

*Алексеев П.А., студент 1 курса  
факультет информационных технологий  
Брянский государственный университет  
г. Брянск, Россия*

## **ОТСЛЕЖИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА**

***Аннотация.** В статье рассматриваются принципы отслеживания пользователей в интернете, даются краткие характеристики каждому из методов.*

***Ключевые слова:** UserAgent, JavaScript, открытые данные, вебвизор.*

***Annotation.** The article discusses the principles of tracking users on the Internet, gives a brief description of each of the methods.*

***Keywords:** UserAgent, JavaScript, open data, webvisor.*

### ***Методы отслеживания пользователей в интернете.***

Слежка за посетителями сайта осуществляется с одной целью – сбор важной информации, делается это для улучшения ресурса, либо для рекламы конкретных товаров. Поначалу владельцы сайтов пытаются определиться с предпочтением посетителей, а после уже начинается тотальный контроль действий и навязывание продукции. В данной статье пойдет речь о самых распространенных методах отслеживания

### ***Использование UserAgent***

Один из самых простых способов получения дополнительной информации о посетителях сайта. User-Agent – это текстовая строка, предназначенная для идентификации веб-браузера и операционной системы для сервера. С ее помощью можно выявить следующую информацию:

- Версия и наименования обозревателя;
- Язык и регион;

- Операционная система;
- Тип устройства, с которого выполнен вход (компьютер, смартфон или планшет);
- Программное обеспечение, которое установлено в девайсе

Благодаря такому подходу владелец ресурса может узнать, откуда и с какой целью был сделан запрос.

При необходимости ЮзерАгент можно заменить. Это позволит изменить параметры индексации и скрыть важную информацию от посторонних лиц. Стоит заметить, что для каждого браузера и операционной системы предусмотрены свои User-Agent.

### *Эффективный JavaScript*

JavaScript представляет собой библиотеку, предназначенную для сбора информации о деятельности пользователей. Сюда относятся клики, переходы по URL и прочие действия, совершенные посетителями сайта. Использовать JavaScript можно в нескольких направлениях: сторонние ресурсы и внутренняя структура сайта. После сбора информации библиотека передает данные владельцу.

В настоящее время существует множество скриптов с различными характеристиками, однако, принцип действия у всех одинаковый:

1. Переход по ссылке.
2. Передача информации в считывающую библиотеку.
3. Передача информации из библиотеки владельцу сайта.
4. Анализ и настройка рекламы.

В частых случаях JavaScript используют через Geolocation API. В этом случае определить информацию о посетителях можно будет по Wi-Fi, GPS и геолокации по IP. Когда будет осуществлен запрос данных, обозреватель задействует одновременно все три способа

### *Деанонимизация*

К этому методу прибегают в крайних случаях, деанонимизация является злостным нарушением анонимности пользователя, да и разведка по открытым

данным, как и грамотное написание следящего ПО — метод, которым владеет далеко не каждый. Суть деанонимизации заключается в поиске и подробном анализе цифровых следов. Дело в том, что каждый посетитель сайта оставляет после себя некую информацию. Это может быть время, которое он находился в ресурсе, версия браузера с установленными плагинами, информация о разрешении экрана, cookie-файлы и т.д. В зависимости от скорости выполнения задачи и нанесения ущерба устройствам пользователя деанонимизация разделяется на несколько методов:

### ***Административный.***

В этом случае выполняется отправка запроса хостинг-провайдеру, чтобы получить разрешение для подключения к серверу. Если в процессе используется несколько VPN, запросы, начиная с последнего, будут отправляться поочередно каждому провайдеру. Такой подход позволит выйти к первому звену, к которому осуществлено подключение с адреса IP.

### ***Вредоносный.***

В случае использования данного метода на компьютер жертвы отправляется вредоносное ПО, которое будет передавать информацию на управляющий сервер. В полученных пакетах данных будет храниться действующий IP-адрес пользователя. Стоит заметить, что вредоносное ПО может выступать в качестве обычной картинки, видео или документа.

### ***Деанонимизация по открытым сведениям***

Одним из самых простых способов деанонимизации пользователя является использование открытой информации. Даже после обычного перехода на сайт посетитель оставляет массу персональных данных, которые можно использовать для выполнения задачи:

### ***Список контактов.***

Используя список друзей на одном ресурсе, можно с легкостью определить подробную информацию о пользователе на другом. Работает даже в том случае, если на сайте указаны ложные данные.

### ***Никнейм.***

Чтобы не запоминать свой логин и пароль, многие пользователи применяют идентичные никнеймы для разных ресурсов. Именно эта информация используется для деанонимизации.

### ***Изображения.***

Один из самых эффективных способов деанонимизации, в процессе которого используются фотографии пользователя. Если посетитель сайта использовал идентичное изображение на разных ресурсах, отыскать о нем информацию не составит труда.

### ***Речь и голос.***

В некоторых случаях прибегают даже к анализу речевых способностей, ведь голосовой отпечаток является уникальным

### ***Вебвизор***

Еще одно эффективное средство для отслеживания посетителей веб-сайтов, разработанное компанией Яндекс. Вебвизор достаточно прост в использовании, так как для его функционирования потребуется всего лишь установить специальный код на свой сайт. После этого удастся отследить следующие действия пользователей:

- Переход по URL и клики;
- Перемещение курсора;
- Копированный или выделенный текст;
- Прокрутка страницы;
- Поиск конкретной информации;
- Заполнение полей и строк;
- Загрузка изображений или видеофайлов.

Благодаря специальным условным обозначениям сервиса владелец сайта может определить:

- Какая область ресурса не нравится пользователям;
- Какой формой заполнения чаще всего пользуются посетители;
- Какие блоки привлекают больше внимания;

- Какой продающий текст стоит улучшить или вообще удалить;
- Какой триггер является наиболее эффективным.

Внимание! Максимальную точность данных можно получить в том случае, когда будет проведен анализ минимум с 1 тысячи посещений. В противном случае будет слишком большая погрешность и собранная статистика не будет являться верной

### ***Подводя итоги***

Как говорилось ранее, к слежке за посетителями на сайте прибегают по нескольким причинам – улучшение своего ресурса или продажа конкретной продукции. Однако перед использованием любого из описанных методов следует помнить, что отслеживание деятельности пользователей не всегда является законным.

### **Использованные источники:**

1. Колисниченко Д.Н. Анонимность и безопасность в Интернете. От «чайника» к пользователю — 2012 — С 30-34
2. Джейми Бартлетт .Подпольный интернет. Кто скрывается в цифровом подполье - 2016 — С 39 - 42