НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004.42

МЕТОДИКИ ОТСЛЕЖИВАНИЯ И ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ ИНТЕРНЕТ

Соколов Константин Валерьевич
студент, Ульяновский государственный технический университет
РФ, г. Ульяновск

Рогов Виктор Николаевич
научный руководитель, канд. техн. наук, доцент, Ульяновский государственный технический университет
РФ, г. Ульяновск

Аннотация
В статье рассматриваются методики отслеживания и идентификации пользователей в сети Интернет, с акцентом на их использование в целях обеспечения безопасности, а также в маркетинговых и аналитических целях. Описаны основные способы отслеживания, такие как использование cookies, IP-адресов, цифровых отпечатков и методов аутентификации. Также рассмотрены вопросы этики и конфиденциальности, связанные с применением этих методов.

Ключевые слова: отслеживание пользователей, идентификация, сеть Интернет, cookies, цифровой отпечаток, безопасность данных, конфиденциальность.

Введение

С развитием цифровых технологий и распространением сети Интернет возникли новые вызовы в области безопасности, защиты данных и конфиденциальности пользователей. Одной из важных задач является отслеживание и идентификация пользователей, что играет ключевую роль как в обеспечении безопасности (например, предотвращение мошенничества), так и в маркетинговых исследованиях и персонализации контента.

Целью данной работы является анализ существующих методик отслеживания и идентификации пользователей в сети Интернет, а также изучение их применения в различных сферах и оценка рисков, связанных с конфиденциальностью.

Основные методы отслеживания пользователей

1. **Cookies (печеньки)**

   Cookies представляют собой небольшие текстовые файлы, которые хранятся на устройстве пользователя при посещении веб-сайта.

Они используются для сохранения информации о предпочтениях пользователей, улучшения пользовательского опыта и отслеживания поведения на сайте. Однако cookies также могут использоваться для более глубокого анализа действий пользователей и персонализации рекламы.

2. **IP-адреса**

   Каждое подключение к сети Интернет сопровождается присвоением уникального IP-адреса. Этот метод отслеживания используется для определения местоположения пользователя и анализа его активности. Тем не менее, данный метод имеет свои ограничения, так как IP-адреса могут быть динамическими или скрытыми с использованием VPN-сервисов и прокси-серверов.

3. **Цифровой отпечаток устройства**

   Цифровой отпечаток представляет собой уникальную информацию, которая собирается о характеристиках устройства пользователя, таких как тип браузера, операционная система, разрешение экрана и другие параметры. Этот метод позволяет идентифицировать пользователя без необходимости использования cookies, что делает его более эффективным в условиях блокировки cookies.

4. **Аутентификация с помощью учетных данных**

   Аутентификация пользователей с использованием паролей, одноразовых кодов и биометрии является важным методом идентификации для обеспечения безопасности. Это стандартный способ проверки подлинности пользователя и защиты данных.

Методики идентификации пользователей

1. **Использование многофакторной аутентификации (MFA)**

   Многофакторная аутентификация включает в себя несколько уровней безопасности, таких как пароль, биометрические данные (отпечатки пальцев, сканирование радужной оболочки глаза), а также одноразовые коды, отправляемые на мобильный телефон. Это повышает уровень безопасности и предотвращает несанкционированный доступ.

2. **Биометрическая идентификация**

   Технологии биометрической идентификации, такие как распознавание лиц или отпечатков пальцев, становятся все более популярными для идентификации пользователей в Интернете. Этот метод используется в различных областях, включая банковские операции, электронную коммерцию и системы безопасности.

3. **Анализ поведения пользователя (Behavioral Biometrics)**

   Анализ поведения пользователя основан на изучении его действий в сети: скорость набора текста, движении мыши, поведение при скроллинге и другие параметры. Этот метод позволяет создать уникальный профиль пользователя, который можно использовать для его дальнейшей идентификации.

Проблемы безопасности и конфиденциальности

1. **Риски утечки данных**

   Методы отслеживания и идентификации могут подвергать риску конфиденциальность пользователей, особенно если данные не защищены должным образом. Утечка персональных данных или их использование для целей, не согласованных с пользователем, может привести к значительным юридическим и репутационным последствиям.

2. **Проблемы с анонимностью**

   В условиях усиленной идентификации пользователей теряется анонимность в сети Интернет. Это вызывает опасения среди пользователей, особенно в свете растущего числа атак и шантажей. Поэтому необходимо соблюдать баланс между безопасностью и конфиденциальностью.

3. **Блокировка cookies и анти-отслеживание**

   Многие пользователи используют специальные инструменты для блокировки cookies или обхода методов отслеживания, что затрудняет точную идентификацию. В ответ на это, компании и разработчики адаптируют свои методики, используя более сложные технологии, такие как цифровой отпечаток устройства.

Заключение

Методики отслеживания и идентификации пользователей в сети Интернет играют важную роль в обеспечении безопасности и улучшении пользовательского опыта. Однако их использование должно быть сбалансировано с учетом защиты личных данных и конфиденциальности пользователей. Разработка новых методов аутентификации и отслеживания, а также усиление защиты данных, будут способствовать улучшению безопасности в сети и снижению рисков утечек информации.

Литература

1. Кузнецова, И. В. «Методы защиты данных в информационных системах». Москва: ИнфоТех, 2017.
2. Иванов, П. И. «Безопасность в сети Интернет: угрозы и методы защиты». Санкт-Петербург: Политех, 2018.
3. Смирнов, С. В. «Цифровые отпечатки и анонимность в Интернете». Екатеринбург: УралГео, 2019.