УДК 004.05
Зайко Т.А.[1], Чернявський К.Є.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. КНТ-139 НУ «Запорізька політехніка»

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧА У МЕРЕЖІ ЗА ДОПОМОГОЮ ВІДБИТКУ БРАУЗЕРА

Сьогодні сучасний світ неможливо уявити без використання Інтернету. Майже усі послуги стали доступні онлайн завдяки мережі. Спілкування з людьми, перегляд фільму, придбання речей, доставка товару та багато чого іншого робиться через використання Інтернету. Проте безпека сайту, аналіз відвідувачів, захист інформації, інтернет-віруси теж розвиваються кожного дня, використовуючи нові технології.

Один з методів відстеження активності користувачів є метод ідентифікації за допомогою відбитку браузера. Цей метод використовується сайтами та сервісами для відстеження відвідувачів.

Користувачам надається унікальний ідентифікатор-відбиток. Він містить багато інформації про налаштування та можливості браузера користувачів, що використовується для їхньої ідентифікації. Крім того, відбиток браузера дозволяє сайтам відслідковувати поведінкові патерни, щоб згодом ідентифікувати користувачів.

Згідно з дослідженням [2] відбиток браузера включає: User-agent, часовий пояс, роздільну здатність екрана та глибину кольору, Supercookies, налаштування cookie, системні шрифти, плагіни до браузера та їхньої версії, журнал відвідувань.

Проте, відбиток браузера має свої недоліки та переваги. До переваг можна віднести можливості, котрі описані далі.

По-перше, це запобігання шахрайству та крадіжці особистості.

Користувач мережі Інтернет сам того не підозрюючи надає дані про себе, без будь-якої згоди, формується профіль людини, здатний містити у собі стать, вік, сімейний стан, фінансовий стан, інтереси, звички тощо.

Друга перевага, коли користувач пристрою отримує оптимізований для нього сайт, незалежно, зайшов він в інтернет з планшета або смартфона.

Третя перевага це виявлення ботнетів. Це реально корисна для банків та фінансових організацій функція. Вони дозволяють відокремити поведінку користувача від активності зловмисників.

Також визначення VPN та proxy користувачів теж відноситься до переваг. Розвідслужби можуть використовувати цей метод для відстеження інтернет-користувачів із прихованими IP-адресами.

Проте недоліки також мають важливу частину у системі ідентифікації відбитком. Загроза конфіденційності – головна причина. Fingerprints набагато підступніші за cookies. Від них складніше захиститися, при цьому неможливо дізнатися про те, чи стежать за користувачем.

Відбитки браузера роблять його власника впізнаним не тільки на ресурсах, що часто відвідуються, але і в інших електронних джерелах.

Fingerprints фіксують цілісну картину, яку ресурс отримує від браузера, що дає можливість ідентифікувати клієнта навіть при змінах в налаштуваннях.

Відбитки можуть звести нанівець конфіденційність і ділового листування, і особистого.

Fingerprints як регенератор шкідливих cookies і розповсюджувач користувача IP. Багато сайтів застосовують super cookies, здатні відновлювати звичайні cookies у разі їхнього видалення клієнтом. Відбиток браузера може не тільки відновити всю бібліотеку cookies, але й обчислити користувача за основними мережевими даними. Це зробить процес очищення системи від cookies марним – сайт все одно дізнається про клієнта.

Автономність. Для ідентифікації відбитків конкретного браузера бібліотеки cookies можуть навіть не знадобитися. Навіть заблокувавши виконання всіх потенційно шкідливих операцій, користувач не може бути впевнений у тому, що fingerprints не помітять його ПК.

Підсумовуючи, можна сказати, що метод відстеження активності користувачів, за допомогою ідентифікації відбитку браузера є актуальним та корисним методом відстеження активності користувача. Проте така система має свої недоліки, котрі мають неякісну захищеність даних, які потрібно вдосконалювати та модернізувати.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Habr.com [Електронний ресурс]. – Режим доступу : https://habr.com/ru/company/selectel/blog/521550/

2. EFF (Electronic Frontier Foundation) [Електронний ресурс]. – Режим доступу: https://www.eff.org/updates/

3. VCRU [Електронний ресурс]. – Режим доступу : https://vc.ru/u/738105-adspower-browser/212732-fingerprint/

4. Whoer [Електронний ресурс]. – Режим доступу : https://whoer.net/blog/ru/unikalnye-otpechatki-brauzera-fingerprints