умови правильної юридичної та технічної імплементації fingerprinting може значно підвищити рівень захисту інформаційних систем, не порушуючи прав громадян.

Література

1. W3C Group Note *Mitigating Browser Fingerprinting in Web Specifications* // 12 September 2025. URL: https://www.w3.org/TR/fingerprinting-guidance/#:~:text=1 (Дата звернення 01.12.2025)

2. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, Gildas Avoine *Browser Fingerprinting: A survey* // arXiv, Vol. 1, No. 1, Article . Publication date: November 2019. – P. 1-32. URL: https://arxiv.org/pdf/1905.01051 (Дата звернення 01.12.2025)

3. Xu Lin, Panagiotis Ilia, Saumya Solanki, and Jason Polakis *Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting* // From the Proceedings of the 31st USENIX Security Symposium. August 10-12, 2022. – Boston, MA, USA. – P. 1651-1668. URL: https://www.usenix.org/system/files/sec22-lin-xu.pdf (Дата звернення 01.12.2025)

4. Xu Lin, Frederico Araujo, Teryl Taylor, Jiyong Jang†, Jason Polakis *Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses* // P. 1-18. URL:https://www.cs.uic.edu/~polakis/papers/lin-sp23.pdf (Дата звернення 01.12.2025)

5. Hari Venugopalan, Tangbaihe Wang, Shaoor Munir, Samuel T. King, Shuaib Ahmed, Zubair Shafiq, *FP-Inconsistent: Detecting Evasive Bots using Browser Fingerprint Inconsistencies* // arXiv:2406.07647v1 [cs.CR] 11 Jun 2024, URL: https://arxiv.org/pdf/2406.07647v1 (Дата звернення 01.12.2025)

6. Alex Berke, Enrico Bacis, Badih Ghazi, Pritish Kamath, Ravi Kumar, Robin Lassonde, Pasin Manurangsi, Umar Syed, *How Unique is Whose Web Browser? The Role of Demographics in Browser Fingerprinting among US Users* // arXiv:2410.06954v2 [cs.CY] 11 Oct 2024, URL: https://arxiv.org/pdf/2410.06954v2 (Дата звернення 01.12.2025)

7. Kiu Nai Pau, Vicki Wei Qi Lee, Shih Yin Ooi and Ying Han Pang. *Communication The Development of a Data Collection and Browser Fingerprinting System* // Sensors 2023, 23, 3087. URL: https://doi.org/10.3390/s23063087. https://www.mdpi.com/journal/sensors (Дата звернення 01.12.2025)

8. Lukas Rist *Locality Sensitive Fuzzy Hashing* // Medium 2018. URL: https://medium.com/@glaslos/locality-sensitive-fuzzy-hashing-66127178ebdc

9. Master https://github.com/fingerprintjs/fingerprintjs (Дата звернення 01.12.2025)

10. Alexander Sjosten, Daniel Hedin, Andrei Sabelfeld, *EssentialFP: Exposing the Essence of Browser Fingerprinting* // URL: https://secweb.work/papers/2021/sjoesten2021essential.pdf (Дата звернення 01.12.2025)

11. Peter Eckerley, Is Every Browser Unique? Results Fom The Panopticlick Experiment. URL: https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick#:~:text=The%20results%20show%20that%20the,IP%20addresses%2C%20and%20supercookies%20are (Дата звернення 01.12.2025)

12. Kaitong Lin, Huazhu Cao, Amin Milani Fard *Browser Fingerprint Detection and Anti-Tracking* // arXiv:2502.14326v1 [cs.CR] 20 Feb 2025. URL: https://arxiv.org/html/2502.14326v1 (Дата звернення 01.12.2025)

13. Marcin Gabryel *Methods of Searching for Similar Device Fingerprints Using Changes in Unstable Parameters* // In book: Artificial Intelligence and Soft Computing, 19th International Conference, ICAISC 2020, Zakopane, Poland, October 12-14, 2020, Proceedings, Part II (pp.325-335) URL: https://www.researchgate.net/publication/345601630 (Дата звернення 01.12.2025)

14. Fingerprinting & Fuzzy Hashing Explained. URL: Https://www.meshsecurity.io/blog/fuzzyhashing#:~:text=original%20email%20in%20a%20database%2C,requirement%20to%20retain%20sensitive%20information (Дата звернення 01.12.2025)

15. Kamarinou D., Millard C., Singh J. Machine Learning with Personal Data: Is Data Protection Law Ready? // Computer Law & Security Review. 2016. Vol. 34(2). P. 539-551.

16. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI // Columbia Business Law Review. 2019. Issue 2. P. 494-620.

17. European Data Protection Board (EDPB). Opinion 5/2019 on the interplay between ePrivacy Directive and GDPR**.** Brussels, 2019. 32 p.

18. Article 29 Data Protection Working Party. Opinion 9/2014 on the application of Directive 2002/58/EC (ePrivacy) to device fingerprinting**.** Brussels, 2014. 38p.

19. Tikk E., Kerttunen M. Cybersecurity Law and Regulation**.** Tallinn: NATO CCDCOE, 2020. 74 p.

20. Mozilla Foundation. Anti-Tracking Policy. Firefox Engineering Documentation, 2023. 22 p.

21. Про захист персональних даних**:** Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

22. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. 1992. № 48. Ст. 650.

23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. №45. Ст. 403.

24. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 404.

25. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. 1994. № 31. Ст. 286.

26. Державна служба спеціального зв'язку та захисту інформації України. Керівництво з організації кіберзахисту об'єктів критичної інфраструктури. Київ: ДССЗЗІ, 2022. 56 с.

27. Концепція розвитку цифрової економіки та суспільства України на 2018-2025 роки, схвалена розпорядженням КМУ від 17.01.2018 № 67-р.

Reference

1. W3C Group Note *Mitigating Browser Fingerprinting in Web Specifications* // 12 September 2025. URL: https://www.w3.org/TR/fingerprinting-guidance/#:~:text=1

2. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, Gildas Avoine *Browser Fingerprinting: A survey* // arXiv, Vol. 1, No. 1, Article . Publication date: November 2019. – P. 1-32. URL: https://arxiv.org/pdf/1905.01051

3. Xu Lin, Panagiotis Ilia, Saumya Solanki, and Jason Polakis *Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting* // From the Proceedings of the 31st USENIX Security Symposium. August 10-12, 2022. – Boston, MA, USA. – P. 1651-1668. URL: https://www.usenix.org/system/files/sec22-lin-xu.pdf

4. Xu Lin, Frederico Araujo, Teryl Taylor, Jiyong Jang†, Jason Polakis *Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses* // P. 1-18. URL:https://www.cs.uic.edu/~polakis/papers/lin-sp23.pdf

5. Hari Venugopalan, Tangbaihe Wang, Shaoor Munir, Samuel T. King, Shuaib Ahmed, Zubair Shafiq, *FP-Inconsistent: Detecting Evasive Bots using Browser Fingerprint Inconsistencies* // arXiv:2406.07647v1 [cs.CR] 11 Jun 2024, URL: https://arxiv.org/pdf/2406.07647v1

6. Alex Berke, Enrico Bacis, Badih Ghazi, Pritish Kamath, Ravi Kumar, Robin Lassonde, Pasin Manurangsi, Umar Syed, *How Unique is*

Whose Web Browser? The Role of Demographics in Browser Fingerprinting among US Users // arXiv:2410.06954v2 [cs.CY] 11 Oct 2024, URL: https://arxiv.org/pdf/2410.06954v2

7. Kiu Nai Pau, Vicki Wei Qi Lee, Shih Yin Ooi and Ying Han Pang. *Communication The Development of a Data Collection and Browser Fingerprinting System* // Sensors 2023, 23, 3087. URL: https://doi.org/10.3390/s23063087. https://www.mdpi.com/journal/sensors

8. Lukas Rist *Locality Sensitive Fuzzy Hashing* // Medium 2018. URL: https://medium.com/@glaslos/locality-sensitive-fuzzy-hashing-66127178ebdc

9. Master https://github.com/fingerprintjs/fingerprintjs

10. Alexander Sjosten, Daniel Hedin, Andrei Sabelfeld, *EssentialFP: Exposing the Essence of Browser Fingerprinting* // URL: https://secweb.work/papers/2021/sjoesten2021essential.pdf

11. Peter Eckerley, Is Every Browser Unique? Results Fom The Panopticlick Experiment. URL: https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick#:~:text=The%20results%20show%20that%20the,IP%20addresses%2C%20and%20supercookies%20are

12. Kaitong Lin, Huazhu Cao, Amin Milani Fard *Browser Fingerprint Detection and Anti-Tracking* // arXiv:2502.14326v1 [cs.CR] 20 Feb 2025. URL: https://arxiv.org/html/2502.14326v1

13. Marcin Gabryel *Methods of Searching for Similar Device Fingerprints Using Changes in Unstable Parameters* // In book: Artificial Intelligence and Soft Computing, 19th International Conference, ICAISC 2020, Zakopane, Poland, October 12-14, 2020, Proceedings, Part II (pp.325-335) URL: https://www.researchgate.net/publication/345601630

14. Fingerprinting & Fuzzy Hashing Explained. URL: Https://www.meshsecurity.io/blog/fuzzyhashing#:~:text=original%20email%20in%20a%20database%2C,requirement%20to%20retain%20sensitive%20information

15. Kamarinou D., Millard C., Singh J. Machine Learning with Personal Data: Is Data Protection Law Ready? // Computer Law & Security Review. 2016. Vol. 34(2). P. 539-551.

16. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI // Columbia Business Law Review. 2019. Issue 2. P. 494-620.

17. European Data Protection Board (EDPB). Opinion 5/2019 on the interplay between ePrivacy Directive and GDPR. Brussels, 2019. 32 p.

18. Article 29 Data Protection Working Party. Opinion 9/2014 on the application of Directive 2002/58/EC (ePrivacy) to device fingerprinting. Brussels, 2014. 38p.

19. Tikk E., Kerttunen M. Cybersecurity Law and Regulation. Tallinn: NATO CCDCOE, 2020. 74 p.

20. Mozilla Foundation. Anti-Tracking Policy. Firefox Engineering Documentation, 2023. 22 p.

21. On the Protection of Personal Data: Law of Ukraine dated 01.06.2010 No. 2297-VI // Bulletin of the Verkhovna Rada of Ukraine. 2010. No. 34. Art. 481.

22. For information: Law of Ukraine dated 02.10.1992 No. 2657-XII // Bulletin of the Verkhovna Rada of Ukraine. 1992. No. 48. Art. 650.

23. On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII // Bulletin of the Verkhovna Rada of Ukraine. 2017. No. 45. Art. 403.

24. On electronic trust services: Law of Ukraine dated 05.10.2017 No. 2155-VIII // Bulletin of the Verkhovna Rada of Ukraine. 2017. No. 45. Art. 404.

25. On the protection of information in information and telecommunication systems: Law of Ukraine dated 05.07.1994 No. 80/94-VR // Proceedings of the Verkhovna Rada of Ukraine. 1994. No. 31. Art. 286.

26. State Service for Special Communications and Information Protection of Ukraine. Guidelines for the Organization of Cyber Protection of Critical Infrastructure Facilities. Kyiv: DSSZZI, 2022. 56 p.

27. Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2025, approved by the Resolution of the Cabinet of Ministers of Ukraine dated January 17, 2018, No. 67-r.

Samoylov Stanislav Vadymovych,
Candidate of Law, Head of the 3rd Department (Information Technologies and Programming) of the Cyberpolice Department (Interregional Territorial Division) of the National Police of Ukraine
ORCID ID 0009-0004-0057-1126
s.v.stan88@gmail.com
Sharonov Andrii Pavlovych,
Postgraduate Student, Odessa State University of Internal Affairs
ORCID ID 0009-0002-1761-9646
andrii.sharonov@cyberpolice.gov.ua
Kraynichuk (Shelepalo) Halyna Vasylivna,
Candidate of Physics and Mathematics, Associate Professor, Department of Information Protection, Vinnytsia National Technical University
ORCID ID 0000-0002-6822-4858
kraynichuk@ukr.net

ORGANIZATIONAL AND LEGAL ASPECT OF USING BROWSER FINGERPRINT FOR CYBER PROTECTION MEASURES

The article shows the current state of research in the field of browser fingerprinting from the point of view of cybersecurity, confidentiality and protection. Theoretical approaches, experimental results and practical protection mechanisms are systematized, based on classical and modern scientific sources. The regulatory and legal framework of Ukraine that regulates the use of user identification technologies is described. The legal basis for processing data obtained through the use of browser fingerprint libraries is given. The use of browser fingerprinting as a tool in a complex of organizational measures for cyber protection and compatibility with the national cyber protection system are established. Recommendations are formulated for state bodies and the private sector on the use of browser fingerprinting for cyber protection, legal guarantees for users are outlined and the balance between security and privacy in Ukraine is given.

Keywords: law; browser fingerprint; method; digital footprint; protection; privacy; attack; cybersecurity; cyber threat.