DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.6

УДК 003.26.7:004.09
ББК 32.973.202

АНАЛИЗ ТЕХНОЛОГИЙ ЗАЩИТЫ ОТ ИДЕНТИФИКАЦИИ ВЕБ-БРАУЗЕРОВ

Валерий Михайлович Московченко

Доктор экономических наук, кандидат военных наук, профессор, генерал-лейтенант,
директор военного института,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
fvo.urgpu.npi@yandex.ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Данил Олегович Столяров

Магистр кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
danil.stolyarov.1994@mail.ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Александр Андреевич Горбунов

Магистр кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
kent1157@bk. ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Владислав Игоревич Белянин

Магистр кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
vbeluev@mail.ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Аннотация. В статье рассмотрена проблема сохранения анонимности в сети. Описаны основные технологии для отслеживания действия пользователей сайтов, принцип их работы. Выделены преимущества и недостатки технологий cookies и fingerprints и методы защиты от данных технологий.

Ключевые слова: анонимность, конфиденциальность, cookies, fingerprint, веб-браузер.

© Московченко В.М., Столяров Д.О., Горбунов А.А., Белянин В.И., 2018

В век информационных технологий становится все тяжелее сохранить неприкосновенность частной жизни. И иногда анонимность в Интернете помогает защитить это право каждого человека. Также анонимность в Интернете позволяет защитить-

ся от возможных противоправных действий третьих лиц.

Существуют ряд технологий, с помощью которых можно отслеживать действия пользователей сайтов. К ним относятся такие технологии, как *cookies* и *fingerprints*.

Технолгия *cookies* – на сегодняшний день важная составляющая большинства операций в Интернете. Данная технология считается одним из главных средств, которые владельцы интернет-ресурсов используют для отслеживания клиентов их ресурса. Однако эта методика постепенно устаревает и нередко не дает требуемый эффект [2].

Этому способствуют несколько причин. В современных реалиях практически любой пользователь Интернета может деактивировать операцию получения *cookies*, либо воспользоваться встроенным в веб-браузер режимом «инкогнито» и сохранить *cookies* только на текущую сессию. Эти приемы позволяют сделать присутствие пользователя и его действия для сайта незамеченными. *Cookies* позволяют передавать данные помимо владельца сайта самим пользователям. Пользователь видит *cookies* и отправителя, поэтому имеет возможность защититься от них.

Ситуация с технологией *fingerprints* в корне отличается. Эта технология базируется на анализе информации, полученной от браузера клиента при посещении электронного ресурса. Эта информация складывает из следующих типов данных: языковые и региональные настройки, установленные системные шрифты, временные настройки, разрешение и характеристики экрана, используемые браузером плагины, цифровые версии и сертификаты программ и т. д. Благодаря этим данным создается цельная картина браузера, которая схожа по своему принципу отображения с отпечатком пальца. В результате даже при отключении или удалении *cookies* ресурс все равно опознает конкретного пользователя по его отпечатку веб-браузера.

Отпечатки, идентифицирующие браузер пользователя, заменяют собой *cookies*. Важно понимать, что выставление в браузере определенных настроек с целью защититься от чрезмерной активности сайтов по идентификации пользователей может привести к тому, что такие настройки делают их более узнаваемыми на фоне других пользователей Интернета [1].

Угроза нарушения конфиденциальности – основная причина, из-за которой пользователь должен быть внимателен. Технология *fingerprints* во многом опаснее *cookies*. От нее сложнее защититься, так как невозможно узнать о том, следят за пользователем или нет. Система помечает персональный компьютер посетителя уникальной цифровой меткой в виде хэш-суммы, снятой по особому алгоритму с настроек браузера, о присутствии которой пользователь даже не догадывается. Таким образом, создается база меток для идентификации пользователей. При следующем посещении пользователем ресурса производится сравнение отпечатка его браузера с базой меток и при совпадении происходит однозначная идентификация.

Технология *fingerprints* является глобальным идентификатором. Опечатки браузера делают его владельца более узнаваемым не только на часто посещаемых интернет-ресурсах, но и в других электронных источниках. *Fingerprints* фиксирует целостную картину, которую ресурс получает от веб-браузера. Это позволяет произвести идентификацию клиента даже при внесении изменений в настройки браузера.

Для самостоятельного определения уникальности браузера можно воспользоваться сервисом https://panopticlick.eff.org (рис. 1). Для того чтобы браузер нельзя было однозначно идентифицировать, сумма показателей *bits of identifying information* не должна превышать 20. Браузер, представленный на рисунке 1, является уникальным, и его можно легко идентифицировать, так как сумма показателей *bits of identifying information* больше 20.

Есть множество различных способов изменить отпечатки веб-браузера и свести его уникальность к минимальным показателям: модернизация браузеров, использование типовых плагинов, изменение разрешения экрана под более распространенное, удаление нестандартных шрифтов из системы и т. д.

Значительный результат обеспечения конфиденциальности достигается за счет изменения часового пояса. Пользователи выставляли некорректное время, а после посе-

щения интернет-ресурса изменяли его на корректное значение. У пользователя с максимальным отклонением от первоначального времени уникальность снижалась максимально.

На данный день гарантированно действенных методов и средств защиты от технологии *fingerprints* пока не разработано, однако есть меры, применение которых позволяет радикально снизить уникальность веб-браузера. Максимально эффективно отключение исполнения в браузере таких компонентов, как: *Flash*, *Javascript* и *WebGL*.

Однако главным недостатком этого способа защиты являются возможные проблемы при отображении некоторых сайтов. Поэтому целесообразно использовать в этом случае комбинированный метод, основанный на отключении *Flash* и *Java* при параллельном использовании специального

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.38	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	6.71	104.66	c262636d55b57e2895fd7b4473fb4c87
Screen Size and Color Depth	2.41	5.31	1920x1080x24
Browser Plugin Details	5.2	36.76	Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 2: Native Client; ; internal-nacl-plugin; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;). Plugin 3: Widevine Content Decryption Module; Enables Widevine licenses for playback of HTML audio/video content. (version: 1.4.8.1029); widevinecdmadapter.dll; (Widevine Content Decryption Module; application/x-ppapi-widevine-cdm;).
Time Zone	4.18	18.13	-180
DNT Header Enabled?	1.23	2.34	False
HTTP_ACCEPT Headers	8.66	405.75	text/html, */*; q=0.01 gzip, deflate, br ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Hash of WebGL fingerprint	7.34	162.08	3b56d0a58c040a495026ccfaa16a2a97
Language	5.78	54.86	ru
System Fonts	10.02	1038.01	Arial, Arial Black, Arial Narrow, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	1.45	2.74	Win32
User Agent	8.13	279.69	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Touch Support	0.58	1.49	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.2	1.15	Yes

Рис. 1. Результат проверки уникальности браузера

плагина типа *NoScript*. Вероятность проблем с отображением страницы становится минимальной, однако уникальность станет немного выше из-за применения данного плагина *NoScript*.

Следует отметить, что применение плагинов отдельно нежелательно. К исключениям относится только специальный продукт *Ghostery*, который защищает от *cookies* и снижает уникальность.

Еще одним простым и действенным методом защиты от *fingerprints* является усиленный контроль за выполнением сценариев в браузере. Специальные плагины для *Google Chrome* или *Mozilla Firefox* могут запрашивать у владельца персонального компьютера разрешение на отображение страницы и выполнение процессов, связанных с получением *cookies* или отправкой данных [3].

После применения вышеизложенных способов защиты от технологии *fingerprints* уникальность браузера значительно снижается (рис. 2). Сумма показателей *bits of identifying information* стала меньше 20.

Как было сказано выше, многие программы генерируют ошибки при проведении обновлений, что приводит к появлению уникальных *cookies*. Этого можно избежать только при полном отключении обновлений, однако большинство элементов системы, такие как драйверы, нуждаются в постоянных и своевременных обновлениях. Установку этих компонентов можно производить самостоятельно в ручном режиме. Это позволит избежать тех ошибок, которые повышают уникальность браузера.

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	0.38	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	3.71	48.86	b56786d55b57e6785ed7b7689gh4r56
Screen Size and Color Depth	1.01	3.2	1024x768x24
Browser Plugin Details	0	0	false
Time Zone	1.28	10.56	-40
DNT Header Enabled?	1.23	2.34	False
HTTP_ACCEPT Headers	5.1	270.67	text/html, */*; q=0.01 gzip, deflate,en-US;q=0.6,en;q=0.9
Hash of WebGL fingerprint	0	0	false
Language	1.15	16.56	en
System Fonts	3.62	320.51	Arial, Arial Black, Arial Narrow, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New,)
Platform	1.45	2.74	Win32
User Agent	2.13	279.69	Mozilla/5.0 (Windows 5.0; Win32; x32) Chrome/63.0.3239.132
Touch Support	0.58	1.49	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.2	1.15	Yes

Рис. 2. Результат проверки уникальности браузера после выполнения защитных действий от технологии *fingerprints*

Одна из множества возможностей веб-браузера *Mozilla Firefox* – защита от *cookies* с возможностью анонимной работы с электронными ресурсами. Эту защиту обеспечивает вышеназванный плагин *NoScript*. В данном случае он используется как отдельная разновидность расширения для браузера, осуществляющая блокировку исполнений *Flash*, *JavaScript*, апплетов *Java* и других элементов *HTML*-страниц. Работа плагина полностью контролируется клиентом. Пользователь включает и выключает расширение, таким образом, разрешая или запрещая выполнение конкретных сценариев.

Также и для остальных веб-браузеров существуют аналоги плагина *NoScript*, но наиболее эффективно они работают на веб-браузере *Mozilla Firefox*.

Изложенный в данной статье материал позволяет утверждать, что защита от отпечатков веб-брауезра или технологии *fingerprints* довольна трудна, а также сделать следующие выводы.

Fingerprints является уникальной технологией слежения за пользователями интернет-ресурсов, основанной на использовании данных, полученных от веб-браузера. Данная технология позволяет собирать большой объем информации, полученной из настроек веб-браузера, и персонального компьютера в целом.

Отпечаток веб-браузера, внесенный в систему идентификации, тяжело изменить. Необходимо полностью изменить настройки веб-браузера и системы. Настройки веб-браузера должны отличаться от настроек большинства веб-браузеров, так как это может привести к увеличению вероятности идентификации браузера.

Следует помнить, что любой отпечаток имеет срок годности. Если не посещать интернет-ресурс продолжительное время, узнаваемость браузера заметно снижается.

На сегодняшний день полностью защититься от технологии идентификации *fingerprints* невозможно, но есть способы минимизировать вероятность внесения отпечатка веб-браузера в базу идентификации с помощью установки плагинов и отключения сценариев, контроля обновлений. Наиболее эффективным средством защиты является применение сети *Tor*.

СПИСОК ЛИТЕРАТУРЫ

1. Гладкий, А. А. Безопасность и анонимность работы в Интернете : Как защитить компьютер от любых посягательств извне / А. А. Гладкий. – М. : Литрес, 2012. – 260 с.

2. Колисниченко, Д. Анонимность и безопасность в Интернете / Д. Колисниченко. – СПб. : БХВ-Петербург, 2014. – 392 с.

3. Уникальные отпечатки браузера – fingerprints. Ч. 1. – Электрон. дан. – Режим доступа: https://whoer.net/blog/article/unikalnye-otpechatki-brauzera-fingerprints-chast-1/. – Загл. с экрана.

REFERENCES

1. Gladkiy A.A. *Bezopasnost i anonimnost raboty v Internete. Kak zashchitit kompyuter ot lyubyh posyagatelstv izvne* [Security and Anonymity of the Internet. How to Protect Your Computer from Any External Attacks]. Moscow, Litres Publ., 2012. 260 p.

2. Kolisnichenko D. *Anonimnost i bezopasnost v Internete* [Anonymity and Security on the Internet]. Saint Petersburg, BKhV-Peterburg Publ., 2014. 392 p.

3. *Unikalnye otpechatki brauzera – fingerprints. Chast 1* [Unique Fingerprint of the Browser. Part 1]. URL: https://whoer.net/blog/article/unikalnye-otpechatki-brauzera-fingerprints-chast-1/.

THE ANALYSIS OF TECHNOLOGIES PROTECTING FROM WEB BROWSERS IDENTIFICATION

Valeriy Mikhaylovich Moskovchenko

Doctor of Sciences (Economics), Candidate of Military Sciences, Professor,
Lieutenant General, Director of Military Institute,
Platov South-Russian State Polytechnic University
fvo.urgpu.npi@yandex.ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Danil Olegovich Stolyarov

Master Student,
Department of Information Security,
Platov South-Russian State Polytechnic University
danil.stolyarov.1994@mail.ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Aleksandr Andreevich Gorbunov

Master Student,
Department of Information Security,
Platov South-Russian State Polytechnic University
kent1157@bk. ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Vladislav Igorevich Belyanin

Master Student,
Department of Information Security,
Platov South-Russian State Polytechnic University
vbeluev@mail.ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Abstract. In the age of information technology, it is becoming increasingly difficult to maintain privacy. Sometimes anonymity on the Internet helps to protect everyone's right. Anonymity on the Internet also helps to protect against possible illegal actions of third parties.

There is a number of technologies that you can use to monitor site user activity. These include technologies such as cookies and fingerprints.

Today, cookies technology is an important component of most operations on the Internet. This technology is considered to be one of the main tools that Internet resource owners use to track customers. However, this technique is gradually becoming obsolete and often does not give the desired effect.

Fingerprint technology is a global identifier. Browser typos make its owner more recognizable not only on frequently visited Internet resources, but also in other electronic sources. Fingerprints capture the holistic picture that a resource receives from a web browser. This allows you to identify the client even if you make changes to your browser settings.

This article deals with the problem of anonymity preservation in a network. The authors describe the main technologies for tracking the users' website activity, the principles of their work, and the protection methods against these technologies. The advantages and disadvantages of the cookies and fingerprint technologies have also been determined.

Key words: anonymity, confidentiality, cookies, fingerprint, web browser.