УДК 004.738.5.056(075.8)

АНТИДЕТЕКТ-БРАУЗЕР ДЛЯ МОДИФИКАЦИИ FINGERPRINTS

Телипко Д.А.

ГУО «Брестский областной лицей имени П.М. Машерова»,
г. Брест, Республика Беларусь

Научный руководитель: Белоусова Е.С. – к. т. н., доцент, доцент кафедры защиты информации

Аннотация. В работе рассмотрены методы модификации *Fingerprints* веб-клиентов с целью обеспечения конфиденциальности пользователей в сети. Проведен анализ сетевых протоколов, использующих *Fingerprints*, а также рассмотрены основные инструменты для отслеживания передачи *Fingerprints* веб-клиентами. Разработана методика модификации *Fingerprints*, которая реализована в виде программного решения, обеспечивающего конфиденциальность пользователей. Проведена проверка эффективности предложенной методики с использованием специализированных инструментов анализа *Fingerprints*.

Ключевые слова: *Fingerprints*, антидетект-браузер, веб-клиент, конфиденциальность.

Введение. Одной из основных задач, решаемых в сфере защиты информации, является обеспечение безопасности пользовательских данных в сети. Тема обеспечения конфиденциальности пользователей в виртуальном пространстве остается актуальной, учитывая постоянное развитие методов сбора и анализа персональной информации. *Fingerprint* (отпечаток браузера) – это информация, собираемая об удалённом устройстве для последующей идентификации. Например, такие атрибуты, как ОС, настройки клавиатуры, оборудование, геолокация, часовой пояс, размер дисплея, браузер, память устройства и др., могут быть использованы компаниями для отслеживания действий пользователей в сети [1].

Целью данной работы был анализ критериев конфиденциальности пользователей в сети при использовании методики модификации *Fingerprints* веб-клиента, на основе которого разработан антидетект-браузер, позволяющий изменять ключевые параметры *Fingerprints*, что подтверждено тестированием с использованием *BrowserLeaks* и *Burp Suite*.

Назначения отпечатков браузера могут быть разными: как легитимными, так и представляющими угрозу конфиденциальности пользователей. К легитимным отпечаткам можно отнести такие как персонализация контента, улучшение работоспособности и производительности, защита от ботов. Однако нарушители могут использовать отпечатки с другими целями: слежка, персональные кибератаки, спуфинг.

Основная часть. Сетевые протоколы, использующие *Fingerprints*. Принцип передачи отпечатков основан на протоколах *HTTP (HTTPS*). Так, например, браузеры отправляют заголовок *HTTP* со следующими параметрами:

1 *User-agent*, содержащий информацию о версии браузера, операционной системе и устройстве.

2 *Accept-Language* передается в *HTTP*-запросе и содержит информацию о предпочитаемых языках пользователя.

3 *Referer* указывает на *URL* предыдущей страницы, с которой был осуществлен переход на текущую. *Referer* используется для анализа путей пользователя в сети и определения источников трафика.

4 *Accept-Encoding* указывает, какие методы сжатия контента поддерживает браузер.

В *HTTP* заголовках также передаются *Cookies*, которые представляют собой небольшие фрагменты данных, хранящиеся на стороне клиента и отправляемые с каждым запросом к серверу. *Cookies* широко используются для отслеживания состояния сеанса пользователя и для хранения информации о предыдущих взаимодействиях. Однако *Cookies*

и *Fingerprints* являются двумя различными методами отслеживания пользователей в интернете, и у них есть ряд существенных отличий, описанных в таблице 1.

Таблица 1 – Сравнительный анализ *Cookies* и *Fingerprints*

Параметры	***Cookies***	***Fingerprints***
Формирование	Создаются сервером	Формируются динамически на основе множества параметров устройства и браузера
Хранение данных	На стороне клиента	Не сохраняются
Срок использования	Устанавливается сервером	Не имеют
Возможность блокировки	Вручную, расширения браузера	Расширения браузера

Важно отметить, что *IP*-адрес пользователя используется для создания *fingerprints*, основанных на определении примерного местоположения пользователя.

Множество параметров протокола *TCP/IP*, таких как *TTL* (*Time To Live*), опции *TCP* и другие, используется для создания *fingerprints*, идентифицирующих характеристики сетевого стека.

Также можно выделить *TLS fingerprints*, основанные на следующих параметрах заголовка *TLS*: протокол шифрования, версии *TLS/SSL* и поддерживаемые шифры.

Выбор инструментов и веб-клиентов для отслеживания передачи *Fingerprints*. В рамках работы были рассмотрены несколько инструментов, которые используются для изучения и передачи *fingerprints* веб-клиентам:

1 *FingerprintJS* – это доступная в исходном коде клиентская библиотека снятия отпечатков браузера, которая запрашивает атрибуты браузера и вычисляет на их основе хешированный идентификатор посетителя.

2 *GoLogin* – веб-ресурс, который позволяет проверить отображение *fingerprints*.

3 *BrowserLeaks* – набор инструментов, который позволяет провести ряд тестов для оценки безопасности и конфиденциальности веб-браузера.

Выбор веб-клиента основан на статистике 2024 года [2], которая показывает, что среди пользователей интернета в Беларуси лидировала поисковая система *Google* (более 67 %). На втором месте – поисковая система Яндекс (31,31 %). Поэтому для сравнения передачи *Fingerprints* веб-клиентами были выбраны *Google Chrome* и Яндекс Браузер.

Методика отслеживания передачи *Fingerprints* веб-клиентами. С помощью веб-ресурса FingerprintJS было установлено, что сайты могут идентифицировать текущую версию браузера путем обработки *HTTP* запросов, что изображено на рисунке 1.

С помощью веб-ресурса *GoLogin* было установлено, что с помощью *fingerprints*, используя инструмент *WebRTC*, можно узнать реальный *IP*-адрес пользователя, что представлено на рисунке 2.

С помощью веб-ресурса *BrowserLeaks* было установлено, что через *Canvas API*, предназначенный для рисования графики, можно узнать уникальную подпись *Canvas*, а с помощью *JavaScript* можно получить информацию об исходном ресурсе (*URL* источника запроса), разрешении экрана и местному времени.

Таким образом, в ходе проведенного исследования по сравнению *fingerprints* браузеров *Google Chrome* и *Yandex* было отмечено сходство в *IP*-адресах через *WebRTC* и *Canvas* идентификаторах, разрешении экрана и местном времени. Различными же в браузерах являются *user-agent*, версии браузеров, хэш данные отчетов *WebGL*.

Способы модификации *Fingerprints* в веб-клиентах. Основным способом модификации *Fingerprints* является использование антидетект-браузеров, которые позволяют подменять отпечатки пользователя.

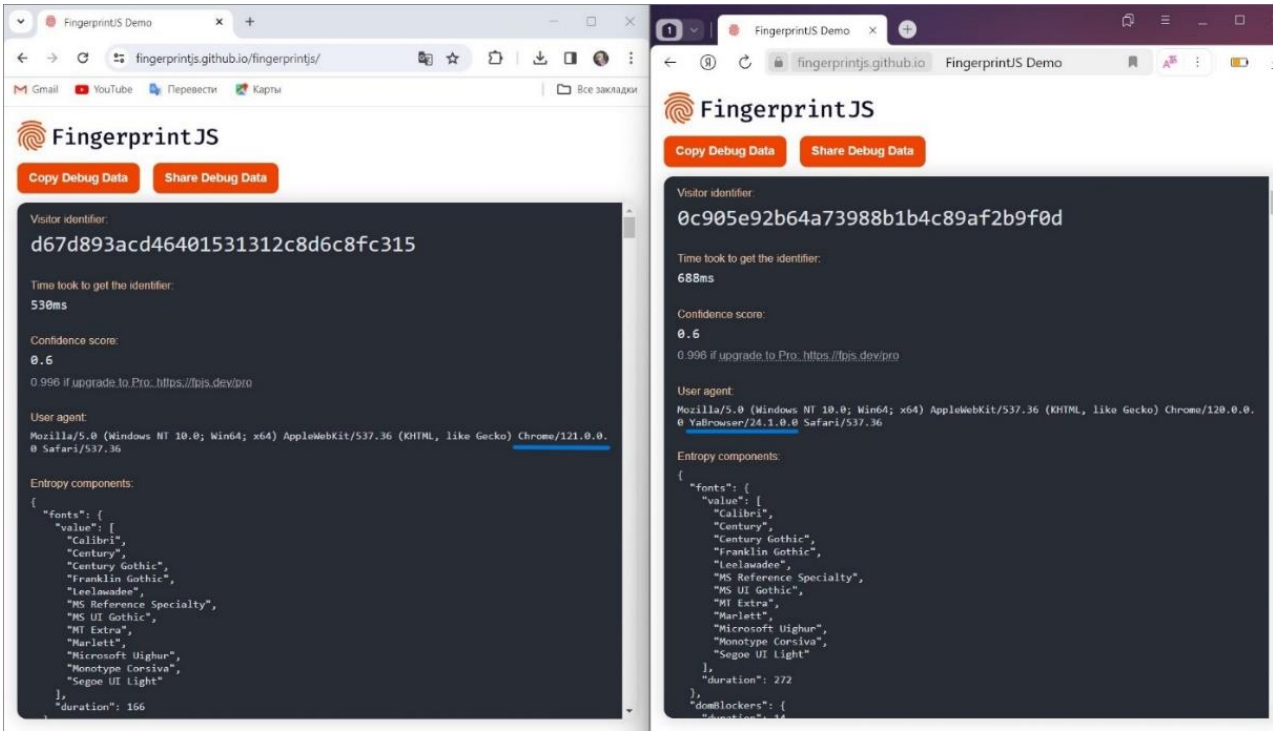

Рисунок 1 – Анализ передачи *user-agent fingerprint* с помощью веб-ресурса *fingerprintJS*

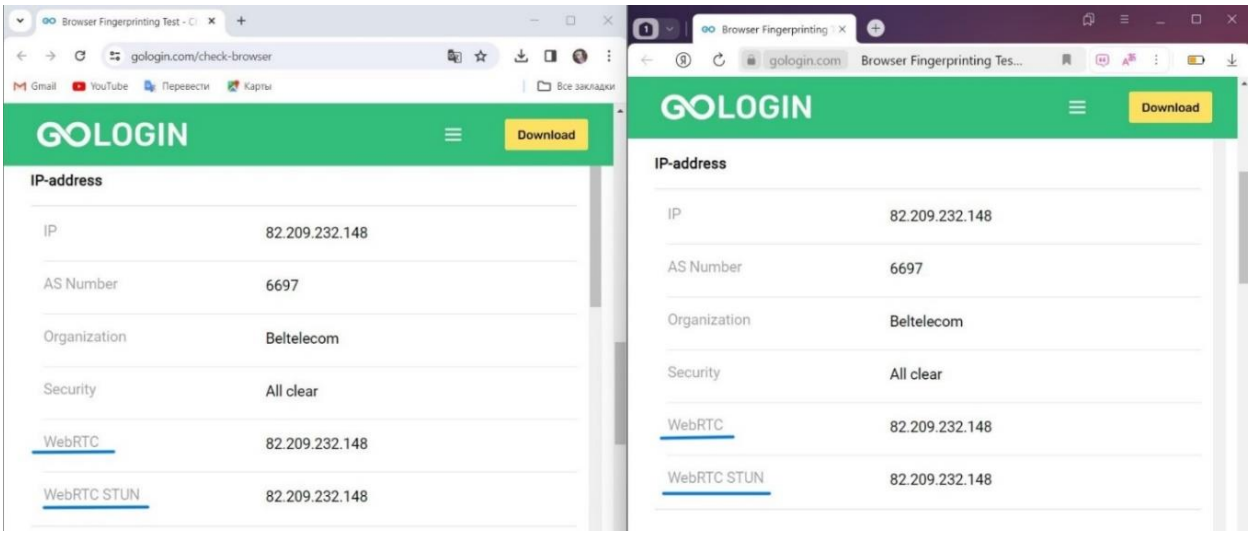

Рисунок 2 – Анализ передачи *IP*-адреса с помощью веб-ресурса *GoLogin*

На сегодняшний день на рынке представлены платные решения, такие как *Linken Sphere* и *GoLogin*, которые предоставляют расширенные возможности по обеспечению конфиденциальности пользователя. Эти антидетект-браузеры предоставляют множество инструментов, позволяющих пользователям маскировать свой цифровой след в сети. Однако, следует отметить, что использование *Linken Sphere* и *GoLogin* является платным и дорогостоящим.

С учетом этой проблемы, для обеспечения конфиденциальности пользователей посредством модификации *fingerprints*, было принято решение разработать общедоступный антидетект-браузер, который предоставляет более гибкие возможности настройки под конкретные потребности, а также является более доступным.

Антидетект-браузер для модификации *Fingerprints*. Для разработки веб-клиента был использован язык программирования Python, на котором реализован антидетект-браузер с возможность модификации следующих параметров: *WebRTC*, *WebGL*, *Canvas*, *JavaScript*, режим инкогнито, язык браузера, агент пользователя и использование прокси-сервера (рисунок 3). Функционал разработанного веб-клиента позволяет гибко настраивать браузер в соответствии с пожеланиями пользователя, а также обеспечивает автоматизацию и управление различными функциональными возможностями браузера.

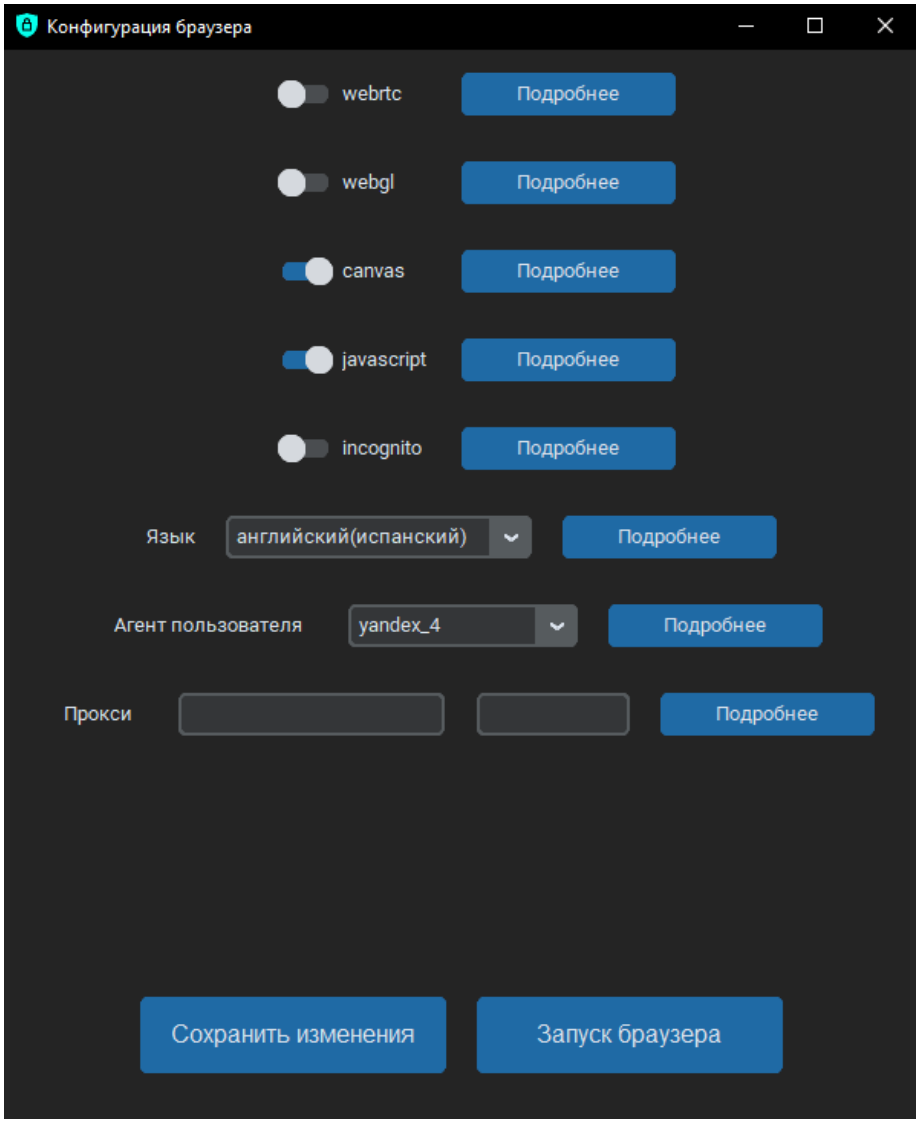

Рисунок 3 – Конфигурация браузера и модификации Fingerprints

Функциональное тестирование антидетект-браузера для модификации *Fingerprints*. Для проверки степени конфиденциальности разработанного антидетект-браузера был использован веб-ресурс *browserleaks* [3], так как он предоставляет максимально детально данные о работе тех или иных функций. На рисунке 4 представлены результаты поверки включения и отключения одной из функций разработанного антидетект-браузера. Например, на рисунке 8 видно, что после отключения *webRTC* не определяется публичный *IP*-адрес пользователя.

Также для функционального тестирования антидетект-браузера было использовано программное обеспечение *Burp Suite*. Как видно из рисунка 5, при включении функции

изменения *Fingerprints* в заголовке *HTTP* изменяются параметры *User-Agent* и *Accept-Language*, что говорит о правильности работы разработанного антидетект-браузера.

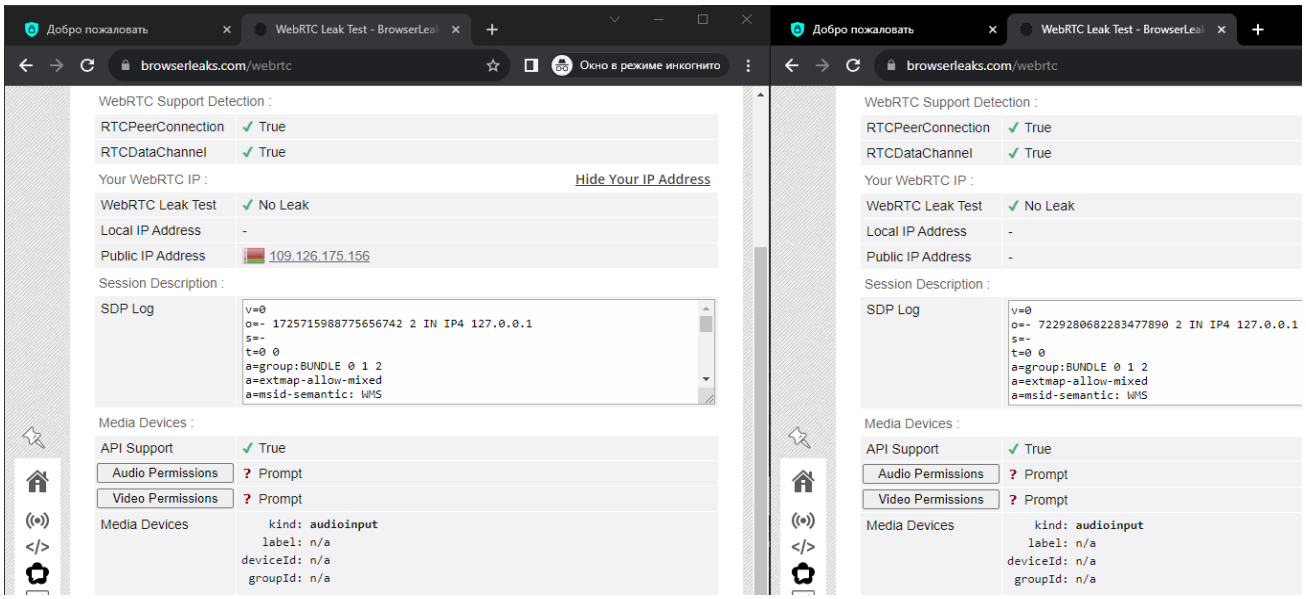

Рисунок 4 – Результат отключения webRTC в разработанном антидетект-браузере

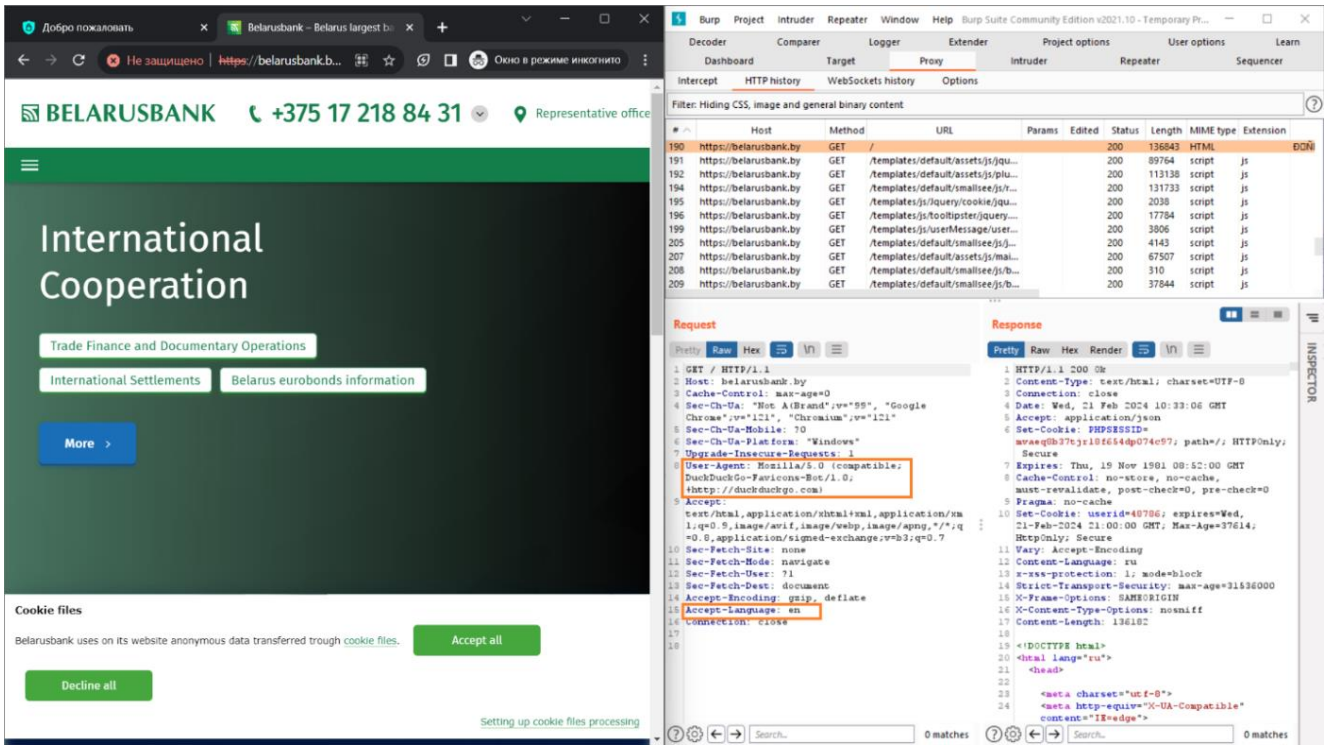

Рисунок 5 – Тестирование подключение к сайту с модифицированными User-Agent и Accept-Language Fingerprints в разработанном антидетект-браузере

Заключение. В рамках работы было доказано, что различные веб-клиенты передают *fingerprints*, посредством которых можно идентифицировать текущую версию браузера, уникальные идентификаторы, подписи, местное время, IP-адрес устройства и др. На основе обзора различных способов модификации *Fingerprints* в веб-клиентах установлено, что наиболее эффективным является использование антидетект-браузеров. Однако использования таких антидетект-браузеров, как *Linken Sphere* и *GoLogin*, является дорогостоящим. Поэтому авторами разработан собственный общедоступный антидетект-

браузер для обеспечения конфиденциальности пользователей посредством модификации *fingerprints*. На языке Python был реализован функциональный антидетект-браузер, в котором пользователь легко может настраивать параметры модификации различных *fingerprints*. Тестирование разработанного антидетект-браузера с помощью выбранных инструментов (*Burp*, *FingerprintJS*, *GoLogin*, *BrowserLeaks*) показало эффективность модификации таких *fingerprints*, как *User-Agent*, *Accept-Language*, *WebGL*, *webRTC* и др., что свидетельствует о корректной работе разработанного антидетект-браузера.

Список литературы

1. *М. А. Айд. Разработка методологии противодействия отслеживания и идентификации пользователей интернета: Национальный исследовательский Томский политехнический университет: магистерская диссертация. Томск, 2018.*

2. *Statcounter Global Stats [Электронный ресурс]. Режим доступа: https://gs.statcounter.com/. Дата доступа: 18.10.2024.*

3. *Browserleaks [Электронный ресурс]. Режим доступа: https://browserleaks.com/. Дата доступа: 18.10.2024.*

UDC 004.738.5.056(075.8)

ANTIDETECT BROWSER FOR FINGERPRINTS MODIFICATION

Telipko D.A.

State Educational Institution «Brest Regional Lyceum named after P.M. Masherov», Brest, Republic of Belarus

Belousova E.S. – Cand. of Sci., associate professor, associate professor of the informational security department

Annotation. The paper considers methods for modifying web clients' Fingerprints in order to ensure the privacy of users on the network. The analysis of network protocols using Fingerprints is carried out, as well as the main tools for tracking the transfer of Fingerprints by web clients. A Fingerprint modification technique has been developed, which is implemented as a software solution that ensures user privacy. The effectiveness of the proposed methodology was tested using specialized Fingerprints analysis tools.

Keywords: Fingerprints, Antidetect Browser, Web Client, confidentiality.