К. С. Перепечкин
Институт бизнеса БГУ, *Минск*, *Беларусь*

АКТУАЛЬНЫЕ ВОПРОСЫ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ КУКИ (COOKIES)

Статья рассматривает современный инструмент аналитики целевой аудитории «куки» (cookies). Описаны принципы их работы, хранения и назначения. Выявлены основные параметры безопасной работы с ними как с точки зрения обычного потребителя, так и владельцев сайтов.

Ключевые слова: *cookies, куки, HTTPS-протокол, безопасность, личная информация*

Куки (*cookies*) – это текстовые файлы, которые компьютер загружает в память с веб-страниц. При повторном посещении сайта, он подгружает свои cookies (далее – куки). Так сайт вспоминает пользователя и подстраивается под него: автоматически пускает в личный кабинет, собирает статистику, создает персональные рекомендации [2]. *Применяется для сохранения данных на стороне пользователя, на практике обычно используется*:

– для аутентификации пользователя (т. е. для входа на свою страницу);

– сохранения личных данных на протяжении одной сессии (имя, логин, e-mail, пароль). При отсутствии куки пользователю пришлось бы авторизоваться на сайте после каждого обновления страницы;

– хранения персональных предпочтений и настроек пользователя;

– отслеживания состояния сеанса доступа пользователя;

– сведений статистики о пользователях;

– настройки профиля (язык, геолокация, включенные функции). Если пользователь настроил содержимое страницы по личным предпочтениям, то при повторном посещении эти настройки сохранятся;

– фиксации действий пользователей (реакции, активности, просмотренные товары). Собранную информацию используют разные сервисы и интернет-магазины. Например, чтобы запомнить ответ при голосовании, собрать статистику;

– идентификации пользователей (тип используемого устройства, время посещения, количество просмотренных страниц). С помощью этих куки сайты собирают необходимые данные о поведении посетителей [1].

Файлы-куки используются в веб-браузерах на протяжении 25 лет. Когда мы совершаем на сайте какое-то действие, например, добавляем товар в корзину или вводим детали входа в аккаунт, сервер записывает эту информацию в куки и отправляет браузеру вместе со страницей. Когда мы переходим на другую страницу сайта или заходим на него через время, браузер отправляет куки обратно.

Куки бывают временными и постоянными. *Постоянные* куки остаются на компьютере, когда мы закрываем вкладку с сайтом, а *временные* удаляются. Какие именно куки использовать на конкретном сайте – временные или постоянные – решает его разработчик. Именно поэтому на одних сайтах мы не выходим из аккаунтов, даже когда заходим на них раз спустя несколько дней, а на других вводим пароль заново, хотя отошли от компьютера на пять минут.

Разработчик решает, какие куки использовать в зависимости от типа сайта, который разрабатывает. Например, если это какая-то банковская система, то куки необходимо обновлять и удалять при малейших подозрениях, что пользователь может отойти от своего устройства или кто-то другой пытается выдать себя за этого пользователя. А если это сайт, где у нас, например, хранится мало нашей личной или важной информации, то разработчик может использовать минимальную

безопасность куки. И если злоумышленник перехватит доступ к сайту, то ничего страшного он не сможет сделать.

Безопасность куки. Сами по себе куки не опасны – это обычные текстовые файлы. Они не могут запускать процессы на компьютере и вообще взаимодействовать с операционной системой. Но их могут попытаться перехватить или украсть, чтобы отследить ваши предыдущие действия в сети или входить в ваши аккаунты без авторизации.

Обычно информацию, которую записывают в куки, зашифровывают перед отправкой, а сами куки передают по HTTPS-протоколу. Это помогает защитить пользовательские данные, но за внедрение шифрования и безопасную отправку отвечает разработчик сайта. Посетителям остается только надеяться, что все настроили грамотно. Со своей стороны, пользователь может только запретить браузеру использовать куки или время от времени чистить их самостоятельно [4].

Совсем отключать куки – не всегда хорошая идея. Например, все интернет-магазины работают с помощью куки. Если запретить браузеру их использовать, сервер не сможет запомнить, что именно вы добавили в корзину. Чистить куки вручную практичнее, но придется каждый раз заново настраивать внешний вид сайта и входить в аккаунты.

Автором разрабатывался личный сайт, и в куки пользователей было добавлено три компонента: имя, фамилия и id. Id у каждого пользователя разное, поэтому одинаковых пользователей просто не может быть. Пример. *Имя: Кирилл*, *Фамилия: Перепечкин*, *Id: 1345.* Эти данные шифруются, и выдается, например, такой куки: (vk1.a.fn9KfD9VpsLeYoIQRCPdV0_AaJgoHYswGTm0EvnJrMnW7wX4gESleOfLNP7xrDVWrjA5430uKItodOCRMbRsKIpnqxaC9Jb_5kC7Nz7_Hc0sXvRpYRucZaFb10UlA4If0hqVZtQIKnZuL0EId9MCA1dTI3JEH02WFJqrw8XpIhvxU59). С помощью этой строки текста браузер может понимать, кто перед ним. Сайт видит имя, фамилию и Id. Это и есть персональные данные пользователя, которые используются.

Пример. Пользователь сделал запрос в браузере, получил ответ и посетил сайт. Но при этом куки-файлы не использовались. Когда пользователь сделает другой запрос и посетит этот же сайт повторно, он будет идентифицирован как новый посетитель. Если сохранить куки-запись о первом посещении, то сайт зафиксирует повторное посещение конкретного пользователя или продолжение сеанса [5].

Многие пользователи переживают, что, принимая куки, они раскрывают доступ к личной информации хакерам. Риски действительно существуют при определенных условиях. Например, если человек использует публичный Wi-Fi, незащищенные или уже взломанные устройства. Необходимо понимать, что, если хакер будет перехватывать доступ к посещению сайты от имени другого человека, то он будет стремиться перехватить аккаунт администратора, потому что у него могут быть более ценные данные и большие возможности.

Как сайтам использовать куки и не нарушать закон? Фраза «Мы используем куки» означает, что сайт собирает информацию о посетителях, отслеживает их действия и сохраняет некоторые сведения.

Куки – это в большинстве своем персональные данные. Потому сайты обязаны запрашивать у пользователей согласие на использование куки. На территории Евросоюза этого требует GDPR, в России – ФЗ «О персональных данных» [3]. От пользователя требуется разрешение на использование куки.

В российском законодательстве персональные данные определяют как «любую информацию, прямо или косвенно относящуюся к определяемому лицу». То есть конкретно о куки ничего не сказано, но по факту они считаются персональной информацией (так как они хранят какие-либо данные пользователя, его имя или другие данные). Если докажут, что сайт без спроса обрабатывал данные посетителей, то владельцу ресурса грозит крупный штраф или даже блокировка. Например, в 2016 г. LinkedIn заблокировали именно за несогласованное использование данных пользователей.

Для соблюдения законодательных требований на сайте, использующем куки, необходимо опубликовать «Политику конфиденциальности», или в европейском варианте – «Соглашение о приватности» (privacy agreement). *В этом документе должна быть указана информация о том*:

– какие пользовательские данные собирает сайт;

– как эти данные будут храниться и применяться;

– каковы цели обработки собранной информации;

– в каких ситуациях данные передают третьим лицам;

– как можно изменить или удалить свои данные.

В «Политике конфиденциальности» Ozon отмечен факт сбора куки и указаны цели их использования [6].

При использовании куки можно отдельно опубликовать «Политику Cookies». В ней указывают, какие именно куки используются и для чего. Политика Cookies в Unilever: Unilever подробно объясняют процесс сбора и использования куки.

Все документы об обработке данных должны находиться в открытом доступе и на них нужно ссылаться, запрашивая согласие пользователя на использование данных [6].

Для того чтобы не нарушать закон, сайт, который использует файлы-куки, должен предупреждать об этом пользователей. Уведомление об использовании файлов-куки: «Этот веб-сайт использует файлы-куки, аналогичные технологии, чтобы отличать вас от других пользователей. Использование файлов-куки помогает обеспечивать лучший пользовательский опыт и постоянно улучшать сайт, понимая, как клиенты его используют. Пожалуйста, внимательно прочитайте это Уведомление об использовании файлов-куки и убедитесь, что вы его понимаете. Вы принимаете наше Уведомление об использовании файлов-куки, если вы продолжаете использовать этот веб-сайт или нажимаете кнопку «Принять cookie» на специальном баннере, расположенном в верхней части страницы. Если вы не согласны с данным Уведомлением об использовании файлов-куки, немедленно прекратите использование этого веб-сайта» [6].

Вывод. Безопасность для обычных пользователей, которые посещают различные сайты, большая. Если пользователь посещает различные сайты банков, то в этой ситуации необходимо быть более внимательным, стараться не оставлять свой компьютер включенным. Для компаний, у которых есть собственные сайты, очень важной составляющей является предупреждение об использовании файлов-куки. Если сайт не предупреждает пользователя о том, что он использует персональные данные пользователя, то такой сайт могут заблокировать, а компания получит штраф. Файлы-куки не опасны, однако всегда необходимо быть внимательным при посещении различных веб-источников.

Список использованных источников

1. Как выглядят cookies и зачем они нужны [Электронный ресурс]. – Режим доступа: https://www.unisender.com/ru/glossary/chto-takoe-cookies. – Дата доступа: 01.10.2022.
2. Cookie [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Cookie. – Дата доступа: 02.10.2022.
3. Чем опасны cookies [Электронный ресурс]. – Режим доступа: https://tproger.ru/articles/chem-opasny-cookies-rasskazyvajut-jeksperty/. – Дата доступа: 04.10.2022.
4. Предупреждение об использовании файлов cookie на сайте Евразийского банка развития [Электронный ресурс]. – Режим доступа: https://eabr.org/about/cookies-info/. – Дата доступа: 06.10.2022.
5. Cookies [Электронный ресурс]. – Режим доступа: https://www.calltouch.ru/blog/glossary/cookies/. – Дата доступа: 08.10.2022.
6. Что такое cookie файлы: зачем они нужны и как их удалить [Электронный ресурс]. – Режим доступа: https://kokoc.com/terminy/cookie/. – Дата доступа: 08.10.2022.