Глава 7

В интернете правда никто не знает, что ты собака?

В этой главе мы обсудим тему анонимности в интернете. Это важная тема: анонимность часто равна безопасности, но корпорации и госорганы борются с ней, чтобы эффективнее учитывать пользователей (и их интересы). В большинстве случаев это происходит по обоюдному согласию: люди жертвуют анонимностью ради удобства. Уровень анонимности может быть разным в зависимости от ситуации; грамотный пользователь должен знать о технических средствах ее защиты и понимать, когда их следует применять, а когда нет.

На рисунке Питера Штейнера, опубликованном 5 июля 1993 года в The New Yorker, изображены две собаки, и та, что сидит за компьютером, говорит: «В интернете никто не знает, что ты собака».

Эта фраза, ставшая впоследствии крылатой, абсолютно точно отражала состояние анонимности в Сети в начале 90-х: действительно, каждая собака (если она была достаточно грамотна, чтобы работать на компьютере) могла зайти в интернет и свободно высказывать свое мнение по любому вопросу, вступать в дискуссии на любые темы, публиковать что угодно — и не раскрывать о себе никакой информации, кроме прозвища (nickname). То есть назваться президентом Соединенных Штатов мог кто угодно, и ему бы за это ничего не было. Впрочем, в то время не существовало и понятия «официальный аккаунт» — назваться-то президентом собака могла, но этому бы никто не поверил. В итоге была полная сетевая вольница.

"Remember when, on the Internet, nobody knew who you were?"

В наши дни эта поговорка утратила актуальность: анонимности в интернете больше нет. Поэтому вполне естественным стало появление 23 февраля 2015 года на страницах того же The New Yorker рисунка Каамрана Хафиза, на котором одна собака спрашивает другую (обе отчетливо напоминают псов с рисунка Штейнера): «А помнишь, когда в интернете никто не знал, кто ты?»

Вот так два рисунка, разделенные 22-мя годами, наглядно демонстрируют эволюцию анонимности в глобальной сети. Как видите, все изменилось.

> *Собак больше не пускают в интернет. Знаете, почему? У них нет удостоверения личности, телефонного номера и банковского счета. А чтобы пользоваться большинством сервисов, теперь нужно сначала подтвердить свою личность.*

По большому счету, существуют две причины такой трансформации. Во-первых, интернет превратился в огромную базарную площадь, где каждый что-то покупает и продает. И, как на всяком базаре, в Сети появились жулики и мошенники — как со стороны продавцов, так и со стороны покупателей. Но если все анонимы и никто никого не знает, то как найти обманщика, чтобы призвать к ответу? Такое положение вещей мешало развитию рынка, поэтому от анонимности стали отказываться в пользу прозрачности и репутации, ведь безупречная репутация — главное условие успеха в торговле.

Второй причиной стало то, что в интернет пришла политика — в самом широком смысле. Сначала появились новостные сайты, потом блоги, следом за ними социальные сети — и вдруг оказалось, что техническая система, созданная некогда учеными для собственных целей, формирует общественное мнение сильнее, чем телевизор. Плюс к тому Сеть превратилась в среду коммуникации всех со всеми, что способствовало созданию сообществ самой разной направленности — от клубов любителей котиков до тоталитарных сект и террористических организаций. Естественно, что правительства всполошились и стали закручивать гайки. Котики их не пугали, чего никак нельзя было сказать о терроризме и манипуляции общественным мнением (и, более того, общественным сознанием) с помощью фейков. Анонимность означала безнаказанность, а это власти предержащие никак не устраивало.

Сегодня опубликовать что-либо в интернете — все равно, что написать это на заборе и приложить свои паспортные данные.

Сегодня опубликовать что-либо в интернете — все равно, что написать это на заборе и приложить свои паспортные

данные. Анонимности больше нет. Строго говоря, ее никогда и не было: технически всегда существовала возможность проследить действия пользователя и установить его личность, как бы он ни пытался замести следы. (Оговоримся: речь идет об обычных пользователях.) Но до относительно недавнего времени киберполицейским и спецслужбам не хватало опыта в таких делах и законодательных рычагов для влияния на провайдеров интернет-сервисов.

Важная вещь, которую следует запомнить: интернет — это публичное пространство, и не существует абсолютно надежных способов сделать что-либо в Сети анонимно. Любая анонимность временна. Поэтому нужно вести себя так, чтобы быть готовым ответить за каждое высказывание и за каждое действие.

«Слепите мне маску от доносчивых глаз...»[1]

В реальном мире для анонимности издавна использовались маски. Их надевали для тайных встреч влюбленные, под ними скрывались знатные особы, когда не хотели привлекать к себе внимание. Не меньше любили маски и преступники, стремившиеся остаться неузнанными и избежать правосудия.

Наиболее известны в широких кругах венецианские маски: у нас они прочно ассоциируются с карнавалом, однако в Венеции было принято носить их и в повседневной жизни — город-то был небольшой, и практически все друг друга знали. Невозможно было выйти

1 *Егор Летов, строка из песни «Слепите мне маску».*

из дому, чтобы не встретить кого-то из знакомых, — какая уж тут тайна частной жизни! Поэтому маски пришлись венецианцам настолько по вкусу, что в XVII веке их стали надевать везде и всюду, причем поступали так не только знатные особы, но и простолюдины. Обычай этот весьма удивил стольника Петра Толстого, посланного царем Петром Первым в заграничное учение в Италию в 1697 году:

> *«И приходит в оперы множество людей в машкарах, по-словенски в харях, чтоб никто никого не познавал, кто в тех операх бывает, для того что многие ходят з женами, также и приезжие иноземцы ходят з девицами; и для того надевают мущины и женщины машкары и платья странное, чтоб друг друга не познавали. Так и все время каранавала ходят все в машкарах: мущины, и жены, и девицы; и гуляют все невозбранно, кто где хочет; и никто никого не знает»*[1].

Властям республики повальное увлечение горожан анонимностью не понравилось. Были введены специальные законы: например, в маске нельзя было заходить в церковь и даже приближаться к ней; запрещено было ношение масок в казино, а также в ряде других случаев. В итоге маски остались разрешены только во время карнавала, и обычай этот сохранился до наших дней.

Сегодня маски раздражают правоохранителей ничуть не меньше, поэтому во многих странах запрещено скрывать лицо во время массовых мероприятий. Такие законы действуют в Канаде, Австрии, Дании, Германии, Испании, Швеции, Франции, Украине, в пятнадцати штатах США и в некоторых кантонах Швейцарии.

---

1 *Толстой Петр Андреевич. Путешествие стольника П. А. Толстого по Европе (1697-1699) // Библиотека Максима Мошкова Lib.ru/Классика.*

Закон Российской Федерации «О митингах»[1] также запрещает участникам митингов скрывать свое лицо, в том числе использовать маски, средства маскировки, иные предметы, специально предназначенные для затруднения установления личности.

Организатор митинга должен требовать от участников не скрывать свои лица. Лица, не подчинившиеся законным требованиям организатора публичного мероприятия, могут быть удалены с места проведения данного публичного мероприятия.

В общем, наивно было бы полагать, что правительства, столь нетерпимые к обычным маскам, спокойно отнесутся к анонимности в интернете. Разумеется, власти пойдут на любые шаги, чтобы исправить свое первоначальное упущение и добиться тотальной идентификации пользователей компьютерных сетей, что мы сейчас повсеместно и наблюдаем. Однако техническая сторона этого вопроса гораздо сложнее, и одними запретами тут не обойтись.

Власти пойдут на любые шаги, чтобы добиться тотальной идентификации пользователей компьютерных сетей.

С одной стороны, нельзя не признать, что анонимность мешает государственным органам выполнять свои прямые обязанности, то есть обеспечивать нашу с вами безопасность и ловить преступников. С другой — средства обеспечения анонимности помогают реализовать законное право граждан на тайну личной жизни и частной переписки, закрепленное в Конституции Российской

1 *Федеральный закон «О собраниях, митингах, демонстрациях, шествиях и пикетированиях» № 54-ФЗ от 19 июня 2004 года.*

Федерации (и других стран). Соблюсти в такой ситуации баланс интересов довольно трудно, поэтому каждое изменение границ анонимности вызывает в обществе горячие дебаты.

Зачем нам анонимность в интернете

Затем же, зачем она была нужна венецианцам в их маленьком городе. Интернет стал большой деревней, где все на виду. И вполне естественно, что людям не хочется выставлять напоказ всю свою жизнь, все свои маленькие слабости, привычки, интересы, друзей, врагов, покупки, перемещения, состояние здоровья и все прочее. Кому какое дело, что за фильмы я смотрю, и какая пицца мне нравится? Если мне захочется, я сам об этом расскажу.

Сегодня мы опасаемся излишнего внимания не со стороны Большого Брата, а со стороны Большого Продавца.

Но нет! Мир сегодня устроен иначе. Сегодня мы больше опасаемся излишнего внимания к себе не со стороны Большого Брата (то есть спецслужб), а со стороны Большого Продавца — всех этих бесчисленных «корпораций добра»[1] — Google, Apple, Amazon, Microsoft и других гигантов ИТ-индустрии, которые очень любят собирать данные о своих пользователях и не раз на этом попадались. Из российских компаний в этом ключе стоит упомянуть «Яндекс» со всеми

1 *Фраза «Don't be evil» (рус. — «Не будь злом») уже давно известна как неофициальный девиз Google, благодаря которому компанию называют «Корпорацией добра». Впервые упоминание этого выражения появилось в 2000 году в корпоративном кодексе сотрудников Google. Спустя 18 лет, как заметило издание Gizmodo, фразу незаметно удалили.*

его многочисленными сервисами и Mail.ru, которой принадлежат популярные соцсети «ВКонтакте» и «Одноклассники».

Зачем они шпионят за нами? Ответ прост: чтобы больше продавать нам. Сбором пользовательских данных занимаются сегодня все интернет-компании от мала до велика, ведь «люди — это новая нефть». Конечно, они хотят сделать нашу работу в интернете удобнее и приятнее, они рекомендуют нам фильмы и книги, отели и экскурсии, кредиты и страховки — и все на основе наших же «предпочтений». То есть на основе нашего цифрового следа, — той информации, которую мы вольно или невольно оставляем, пользуясь различными сервисами.

> *Мегакорпорации типа Google обладают сегодня фантастическими ресурсами и могут консолидировать информацию о человеке, собранную из различных источников.*

Чтобы «засветиться», нам даже необязательно называть свое имя и показывать фотографию — достаточно входить в интернет со своего телефона или компьютера. С телефоном все просто — его номер указывает на вас однозначно. С компьютером, в принципе, тоже: открыли один раз свою почту или зашли в соцсеть — и это устройство будет привязано к вашему профайлу.

Так что забавная история, которая гуляет по Сети, и которую я привел ниже, на самом деле отнюдь не выглядит фантастической. Можно только добавить, что отвечать вам будет не сотрудник «Корпорации добра», а голосовой ассистент — искусственный интеллект, знающий о вас абсолютно все.

— Пиццерия Google, добрый день, слушаю вас!
— Пиццерия чего?

— Пиццерия Google. Что будете заказывать?
— Но... Разве это не пиццерия «Синьор Помидор»?
— Да, была, но Google ее купил, и теперь объем наших услуг стал полным.
— Прекрасно. Примете заказ?
— Естественно! Хотите повторить ваш обычный заказ?
— Обычный заказ? Откуда вы знаете, какой?
— У нас установлен идентификатор заказчиков, и мы знаем, что последние 53 раза с этого номера заказывали пиццу «Везувий», с двойным сыром и ветчиной, плюс бутылка хорошо охлажденного пива «Лагер».
— Надо же, я и не думал... Хорошо, давайте.
— Простите, могу вам дать совет?
— Конечно.
— У вас есть наше полное меню?
— Нет.
— Это самое полное меню, и я хотела бы посоветовать вам пиццу с творогом и зеленью, и бутылку минеральной воды с малым содержанием солей.
— Творог? Зелень? Соли? Вы с ума сошли? Я все это ненавижу!
— Понимаю, но это только на пользу вашему здоровью. Кроме того, у вас очень высокий холестерин...
— Откуда вы это знаете?
— Наша фирма располагает самой большой базой данных на нашей планете. Через номер телефона мы знаем ваше имя, и поэтому имеем доступ к вашим анализам в поликлинике.
— Плевать на вашу базу данных! Я не хочу пиццу с творогом и зеленью! Я принимаю медикаменты, и поэтому могу есть все, что мне вздумается, понятно?
— Сожалею, но вы не принимали таблетки в последнее время.
— Откуда вы знаете? Шпионите за мной каждый день?

— Нет, нет! Просто мы располагаем базой данных всех аптек в городе, и последний раз вы там были 3 месяца тому назад. А в одной упаковке только 30 таблеток.
— Это правда. И откуда вам это известно?
— Из вашей кредитки...
— Чего?
— Да, вы, когда платите в своей аптеке картой своего банка, получаете скидку. В нашей базе данных все ваши расходы по карте. И за последние три месяца вы там ничего не покупали, но покупали в других магазинах, что означает, что вы карту не потеряли.
— А что, я не могу заплатить наличными? А? Что? Что теперь скажете?
— Это невозможно. Вы платите наличными только 100 долларов в неделю своей служанке, все остальное платите только кредиткой.
— Откуда вам известно, сколько я плачу служанке?
— Но она же платит соцстрах...
— Да пошли вы!
— Как хотите. Сожалею, но вся эта информация у меня на экране, и я хочу только помочь вам. Думаю, что вы должны зайти к своему врачу и взять анализы, которые вы сделали в прошлом месяце, чтобы уточнить дозировку медикаментов.
— Вы мне все осточертели — и ты, и компьютеры, и базы данных, и интернет, и Google, и Facebook, и отсутствие личной жизни в XXI веке, и это проклятое государство...*
— Пожалуйста, не расстраивайтесь. Это не в ваших интересах...
— Заткнись! Завтра же уеду куда-нибудь дальше от всего этого дерьма. Поеду на острова Фиджи, или куда угодно, где

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

нет интернета, компьютеров, телефона, ни людей, которые будут за мной все время подглядывать...
— Я вас понимаю...
— В последний раз воспользуюсь кредиткой, чтобы купить билет на самолет и улететь на край света!
— Прекрасно...
— Снимите заказ на пиццу. Я ее не хочу.
— Хорошо, уже снят. Если вы позволите... одна маленькая деталь...
— ЧТО ЕЩЕ!?
— Хочу только напомнить, что ваш паспорт просрочен...

Ну, а что такого? Ведь они следят за нами для нашего же блага. А то купил бы человек билет на самолет, а улететь бы не смог. Все так, но кому-то такая забота может показаться чрезмерной. К тому же рекомендации, которые дает искусственный интеллект, запросто могут оказаться ошибочными. Когда это касается выбора пиццы, в том нет большой беды, а вот насчет здоровья совсем другое дело — тут ошибка ИИ может стоить кому-то жизни. Или банк откажет студенту в кредите на обучение, сочтя его IQ слишком низким на основе анализа просмотренного им контента, — а он-то всего лишь дал побаловаться телефоном младшему брату. Иными словами, вся эта система рекомендаций и целевой рекламы, якобы максимально точно отражающей потребности человека, все еще очень несовершенна и при этом очень назойлива, поэтому желание от нее скрыться вполне понятно.

Система рекомендаций и целевой рекламы, якобы точно отражающая потребности человека, все еще очень несовершенна.

На самом деле, мы хотим не так уж и много: анонимного серфинга и анонимных публикаций. То есть чтобы никто не подглядывал,

на какие сайты мы ходим и что там смотрим, и чтобы можно было высказать любое мнение или выложить фотографии, не подписывая их своим именем, — анонимно. Заметьте: это не означает автоматически возможности публиковать преступные или запрещенные материалы — модератор сайта или провайдер их должен удалить, а ваш аккаунт заблокировать.

Псевдоним — это почти как аноним, но не совсем

Кроме анонимности, есть такое понятие как псевдонимность. Оно обозначает действия от лица вымышленного персонажа, чье имя обычно напрямую не связанно с настоящей личностью человека.

Очень любят псевдонимы деятели искусства — писатели, художники, актеры, музыканты. У Чехова было более 50 псевдонимов — вот уж он бы разошелся в наше время! Создал бы полсотни разных профайлов и постил бы там свои рассказы. Псевдонимы заводят по разным причинам: например, когда собственное имя не слишком благозвучно — была Норма Джин Бейкер, а стала Мэрилин Монро. Или когда уважаемый в своей профессии человек вдруг решает написать детективный роман, — так мы сначала познакомились с писателем Борисом Акуниным и только потом узнали, что есть известный ученый-японист и переводчик Григорий Чхартишвили, и что это один и тот же человек.

Если ваша цель — отделить часть интернет-активности от обычной сетевой жизни, то псевдонимность — вполне приемлемый вариант.

Короче говоря, если ваша цель состоит в том, чтобы отделить некоторую часть вашей интернет-активности от вашей же обычной сетевой жизни, то псевдонимность — вполне приемлемый вариант. Создаете несколько аккаунтов на разные случаи — и готово. Например, захотели попробовать себя в поэзии, но побаиваетесь критики друзей, да и вообще у вас серьезная работа, — псевдоним как раз то, что нужно. Или любите погонять танчики в свободное время — тоже лучше под псевдонимом. Главное — не запутаться самому в своих виртуальных личностях.

Профессор физики Ричард Фейнман очень любил играть на барабанах и достиг в этом деле такого мастерства, что его стали приглашать поиграть настоящие музыканты. Однажды их игру услышала жена одного из преподавателей Калтеха[1] *— она была хореографом и ей захотелось поставить балет, где в качестве музыкального сопровождения использовались бы ударные инструменты. Фейнман согласился сотрудничать, но настоял на том, чтобы никому не стало известно, что он — профессор физики, лауреат Нобелевской премии и тому подобное. Он хотел, чтобы зрители пришли посмотреть балет и послушать музыку, а не поглазеть на мировую знаменитость, играющую на барабанах.*

Балет имел успех. Хотя аудитория была не слишком большой, зрителям, которые пришли посмотреть представление, оно очень понравилось. Позже музыку

1 *Калифорнийский технологический институт (англ. California Institute of Technology; часто сокращается до Caltech) — частный исследовательский университет, расположенный в городе Пасадина в штате Калифорния, один из ведущих университетов в США и один из двух самых важных, наряду с Массачусетским технологическим институтом.*

записали на кассету, хореограф переехала на Восточное побережье и поставила там свой «Карибский балет» — так назывался ее спектакль на музыку Фейнмана. А потом он узнал, что она выдвинула балет на конкурс, собравший хореографов со всех Соединенных Штатов, и заняла призовое место[1].

Только не надо строить иллюзий, что стоит назваться другим именем — и вас никто не найдет. Возможно, обычному пользователю соцсети или форума, чувства которого вы ранили ехидным комментарием, найти вас окажется не по силам, и все его угрозы «вычислить вас по IP и ноги переломать» останутся пустыми словами. Но не пытайтесь играть в прятки с настоящим Большим Братом — с правоохранительными органами и спецслужбами, а также с мафией. Вас действительно вычислят, встретят возле дома и предложат поговорить так, что не будет возможности отказаться.

Да и для компаний типа Google раскрыть подобный уровень конспирации — детская задача. Зашли с одного компьютера в два аккаунта? OK, вот вы и попались. Использовали один телефон для регистрации? Пополнили базу сведений о себе. Для начинающего поэта беды в этом никакой нет — пишите себе под псевдонимом. В случае успеха ваш псевдоним может оказаться известнее и популярнее, чем ваше настоящее имя. А нет — так и не страшно.

Но если у вас есть причины для более тщательной маскировки в Сети, то стоит подумать о более продвинутых методах анонимизации.

---

1 *Из книги «Вы, конечно, шутите, мистер Фейнман».*

Применительно к интернету под анонимностью понимают техническую невозможность связать действия, выполняемые на интернет-ресурсах, с человеком, выполняющим эти действия.

IP-адрес вашего компьютера или телефона как раз и выполняет роль этого связующего звена между вами и вашим устройством — его вам выдает интернет-провайдер или оператор связи, с которым у вас есть договор.

Вычислить по IP — что это значит?

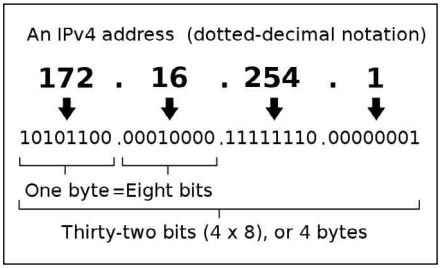
Что же такое этот IP-адрес, знание которого так важно для определения личности пользователя?

IP — это сокращение от Internet Protocol, дословно означающее «межсетевой протокол». Его придумали в середине 1970-х годов отцы-основатели интернета Винт Серф (Vint Cerf) и Боб Кан (Bob Kahn), когда решали задачу, как обеспечить передачу информации в Сети в условиях нестабильной работы каналов связи и отдельных узлов.

Есть легенда, что это делалось на случай ядерной войны, чтобы сохранить управление войсками, если какие-то из командных центров попадут под удар. На самом деле все гораздо прозаичнее: в то время для связи использовались обычные телефонные линии, имевшие свойство разрывать соединение в самый неподходящий момент. Люди в такой ситуации просто перезванивают, спрашивают друг друга, на чем оборвался разговор, и продолжают дальше, а компьютеры этому надо было научить.

IP-протокол вместе со своим «братом», протоколом TCP, позволяют компьютерам восстановить соединение и продолжить передачу данных с момента, когда связь нарушилась. IP-адрес — это аналог телефонного номера, он должен быть у каждого устройства, подключенного к Сети.

IP-адрес состоит из четырех чисел в диапазоне от 0 до 255 и выглядит так:



Максимальное число адресов в Сети — 4 294 967 296, всего четыре с небольшим миллиарда, причем некоторые серии адресов зарезервированы для разных технических нужд и не используются, так что реально доступное число адресов еще меньше.

Значит, у интернета тоже есть номерная емкость, и она может исчерпаться? Да, именно так и произошло. К настоящему времени свободные IP-адреса закончились, а нужно подключить еще пару миллиардов новых пользователей и десятки миллиардов всяких датчиков и умных устройств, поэтому все интернет-провайдеры постепенно переходят на новую версию IP-протокола — IPv6, где адресов хватит на всех. Похоже на то, как было в Москве, когда к семизначным городским номерам пришлось добавить код 495 или 499.

Как и телефонные номера, IP-адреса выдают блоками: сначала региональным интернет-регистраторам, которых всего пять: Америка, Европа (включая Ближний Восток), Азиатско-Тихоокеанский регион, Латинская Америка и Африка. Те, в свою очередь, делят свою квоту между странами, входящими в их регион; дальше блоки распределяются по провайдерам, которые и раздают их конкретным пользователям, но далеко не всем, а только тем, кто попросил выделить статический (то есть постоянный) адрес. Большинству же обычных пользователей дается динамический адрес из числа свободных в настоящий момент.

Статический адрес может вам понадобиться в случае, если вы решили завести собственный веб-сайт — чтобы посетители знали, куда приходить. Для того, чтобы гулять по интернету, хватит и динамического. Да, он будет каждый раз разный, и узнать, кто под ним «сидит», не получится — если только не попросить провайдера показать свои записи, где зафиксировано, когда и какому клиенту данный IP-адрес был выдан. Такая информация может быть получена только по запросу правоохранительных органов, человеку с улицы провайдер ничего не скажет.

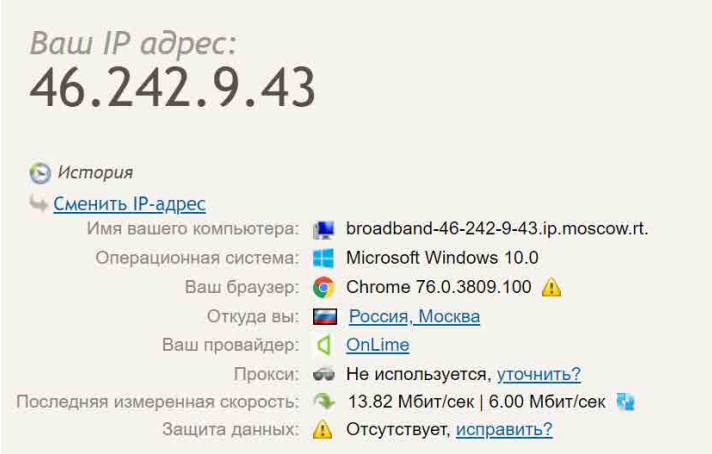
Важно: если вы хотите найти злоумышленника или хулигана по IP-адресу, обязательно фиксируйте время, в которое он предположительно выходил в интернет. Адрес-то у него, скорее всего, динамический.

А потом предстоит доказывать, что с этого устройства совершил противоправные действия именно тот человек, который официально числится его владельцем; что он его не потерял, не оставил без присмотра в общественном месте, где к нему мог иметь доступ

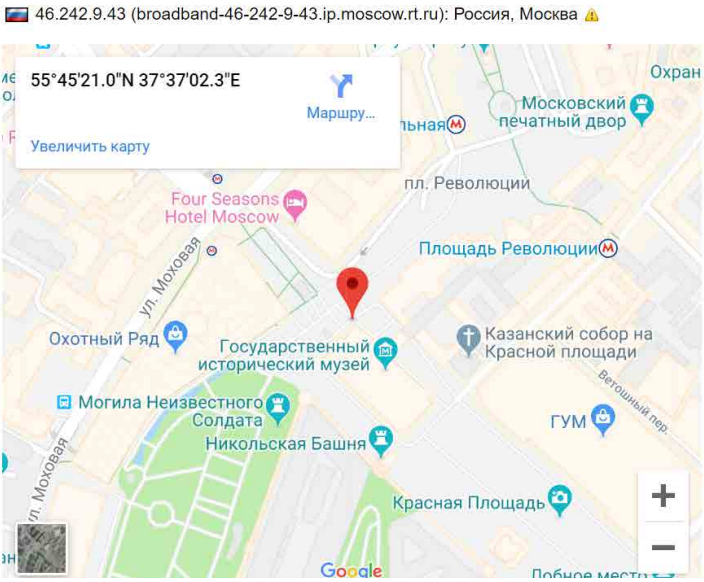
неограниченный круг неизвестных лиц, что wi-fi в его квартире не взломали хакеры и т.д. и т.п.

Кстати, для внешнего наблюдателя IP-адрес всех устройств, подключенных к вашему роутеру, — ноутбуков, планшетов, телефонов, своих и гостей, в том числе и непрошенных, — будет один и тот же. Чтобы вычислить нарушителя, нужно будет провести более детальное расследование.

Как узнать свой IP-адрес, под которым вас видно в интернете? Очень просто. Напишите в окне поиска Google «ip», нажмите «Ввод» — и сразу увидите свой публичный адрес, выданный вам провайдером. Если вам хочется более подробной информации, то можно перейти на сайт ***2ip.ru****. Также здесь можно проверить и любой другой адрес — просто введите его в специальном окне.*



Здесь уже видно, откуда вы: Россия, Москва. Если кликнуть по этой ссылке, то сервис покажет более точно ваше местоположение. Но не спешите волноваться, что все видят, где вы сидите:



публично доступны только координаты города: для Москвы это будет нулевой километр — помните это место перед Иверскими воротами, где туристы бросают монетки?

И еще раз: без запроса из правоохранительных органов физический адрес пользователя по его IP-адресу узнать нельзя. Полиция, Следственный Комитет или ФСБ направит провайдеру

запрос только в рамках расследования какого-либо дела; просто так из любопытства никто работать не будет. Но даже это вовсе не означает, что злоумышленника мгновенно возьмут, — если только он не круглый идиот, то он позаботился о том, чтобы скрыть свой настоящий IP-адрес.

Другое дело, если вас ищут за пост, например, «ВКонтакте», нарушающий законодательство РФ: тут данных, предоставленных провайдером и администрацией соцсети, будет достаточно для идентификации. Поэтому не мешает лишний раз подумать перед тем, как публиковать контент на потенциально опасную тему.

Что скрывать честному человеку?

Прежде чем продвинуться немного дальше к цели стать интернет-невидимкой, давайте еще раз поразмыслим, зачем это нужно. «Честному человеку скрывать нечего», — говорят противники анонимности, мотивируя свою позицию интересами общественной безопасности. Дескать, тотальная слежка нужна, чтобы ловить террористов. Обычно под такими лозунгами выступают представители власти, уговаривая общество согласиться с очередным ограничением свободы. Этот мотив тут же подхватывают и представители бизнеса, не менее госорганов заинтересованные в сборе данных на своих пользователей. Возьмем, к примеру, слова исполнительного директора Google Эрика Шмидта (Eric Schmidt), сказанные в интервью каналу CNBC в 2009 году:

> *«Если у вас есть то, о чем не должен знать никто, возможно, в первую очередь, вам не стоило делать этого. Но если вам*

> *действительно нужна такого рода конфиденциальность, реальность заключается в том, что поисковые системы, включая Google, хранят подобную информацию в течение некоторого времени. И это важно, потому что, например, все мы в Соединенных Штатах должны соблюдать Патриотический акт. Вполне возможно, что эта информация может предоставляться органам власти»*[1].

С тех пор возможности Google по отслеживанию действий пользователей фантастически выросли, и это вызывает все большее беспокойство в обществе, в то время как политики и крупный бизнес продолжают изображать недоумение: «Разве вы делаете что-то незаконное? Что вы хотите скрыть?»[2]

На самом деле речь идет не о сокрытии, а о защите. Мы живем в мире, полном тайн. Есть тайна государственная, коммерческая, банковская, налоговая, адвокатская, врачебная, тайна завещания, тайна усыновления, тайна следствия (куда без нее), а у журналистов есть право не раскрывать источник информации. В конце концов, есть тайна связи, раз уж мы говорим про интернет.

> *Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (действующая редакция) гласит, что на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.*

---

1 *Google CEO Eric Schmidt on privacy. // YouTube,* ***https://youtu.be/A6e7wfDHzew***

2 *Честному человеку нечего скрывать? // BitNovosti.com, 13 июля 2015.*

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

Но, как говорится, на оператора надейся, а сам не плошай: граждане тоже имеют право позаботиться о сохранении своих тайн, если считают меры, предпринимаемые операторами, недостаточными. И анонимность может быть очень полезным инструментом в этом деле.

Вот несколько примеров.

Допустим, вы работаете над новым проектом и придумали гениальную идею, способную изменить мир. Всякой идее такого масштаба предшествует долгий и кропотливый поиск, изучение массы научных работ, просмотр тысяч статей и публикаций. Это значит, что вам непременно придется воспользоваться поисковиком в интернете — и если это будет наш любимый Google, то все ваши поисковые запросы будут сохранены, проанализированы и привязаны к вашему профайлу. А значит, есть риск, что эта информация куда-то утечет. Да, сама по себе она несекретна, но на ее основе можно сделать вывод о направлении работ вашей лаборатории, а это уже хлеб для шпионов.

Или, предположим, вы врач и ведете анонимный прием больных. При некоторых диагнозах, таких как алкогольная или наркотическая зависимость, психические или венерические болезни, это вполне распространенная практика. Не исключено, что с кем-то из пациентов

вам понадобится общаться через интернет, и в таком случае, разумеется, стоит позаботиться об анонимности и на техническом уровне, чтобы сохранить врачебную тайну. (Строго говоря, оказание телемедицинских услуг в анонимном порядке на данный момент в нашем законодательстве не предусмотрено, но и не запрещено.)[1]

Работа адвокатов, следователей и журналистов тоже требует анонимных контактов со свидетелями и информаторами, и нужно понимать риски, которые при этом возникают, — в первую очередь, у людей, которые, возможно, рискуют жизнью, передавая вам какие-то сведения. В такой ситуации тезис, что «честному человеку нечего скрывать» выглядит особенно лицемерно — даже если идентификация пользователей производится суперзащищенной государственной системой, риск утечки этих данных все равно остается. Уж лучше оставаться анонимом.

Общепринято, что благотворительность должна быть анонимной. Благотворитель может иметь разные причины сохранять инкогнито: нежелание раскрывать свое финансовое состояние, стремление избежать персонифицированного чувства благодарности и так далее. (В связи с этим возникает вопрос об анонимных платежах, но это отдельная большая тема.)

И, в конце концов, право на тайну частной жизни тоже еще никто не отменял. «Дело не в том, что у меня есть что скрывать, а в том, что мои дела не касаются всех остальных». Может быть, я хочу смотреть мультики про розовых пони, но не желаю, чтоб об этом

1 *Возможно ли анонимное обращение пациента за получением телемедицинской консультации? // ГАРАНТ.РУ, 21 мая 2018.*

знали все на свете. Это не бог весть какая тайна, просто мне так спокойнее.

Анонимность для «чайников»: начнем с прокси

Достичь базового уровня анонимности в ситуации, когда большинство людей не знают, кто вы, — простая задача даже для «чайника».

> *«Все, что нужно — это VPN, блокировщик рекламы и инструмент конфиденциальности (privacy tool), например, Privacy Badger[1]. Этот уровень контроля поможет запутать ваши следы в интернете и сбить с толку тех, кто попытается собрать личные данные», — объясняет Бен Уильямс, операционный директор блокировщика рекламы Adblock Plus[2].*

Стоп-стоп, давайте по порядку, не так быстро.

Итак, чего, прежде всего, хочет путешественник по интернету? Посещать любые сайты, которые ему заблагорассудится, сообщая им

---

1 *Privacy Badger — это надстройка для браузера, которая запрещает рекламодателям и другим сторонним трекерам тайно отслеживать, куда вы переходите и какие страницы просматриваете в интернете. Если рекламодатель отслеживает вас на нескольких сайтах без вашего разрешения, Privacy Badger автоматически блокирует загрузку любого содержимого от него в вашем браузере. Для рекламодателя это выглядит так, как будто вы внезапно исчезли. Проект организации Electronic Frontier Foundation. Есть версии для Firefox и Chrome.*

2 *Возможна ли анонимность в интернете? // **GeekBrains.ru**, 15 мая 2018.*

о себе только те сведения, которые он сочтет нужным сообщить, а может, и вовсе ничего, — ведь оказавшись где-то за рубежом, мы хотим бродить по городу, слившись с толпой туристов, а вовсе не расхаживать все время с российским флагом, тем более что неизвестно, как там относятся к русским. Но наш IP выдает нас с головой. По IP-адресу владелец каждого сайта сразу видит, откуда вы — с точностью до города.

По IP-адресу владелец каждого сайта сразу видит, откуда вы — с точностью до города.

Дальше возможны варианты. Например, в зависимости от страны, вам могут ограничить доступ к какому-либо контенту. Часто так бывает с онлайн-кинотеатрами, потому что правообладатели предоставляют им лицензию для показа фильмов на определенной территории. Для интернета, где нет физических границ, это звучит глупо, но тем не менее такие ограничения существуют со времен, когда фильмы продавали на кассетах и DVD, и, купив диск в Англии, дома вы с удивлением обнаруживали, что его нельзя посмотреть на вашем плеере.

Кстати, бывает и наоборот: если вы попробуете зайти в свой оплаченный аккаунт в легальном российском онлайн-кинотеатре из-за рубежа, то, скорее всего, вас не пустят — местный провайдер даст вам IP-адрес, с которым вы будете выглядеть для администрации как иностранец — и все, «кина не будет».

Чтобы избежать всех этих неприятностей, вам нужно скрыть свой IP-адрес. Но интернет так не работает: для установления сеанса связи с любым сайтом какой-то адрес обязательно нужен.

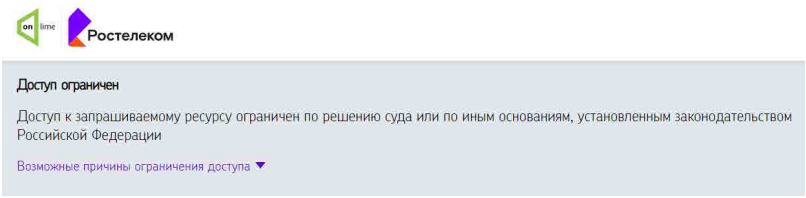
Эту задачу решают сервисы-анонимайзеры, которые подставляют вместо вашего настоящего IP-адреса IP-адрес любой страны по вашему выбору, устраивая эдакий бал-маскарад в интернете. Хотите нарядиться ковбоем с дикого Запада — пожалуйста! Предстать немцем в баварской шляпе с пером — не вопрос! Венецианцем в таинственной маске — тоже организуем!

Технически анонимайзеры, кроме самых примитивных, представляют собой прокси-сервер (от англ. proxy — «представитель», «уполномоченный»). Что это такое? На самом деле — очень полезная вещь, которая есть у каждого провайдера и в каждом крупном офисе. Причем сокрытие вашего IP-адреса — далеко не основная цель ее работы.

> *Представьте: в офисе работают сто человек, и все заходят с утра посмотреть новости в «Яндексе». Это значит, что с сервера «Яндекса» нужно сто раз загрузить одну и ту же страницу, — даже если трафик у вас безлимитный, скорость-то все равно ограничена, а всем хочется, чтобы интернет работал быстро. Поэтому и придумали сохранять на промежуточном сервере информацию, скачиваемую извне, чтобы экономить трафик. Еще прокси защищает компьютеры внутренней сети от внешних атак. Не то чтобы на сто процентов (это было бы слишком легко) — но, по крайней мере, от прямых посягательств. А в качестве бонуса как раз и прилагается анонимизация — для внешних наблюдателей все внутренние пользователи имеют один и тот же IP-адрес.*

Есть у прокси и неприятное для пользователей свойство: его можно настроить так, что он будет блокировать какие-то сайты. Для этого используют черные и белые списки: например, в офисе

могут закрыть доступ к соцсетям, занеся их в черный список, чтобы в рабочее время сотрудники не отвлекались; или закрыть доступ вообще ко всему интернету, кроме нескольких нужных для работы серверов, включенных в белый список. Кстати, примерно также работают блокировки Роскомнадзора: ведомство издает список запрещенных сайтов, а провайдеры его регулярно скачивают, чтобы настроить черные списки на своих серверах. И когда вы идете, куда не положено, вам показывают вот такую страницу:



Кроме провайдерских и офисных прокси есть и прокси-анонимайзеры, специально созданные для обеспечения анонимного доступа. Они-то и меняют ваш настоящий IP-адрес на случайный (обычно давая вам выбрать страну). Таким образом, прокси помогает обходить блокировки: провайдер видит, что вы заходите на разрешенный сайт, и спокойно вас пропускает, а дальше вы говорите прокси-серверу, куда вам на самом деле хочется попасть — и идете.

Благодаря активности Роскомнадзора, который в своих попытках закрыть доступ к мессенджеру «Телеграм» в 2018 году массово блокировал миллионы IP-адресов, на время переставали работать ни в чем не повинные сайты; «под раздачу» попали, в частности, «ВКонтакте», «Яндекс», «Одноклассники», Yahoo, Twitter и многие другие. Ошибочные блокировки быстро исправили, но, как говорится, осадочек

остался[1]. Граждане занялись повышением компьютерной грамотности, и все от мала до велика узнали о существовании прокси (и VPN, но про них чуть позже) как средства доступа к заблокированным ресурсам. Впрочем, кибербезопасность — такая тема, где поверхностные знания могут оказаться хуже, чем полная неосведомленность.

Кибербезопасность — такая тема, где поверхностные знания могут оказаться хуже, чем полная неосведомленность.

«В интернете есть много открытых бесплатных прокси-серверов, и некоторые из них предоставляют разнообразные полезные услуги», — встретив такую фразу, стоит насторожиться. Как же они себе на жизнь зарабатывают, если не берут денег с пользователей? Вариантов всего два: либо это честный сервис, который сначала даст бесплатно какую-то ограниченную функциональность и будет потом очень настойчиво предлагать купить полный пакет (что, в целом, вызывает понимание); либо это чей-то очень «мутный» бизнес, который на самом деле собирает ваши данные с корыстными целями — например, чтобы продать их рекламодателям (в лучшем случае) или хакерам (что гораздо хуже). А может быть, такой «левый» прокси вообще работает под колпаком у спецслужб, чтобы учесть всех несознательных граждан.

Какой же прокси выбрать? Платный или бесплатный? Российский или обязательно зарубежный? Вообще говоря, никакой. Прокси в чистом виде сейчас уже почти не используются. Все разработчики предлагают более совершенное решение — VPN.

---

1 *После двух лет безуспешных попыток Роскомнадзор объявил о снятии требования по ограничению доступа к мессенджеру Телеграмм. О мессенджере «Телеграмм». // Роскомнадзор, официальный сайт, 18 июня 2020.*

Сайт в конце туннеля, или Зачем нам VPN

Fig.1 VPN functional principles

Так что же это такое — VPN? Чем она лучше прокси? VPN расшифровывается как Virtual Private Network, а по-русски — «виртуальная частная сеть». По правде говоря, название ничуть не проясняет того, как эта штука работает и как помогает нашей анонимности в интернете. Разгадка, как это часто бывает, лежит в истории.

> *Изначально VPN были созданы для того, чтобы позволить сотрудникам удаленно работать с корпоративными серверами не только находясь в офисе, но и дома или в командировке.*

Компании были очень озабочены конфиденциальностью своих данных и не доверяли публичным сетям. (Кстати говоря, правиль-

но делали — мы к этой теме еще вернемся.) Начальник службы безопасности какого-нибудь условного банка или госкорпорации упал бы в обморок, если бы узнал, что сотрудники пересылают файлы, сидя со своим ноутбуками где-нибудь в «Макдональдсе». А что делать? Пропустить день рождения ребенка и ехать в офис, чтобы пару раз кликнуть мышкой?

К счастью, программисты придумали решение. Чтобы исключить возможность кражи или подмены данных при их передаче по публичным сетям, они разработали технологию, которая позволяет установить защищенное соединение между компьютерами одной организации, даже если они находятся за пределами офиса. Это похоже на то, как члены тайного общества узнают друг друга по особым знакам на званом приеме, и среди общего шума находят минуту-другую, чтобы пошептаться о своих коварных планах по захвату мира.

> *Использовать VPN специально для того, чтобы анонимно ходить в интернет, никто не собирался. Она потому и частная, что была предназначена только для своих. А виртуальная — потому, что работает поверх обычной сети и каждый раз коммутируется по-новому.*

Как же это происходит? Вот, допустим, вы сидите в кафе и хотите подключиться по VPN к своей рабочей электронной почте. Если вы внимательно читали предыдущий раздел про IP-адреса, то, наверное, догадались, что сначала вам придется через местный (небезопасный) wi-fi подключиться к интернету, и тогда вашему компьютеру дадут IP-адрес. Так, а дальше? Дальше ваш компьютер видит в сети VPN-сервер и подает ему тайный знак. Сервер отвечает, и они прокладывают между собой туннель, то есть уста-

навливают логическое соединение, которое для внешнего наблюдателя выглядит как обычный обмен пакетами. А на самом деле они обмениваются зашифрованными сообщениями, которые даже если перехватить, то прочитать все равно не получится. На выходе из туннеля VPN-сервер расшифровывает ваш трафик и выпускает его в офисную сеть.

Вы входите где-нибудь в Польше, а выходите в Канаде — и ни один провайдер этого не видит.

Зачем все эти хитрости обычному пользователю? Представьте, что VPN-серверы стоят во всех (ну, хорошо, во многих) странах мира и между ними прорыты туннели, и это все единая сеть. Вы входите где-нибудь в Польше, а выходите в Канаде — и ни один провайдер этого не видит. Что значит «выходите в Канаде», спросите вы? Это значит, что VPN работает и как прокси — то есть выдает вам IP-адрес той страны, какой вы попросили, и дальше вы обращаетесь к любым сайтам так, как будто находитесь в Канаде.

Чем же это отличается от обычного прокси? Во-первых, прокси обычно не шифруют трафик, и он может быть перехвачен (встречаются и шифрованные прокси, но это уже почти VPN). Во-вторых, чтобы обходить блокировки, прокси-сервер должен стоять за границей, но тогда и он сам может быть заблокирован. А сервер VPN может стоять и дома — трафик-то передается по шифрованному туннелю! (Правда, у провайдера остается возможность блокировать подозрительный трафик — все, что непонятно, то и подозрительно.)

Современные VPN установить не сложнее, чем какой-нибудь антивирус, — просто скачиваете дистрибутив и ставите.

Первые VPN были очень дороги и сложны, установить и правильно их настроить могли только специально обученные люди, и потому технология оставалась недоступной обычным пользователям. Да и секретов у них особых не было, чтобы платить за такой сервис. Современные VPN установить не сложнее, чем какой-нибудь антивирус, — просто скачиваете дистрибутив и ставите. Или того проще: устанавливаете плагин в браузере, и — вуаля! Но у браузерных VPN есть ограничение: через них идет только веб-трафик, а ведь бывает, что некоторым приложениям тоже нужен защищенный канал — например, почтовому клиенту. Короче говоря, десктопные VPN более универсальны.

Остается вопрос: платить или не платить? Решайте сами, не давая, однако, жадности пересилить голос разума. Вот, например, что пишут в новостях:

> *Каждое пятое VPN-приложение в Google Play — потенциальный источник вредоносного ПО.*
>
> *22 января 2019 года стало известно, что наиболее популярные бесплатные VPN-приложения в Google Play Store содержат проблемы, которые могут угрожать безопасности пользователей. Согласно результатам исследования, проведенного специалистом Metric Labs Симоном Мильяно (Simon Migliano), каждое пятое приложение является потенциальным источником вредоносного ПО, а в четверти проанализированных программ содержатся уязвимости, связанные с утечками DNS-запросов пользователей*[1].

1 ***TAdviser.ru.***

Конечно, сам по себе факт оплаты не гарантирует, что продукт надежный, но риск нарваться на преднамеренное хищение ваших данных при использовании коммерческих продуктов все-таки значительно меньше.

Из минусов VPN обычно упоминают низкую скорость работы, однако чаще причина медленного интернета кроется в настройках wi-fi или ограничениях провайдера. На хорошем канале замедление из-за включенного VPN практически незаметно. К сожалению, факт использования VPN невозможно полностью скрыть: некоторые программы могут по этой причине работать некорректно. Сам провайдер тоже может счесть трафик VPN подозрительным и блокировать его, хотя расшифровать и прочесть — не сможет.

Можно сказать, что VPN — это основной инструмент защиты вашей анонимности в интернете.

Итак, можно сказать, что VPN — это основной инструмент защиты вашей анонимности в интернете. Фактически VPN включает в себя функции прокси, то есть позволяет скрывать ваш IP-адрес и шифрует данные при передаче, чтобы не допустить их утечки.

По статистике за 2018 год сервисами VPN хотя бы однажды пользовались 19% российской аудитории. Согласно данным Brand Monitor, чаще всего VPN устанавливают молодые пользователи (18–24 лет) — 22% опрошенных. Вероятнее всего, число пользователей VPN продолжит расти вместе с ростом понимания, что анонимность в Сети имеет большую ценность.

Ситуация на рынке VPN меняется динамично, поэтому трудно дать совет, какой именно продукт выбрать. Почитайте свежие обзоры

и выберите для себя VPN, платный или бесплатный — на ваше усмотрение. Не забудьте защитить все устройства, с которых вы выходите в интернет, включая смартфоны.

Интернет как госуслуга? Еще нет, но может быть

Государство (любое) выступает последовательным противником анонимности. С точки зрения властей, идеальной была бы ситуация, когда все граждане заходят в интернет по предъявлению паспорта (например, через сайт госуслуг), и все их шаги записываются в специальный журнал. Посетил такой-то сайт, прочитал новости, оставил комментарий. Написал письмо иностранцу, вот текст. В интернет-магазине заказал черную футболку, зонт и велосипедный шлем. Очень подозрительно!

Это не шутка, это правда жизни: летом 2019 года в Гонконге эти предметы входили в стандартную экипировку участников протестов, поэтому китайские интернет-магазины прекратили их продажу жителям города. Зачем протестующим зонты? Очень просто — чтобы скрывать лица от камер видеонаблюдения[1].

1 *В связи с пандемией коронавируса во многих городах и странах ношение масок в общественных местах стало обязательным. И даже после снятия ограничительных мер едва ли власти станут заставлять граждан перестать носить маски. Интересно, как это отразится в законодательстве о митингах? Поставщики систем распознавания лиц заявляют, что могут узнать человека и в маске, но маска ведь может быть любой, не только стандартной медицинской.*

Зачем протестующим зонты? Очень просто — чтобы скрывать лица от камер видеонаблюдения.

Если в целях борьбы с анонимностью власти готовы запретить обычные зонты, то что уж говорить о специализированных средствах сокрытия личности в цифровом пространстве. Естественно, они попали под огонь законодательной «артиллерии».

> *С 1 ноября 2018 года в России действует закон[1], который обязывает владельцев VPN-сервисов и анонимайзеров не предоставлять пользователям возможность обхода блокировок сайтов, внесенных в Единый реестр Роскомнадзора.*

Технология VPN не создавалась специально для обхода блокировок, так получилось. После введения упомянутого закона эта возможность, скорее всего, останется только в продуктах зарубежных поставщиков. Что касается российских разработчиков, то они, безусловно, вынуждены подчиниться, о чем, в частности, объявила «Лаборатория Касперского». С июля 2019 года VPN-сервис Kaspersky Secure Connection выполняет требования Роскомнадзора и блокирует трафик, сообщая пользователям при попытке доступа к сайтам из реестра, что «данная страница недоступна в РФ».

Зарубежные VPN могут уйти из России, если на них будет оказываться давление: например, штрафы за неисполнение требований РКН. Об этом прямо сказал представитель Tor Guard:

---

1 *Федеральный закон от 29 июля 2017 года № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».*

«Удаление серверов в стране, в которой “правовой климат может представлять угрозу для онлайн-безопасности наших клиентов” — стандартная политика компании. По этой причине решено немедленно прекратить работу серверов в Санкт-Петербурге и Москве».

Анонимайзеров и служб VPN так много, что заблокировать их все нереально.

Такой поворот событий может создать сложности для пользователей — ведь IP-адреса VPN-сервера, находящегося за рубежом, тоже могут быть заблокированы, а пока ты не добрался до сервера, туннель не построишь. Успокаивает то, что анонимайзеров и служб VPN так много, что заблокировать их все нереально. Теоретически возможен и китайский сценарий, когда блокируется весь подозрительный трафик, который не поддается расшифровке спецслужбами, но это маловероятно.

Пока закон не запрещает частным лицам пользоваться анонимайзерами и VPN-сервисами, в том числе и зарубежными. Нет ответственности для граждан и за просмотр заблокированных страниц — ответственность наступает только за распространение запрещенного контента и за высказывания, нарушающие законодательство РФ. Для обычного пользователя это выглядит как запрет продажи сигарет несовершеннолетним: когда подросток покупает сигареты, наказывают не его, а продавца.

И еще раз: VPN — средство безопасного доступа к сетевым ресурсам, а не средство обхода блокировок. За заботу о собственной безопасности пользователя надо хвалить, а не наказывать.

Пространство для анонимности сокращается не только из-за гонений на анонимайзеры и VPN. 1 июля 2018 года в России вступил в действие так называемый «Закон Яровой»[1]. Согласно этому закону, все провайдеры должны хранить на своих серверах переписку и звонки пользователей в течение полугода. Такие меры обосновывают борьбой с терроризмом. Но при этом они еще дают спецслужбам неограниченные возможности слежки за всеми гражданами без исключения.

О том, какие конкретно данные будут о нас собирать, было сказано позже в приказе Минкомсвязи. Согласно этому документу, интернет-компании и сервисы должны хранить и предоставлять спецслужбам: псевдоним, дату рождения, адрес, фамилию, имя, отчество, паспортные данные, языки, которыми владеет пользователь, список его родственников, текст сообщений, аудио- и видеозаписи, адрес электронной почты, дату и время авторизации и выхода из информационного сервиса, наименование программы-клиента.

«Закон Яровой» определяет, что сохраняемая информация должна предоставляться сотрудникам ФСБ по их запросу. В то же время последующим постановлением Правительство прописало возможность круглосуточного доступа ФСБ к хранилищу и базе данных — между системой оператора и соответствующими структурами ФСБ должен быть налажен постоянный канал связи. Кроме того, не исключено, что ФСБ

1 *Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи».*

сможет получить у владельцев некоторых соцсетей, почтовых служб и мессенджеров доступ к ключам шифрования.

К «Яндексу» с требованием предоставить ключи шифрования для сервисов «Яндекс.Диск» и «Яндекс.Почта» уже пришли. Пока непонятно, чем эта история закончится, но лучше исходить из предположения, что все российские интернет-сервисы будут полностью прозрачными для спецслужб[1].

Что нужно объяснить подростку: не надо изображать из себя крутого хакера; надо понимать, что все доступные пользователю средства анонимизации, скорее всего, будут неэффективны против государственных систем, поэтому надо учиться ответственному поведению в Сети.

Пользователь, иди сюда, у нас есть печеньки!

Анонимность всегда продается в обмен на удобство и маленькие радости жизни. Если вы регулярно ходите в одно и то же кафе, вас начинают там узнавать, здороваться при входе и спрашивать: «Вам как обычно?» И вы отвечаете: «Да». Постепенно вы разговоритесь с официантом, расскажете, что живете здесь неподалеку, что ваш ребенок ходит в соседнюю школу, в пятый класс, ваша мама как раз приехала посидеть с внуком, и сегодня вы можете задержаться в кафе подольше. То есть сообщите о себе много личной инфор-

1 *За год применения «Закон Яровой» угодил в патовую ситуацию. // **Telesputnik.ru**, 18 июля 2019.*

мации, которую официант запомнит и, возможно, даже передаст своему сменщику, чтобы тот позаботился о постоянном клиенте. Вы расслаблены и не думаете о безопасности. А вместе с чашкой кофе и счетом вам принесут печеньку — комплимент от заведения.

Веб-сайты тоже раздают посетителям печеньки-куки[1], только виртуальные. И не вам лично, а вашему браузеру, который хранит их в специально отведенном месте, — как мы, бывает, кладем в карман фирменные леденцы, взятые на ресепшне какой-нибудь респектабельной фирмы, и забываем про них. Но если кто-то не в меру любопытный заглянет в ваш карман, он сразу поймет, где вы были. Куки — это отметка, свидетельствующая, что вы были на данном сайте.

Вот что про куки говорит Google:

> *Файл cookie — это небольшой фрагмент текста, передаваемый в браузер с сайта, который вы посетили. Он помогает сайту запомнить информацию о вас, например, то, на каком языке вы предпочитаете его просматривать. Это будет полезно при следующем посещении этого же сайта. Благодаря файлам cookie просмотр сайтов становится значительно более удобным.*
>
> *Файлы cookie применяются в различных целях. Например, они позволяют сохранять настройки рекламных предпочтений и безопасного поиска, подбирать интересующие пользователей объявления и подсчитывать количество посещений страницы. Также они необходимы при регистрации в сервисах Google и обеспечении безопасности личных данных.*

1 *Куки (англ. cookie, буквально — «печенье»).*

Почему же их так боятся? Вроде же отличная вещь, придуманная для нашей же безопасности!

Не совсем так. На заре интернета браузеры были программами для просмотра веб-сайтов и не умели ничего больше. У самого сайта технически не было возможности идентифицировать посетителя, если тот не представится, то есть не введет имя и пароль (а если сайт не подразумевал регистрацию, то вообще никак). Как если бы вы приходили в свое любимое кафе, а официант, с которым вы вчера мило болтали, смотрел бы на вас в полном изумлении, как будто у него отшибло память, пока вы не назовете свое имя. Вот тогда он сразу бы включался, вспоминал ваши привычки и предлагал вам ваш любимый столик.

Но это еще полбеды: стоило бы вам на минуту выйти, допустим, покурить (хотя в то время не возбранялось курить и в заведениях) — и по возвращении нужно было бы начинать диалог с официантом с начала, потому что добрый малый уже не помнил, за каким столиком вы сидели и что заказали. Не очень-то удобно, не правда ли?[1]

> *В общем, дело было так. Шел 1994 год. Программист компании Netscape Communications Лу Монтулли ломал голову над тем, как излечить интернет-браузер от амнезии. Его компания разрабатывала первую в мире систему электронной коммерции, и нужно было заставить браузер запоминать состояние виртуальной корзины клиента. Идея, пришедшая ему в голову, была гениально простой — пусть веб-сайт посылает на каждый клиентский компьютер небольшой файл,*

1 *Giving Web a Memory Cost Its Users Privacy. // The New York Times, 4 сентября 2001.*

в который мы запишем его уникальный номер и нужные параметры. Когда клиент вновь посетит наш сайт, мы тихонько считаем этот файл и сразу вспомним, кто он такой. Продолжая аналогию с кафе, это, как если бы забывчивый официант записывал имя гостя на карточке и незаметно подкидывал бы ему в карман, а при следующем визите также незаметно бы доставал ее, чтобы вспомнить, как его зовут.

Но ведь шарить по чужим карманам нехорошо, скажете вы. Да, нехорошо. Однако разработчики именно так и сделали — втихаря стали записывать куки с важными данными на компьютеры клиентов. Естественно, когда после публикации в Financial Times, где говорилось об угрозах приватности, возникавшей из-за применения этой технологии, все выплыло наружу, общественность возмутилась. Вопрос даже был рассмотрен Федеральной комиссией по торговле США в двух слушаниях — в 1996 и 1997 годах. Но механизм оказался настолько удобным для рекламщиков и продавцов (и спецслужб), что дело в итоге замяли, а печеньки-куки распространились повсеместно. Сегодня их использует почти каждый из посещенных вами сайтов. Найдите в своем браузере список сохраненных куки и ужаснитесь, как их много, — в том числе от сайтов, о существовании которых вы даже не знали.

Механизм оказался настолько удобным для рекламщиков, продавцов и спецслужб, что дело замяли, а печеньки-куки распространились повсеместно.

Нет, ну а что вы хотели от 24-летнего программиста? Ему сказали решить задачу — он решил. Ему же не поручали думать о безопасности и анонимности пользователей. «Это вроде работает, но определенно придумано за одну ночь», — так отзывались о первой

реализации cookie специалисты. Конечно, потом технологию доработали, самые острые проблемы с безопасностью удалось решить, но все равно «печеньки», на скорую руку придуманные Лу Монтулли, остаются одной из основных угроз анонимности пользователей интернета.

Чем же они так опасны?

> *Есть два связанных с куки неприятных момента. Во-первых, с их помощью можно отслеживать пользователей — этим пользуются как продавцы, так и спецслужбы. Во-вторых, куки можно похитить и добыть таким образом конфиденциальную информацию о вас — этим промышляют хакеры.*

Давайте сначала разберемся с хакерами: где и как они могут украсть наши печеньки? Вот вы сидите в своем любимом кафе (не в нашем гипотетическом кафе с беспамятными официантами, а в настоящем) и подключаетесь по wi-fi к интернету. О'кей, раз закон требует, то регистрируетесь — сообщаете свой телефон, вам приходит SMS, вы вводите код в нужное поле и выходите на цифровой простор. Вы замечали, что иногда сайт провайдера спрашивает, сколько вас помнить — неделю, месяц, квартал? Вот это как раз про куки.

Условно говоря, кафе выписывает вам читательский билет со сроком действия 7, 30 или 90 дней. Когда придете в следующий раз в течение этого периода, вас пустят без регистрации, а по истечении указанного времени куки автоматически удалятся. А что будет, если ваши куки достанутся жулику? Правильно, он сможет подключаться к этому wi-fi вместо вас. (На самом деле все сложнее, но в общих чертах примерно так.) Поэтому у жуликов есть мотивация охотиться за куки.

Способов украсть куки множество. Вот, например: берете wi-fi-роутер, называете свою сеть так, чтобы в имени были слова «WIFI_FREE», садитесь в людном месте и ловите «рыбку».

Все любят «халявный» wi-fi, поэтому люди сами принесут вам свои куки на блюдечке с голубой каемочкой, даже уговаривать никого не надо. А в них часто — логины и пароли. (Вы все еще пользуетесь публичными wi-fi без VPN? Ну-ну...) Есть и специальные программы-снифферы для перехвата куки — они могут встретиться не только в публичных wi-fi-сетях (так что VPN всегда полезен). И это далеко не все варианты.

К счастью, крупные интернет-сервисы — «Яндекс», «ВКонтакте», Mail.ru и другие — используют сегодня шифрованные куки. Но в мире по-прежнему полно программистов, которым нужно сделать что-то по-быстрому. Их подгоняют менеджеры проектов, на которых покрикивают основатели стартапов, опасающиеся гнева инвесторов за бездарно потраченные деньги... Скорость выхода на рынок все еще важнее безопасности. А сделанное однажды кое-как, но работающее решение имеет все шансы просуществовать очень долго. За это время разработчики станут миллионерами, как мистер Монтулли, а проблемы безопасности будет решать кто-то другой, если, конечно, уязвимость будет обнаружена.

Сделанное кое-как, но работающее решение имеет все шансы просуществовать очень долго.

Зачем хакерам ваши куки? Чаще всего, чтобы угонять аккаунты соцсетей, мессенджеров, игровые аккаунты и другие цифровые активы. Или войти под вашими учетными данными в ту же wi-fi-сеть

и обстряпать свои черные делишки. А искать по IP потом будут вас. Натворить они могут что угодно, фантазия у них богатая — Ограбить банк или взломать государственный сайт, например. В общем, лучше не давать им такого шанса.

Для этого нужно усвоить следующие правила:

- При пользовании чужими компьютерами или телефонами всегда включайте в браузере режим «Инкогнито». По окончании работы обязательно закрывайте все сессии, все открытые вами окна и удаляйте куки;

- При пользовании публичными сетями обязательно включайте VPN. Если нет такой возможности, не посещайте сайты, требующие ввода конфиденциальных данных;

- Включите двухфакторную авторизацию на всех важных сервисах (соцсети, почта, мессенджеры, облачные хранилища, платежные системы и т.д.).

Спасет ли двухфакторная авторизация при краже куки? Абсолютной гарантии нет, потому что есть вероятность подделки вашей SIM-карты для перехвата SMS или хищения пароля от почты, но в целом эта мера значительно снижает риски. (Подробнее о двухфакторной авторизации см. главу про пароли.)

Помните, что куки задумывались как полезная технология, призванная сделать вашу жизнь более удобной. Поэтому не надо объявлять «печенькам» тотальную войну — многие из них честно несут свою службу. Без куки большинство сайтов не смогут функционировать нормально, а ваш браузер снова станет очень

забывчивым. Проблема не в технологии, а в том, что есть люди, скажем так, с очень размытыми этическими принципами, которые используют куки в своих целях.

«Он и меня посчитал!» Как за нами следят с помощью куки

Наиболее беспардонно используют куки для слежения за пользователями компании, занимающиеся интернет-рекламой. Это стало возможным благодаря так называемым «сторонним куки». Если вы уже посмотрели список куки в своем браузере, то наверняка заметили, что там полно «печенек» от сайтов, которые вы никогда не посещали и даже не знали об их существовании. Откуда они все взялись?

А это и есть сторонние куки — ваш браузер получает их, когда открывает страницу, где, кроме основного контента, показываются рекламные баннеры, блоки новостей, прикольные картинки и видео, прогноз погоды, курсы валют, турнирные таблицы, гороскопы, программы ТВ и тому подобное. Такая веб-страница представляет собой коллаж фрагментов с разных сайтов — вот они-то и присылают сторонние куки. Вам даже не надо кликать на баннер — достаточно того, что он отобразился на экране, это уже засчитывается за посещение его родного сайта, и его куки остаются на вашем устройстве.

> *Итак, если веб-сайт А содержит рекламное объявление, которое обслуживается веб-сайтом В, веб-сайт В может установить cookie в вашем браузере.*

Вообще-то изобретатель технологии такого не планировал, это получилось по недосмотру, и он потом это признал. В то время веб-страницы чаще всего были целыми, взятыми с одного сайта, поэтому никто и не думал, что сторонние куки могут превратиться в инструмент отслеживания пользователей. А когда заметили, то было уже поздно — крупные рекламные сети начали активно эксплуатировать этот изъян конструкции. В первых рядах была компания Double Click, которая давно стала частью Google, — куки с ее именем наверняка есть и на вашем компьютере.

Козленок из известного мультфильма тоже всех считал — как и продавцы интернет-рекламы.

> *Помните, гуляя по лесу, он начинает присваивать номера всем, кого встречает по пути: «...один — это я, два — это Теленок, три — это Корова. Один, два, три!», на что посчитанные неизменно обижаются, жалуются друг другу и хотят наказать Козленка за самоуправство. Обидно им просто потому, что какой-то Козленок без разрешения и объяснений произвел с ними непонятную процедуру, поставив их перед фактом.*
>
> *Компания недовольных растет, и вот уже все они дружно бегут за Козленком, чтобы его побить (или вразумить на тему недопустимости посягательств на персональные данные граждан).*

Кстати, если вы не знали: ситуация, показанная в мультфильме, совсем не про обучение устному счету. Она связана с психологическим феноменом оценивания, стрессом, который вызывает у индивида осознание ситуации, что он стал объектом чьей-то оценки. Ряд

граждан, например, испытывают чувства, схожие с переживаниями героев «Козленка...» во время переписи населения. Примерно также дело обстоит и с озабоченностью людей тем, что их действия в интернете отслеживаются, да еще неизвестно кем и с какой целью. Конечно, из-под такого контроля хочется выйти.

Чтобы уменьшить внимание к своей персоне, включите в браузере блокировку сторонних cookie, выполнив следующие действия:

- **в Firefox**
  Сервис> Параметры> Конфиденциальность. Снимите флажок «Принимать сторонние cookie»;

- **в Chrome**
  Настройки> Расширенные настройки> Конфиденциальность> Настройки контента. Установите флажок «Блокировать сторонние файлы cookie»;

- **в Internet Explorer 11**
  Сервис> Свойства браузера> Конфиденциальность> Дополнительно. Выберите «Блокировать» в разделе «Сторонние файлы cookie».

Вы спросите: а как именно с помощью куки за нами следят? Мы же не логинимся на этих рекламных сайтах, значит, наши имена им неизвестны. Но дело в том, что им и не нужно знать ваше имя, чтобы попытаться вам что-нибудь продать. Им достаточно однажды дать вашему браузеру уникальный номер, чтобы потом видеть, на сайты какой тематики вы ходите и какие страницы просматриваете. При этом рекламщики уверяют, что все это делается для вашего же блага — чтобы показывать

вам только рекламу, отвечающую вашим интересам. Еще это помогает им контролировать показы рекламы — чтобы считать, сколько и кому баннеров продемонстрировали, и как клиенты на это реагировали, с каких сайтов пришли реальные покупатели, и делать прочую аналитику.

> *Можно было бы предположить, что раз ваше имя им неизвестно, то и анонимность вашу куки не нарушают. Но это, увы, не так. Достаточно вам один раз зайти на сайт, где требуется регистрация, как по номеру браузера с вашим именем свяжут все посещенные вами страницы.*

То есть рекламная компания может собрать на пользователя практически полное досье, а уж что с ним потом делать, они решат. Например, продать банкам, которым очень пригодится информация о том, что потенциальный заемщик тщательно изучал сайты по теме «как взять кредит и не платить» — почти наверняка такому клиенту откажут. (Хотя вполне может быть, что это всего-навсего журналист отрабатывал задание редакции, вовсе не собираясь становиться злостным неплательщиком.) Или наоборот: тому, кто активно смотрит сайты застройщиков, можно попробовать продать ипотеку. Вариантов использования информации о вас масса.

Спецслужбы тоже не гнушаются использовать куки как средство негласного наблюдения за пользователями — потому что это просто и удобно

Спецслужбы тоже не гнушаются использовать куки как средство негласного наблюдения за пользователями — потому что это просто и удобно. Показал один раз человеку картинку и дальше можешь видеть все его шаги. Да, это незаконно, но когда и где это останавливало спецслужбы?

Правительство Соединенных Штатов приняло строгие законы в отношении куки в 2000 году после того, как выяснилось, что Агентство по борьбе с наркотиками США использовало куки для отслеживания пользователей, просмотревших их антинаркотическую рекламу в Сети.

Тем не менее в 2002 году стало известно, что ЦРУ устанавливает на компьютеры постоянные куки со сроком хранения до 2010 года. Когда ЦРУ было уведомлено о неправомерности подобного использования куки, Управление заявило, что это было непреднамеренно, и прекратило их установку.

А в 2005 году обнаружили, что Агентство национальной безопасности оставляло пару постоянных куки после обновления программного обеспечения. После этого сообщения Агентство немедленно отключило куки.

Полагать, что на этом история закончилась, и что спецслужбы других стран не занимаются тем же, было бы, пожалуй, наивно.

Когда вы удаляете куки, где-то плачет рекламщик

«У куки есть один большой недостаток — его можно очистить. Любой, даже технически неподкованный пользователь знает, как очищать куки — Он нажимает «Настройки», заходит и очищает. Все, пользователь опять становится для вас анонимным, вы не знаете, кто он такой», — жалуется на жизнь один из представителей рекламной индустрии.

Что произойдет при удалении куки из браузера? Да ничего страшного. Можно сказать, что у браузера просто будет стерта память, в которой он хранил ваши действия при посещении сайтов. (Обычно говорят, что браузер забудет все сохраненные пароли, и придется везде заново логиниться, но это не так. Пароли хранятся во встроенном менеджере паролей, а не в куки.)

> *Совершенно точно нужно удалять куки, если вы работали за чужим компьютером, или если компьютером пользуются несколько человек под одной учетной записью. (Так часто бывает с домашними компьютерами.)*

Если вы еще сомневаетесь, стоит ли это делать, то давайте взглянем на цифры. По данным сайта Cookiepedia (**https://cookiepedia.co.uk/**), в базе данных которого собрана информация более чем о 10 миллионах куки, по своему назначению они распределяются следующим образом:

- 1% — строго необходимые, без которых работа сайта будет невозможна;
- 5% — используемые для анализа производительности, который включает в себя подсчет посещений страниц и скорости их загрузки, времени задержки, показателей отказов, и технологий, используемых для доступа к сайту;
- 3% — функциональные, позволяющие веб-сайту запоминать ваш выбор (например, имя пользователя, язык или регион, в котором вы находитесь) и предоставлять расширенные, более персонализированные функции;

- 58% — рекламные (это почти всегда будут сторонние куки);
- 32% — неизвестного назначения.

Статистика недвусмысленно намекает, что на самом деле куки больше нужны рекламщикам, чем пользователям. Так что периодическая их чистка должна стать обязательным элементом вашей цифровой гигиены.

Если у вас установлено несколько браузеров, операцию придется повторить в каждом из них. Не забудьте и про телефон: там тоже есть браузер (возможно, и не один), — значит, есть и куки. Разумеется, на детских устройствах чистка также обязательна.

Если у вас установлено несколько браузеров, операцию придется повторить в каждом из них.

Но не спешите радоваться, что вам удалось уйти из-под колпака мировой индустрии интернет-рекламы. Распробовав печеньки, они вошли во вкус и продолжают изобретать все новые методы трекинга пользователей. Они искренне не понимают, зачем людям анонимность, и досадуют, что пользователи становятся умнее и учатся использовать различные средства, препятствующие отслеживанию. Поэтому они постоянно совершенствуют куки.

> *Так появились evercookie — трудноудаляемые куки, которые прописывают информацию о себе в 13 различных местах системы, поэтому их очень трудно вычистить. Есть PNG Cookies, которые притворяются обычной картинкой и пытаются навечно закрепиться в кэше браузера. Есть Flash Cookies, бывшие до недавнего времени практически*

неудаляемыми. Наконец, это супер-куки, которые привязываются к домену верхнего уровня типа .com, а не к конкретному сайту; они являются потенциальной проблемой безопасности и поэтому часто блокируются веб-браузерами. Их иногда называют «зомби-куки», потому что они умеют «оживать» после того, как пользователь их «убил». Сколько бы вы их не удаляли, они появляются снова — поможет только осиновый кол.

Надо сказать, что разработчики браузеров всерьез озаботились этой проблемой и начали предпринимать активные шаги по наведению порядка. Осведомленные источники говорят, что в Google идут внутренние дебаты, которые могут привести к ограничениям использования технологий слежения и таргетинга (целевой рекламы). Поскольку Google владеет самой мощной рекламной и вездесущей платформой Google Marketing Platform, и самым популярным браузером Chrome, занимающем 63% мирового рынка, то решение будет трудным.

Apple представила умную технологию защиты от отслеживания Intelligent Tracking Protection (ITP) в браузере Safari еще в 2017 году, а в начале 2019 выпустила обновление, устанавливающее весьма жесткие правила по использованию куки. Теперь «срок годности печенья» от основного сайта сокращен до 7 дней, а сторонние куки блокируются сразу. Стоит также отметить, что в ITP 2.1 удалена поддержка параметра «Не отслеживать» (DNT — Do Not Track), поскольку разработчики рекламных технологий все равно полностью игнорировали этот параметр, даже если пользователи включали его.

Но ведь это же фактически «пчелы против меда», скажете вы. Неужели у кого-то проснулась совесть?

Едва ли. Скорее, дело в давлении общественности, выразившееся в принятии новых законов по защите прав пользователей. Люди возмутились тотальной слежкой со стороны интернет-гигантов, и теперь технологические компании вынуждены принимать меры, чтобы не попасть под нешуточные штрафы.

В мае 2018 года в Евросоюзе начал действовать Общий регламент по защите данных (GDPR[1]), обязательный для всех сайтов, посещаемых из Евросоюза, и приравнивающий большую часть куки к персональным данным. В изначальном проекте предполагалось, что настройки браузера могут признаваться достаточным выражением согласия пользователя на установку куки, а согласно окончательной версии, нужно было всего лишь уведомление об установке куки, чтобы получить «информированное согласие» пользователя.

Ассоциация потребителей Нидерландов решила проверить, как исполняется новый европейский закон. Оказалось, что 49% веб-сайтов (74 из 150 исследованных) размещают маркетинговые и/или рекламные файлы cookie непосредственно при открытии сайта, без вашего разрешения. Да, они обычно показывают посетителям окно куки с кнопкой OK для получения вашего согласия, но по факту они уже их разместили. Эта практика была незаконной в соответствии с предыдущим законом о cookie-файлах и остается таковой с GDPR.

Голландские исследователи рекомендуют пользователям не рассчитывать на соблюдение закона владельцами сайтов и позаботиться о конфиденциальности своих данных само-

1 *General Data Protection Regulation, подробнее см.* ***https://gdpr.eu/***

стоятельно. В частности, чтобы воспрепятствовать установке куки, они советуют устанавливать блокировщики рекламы.

В 2020 году вступил в силу Калифорнийский закон о защите персональных данных интернет-пользователей (California Consumer Privacy Act, CCPA), который называют самым жестким из всех подобных. Поскольку именно в Калифорнии расположены штаб-квартиры многих ведущих ИТ-компаний (Google, Apple, Netflix и др.), закон может оказать очень сильное влияние на всю интернет-индустрию.

Внимание! Даже если вы будете использовать прокси-анонимайзер или VPN, через куки-файлы информация о вас может быть передана на сервер, к которому вы будете обращаться. Поэтому перед настройкой браузера на работу через прокси или до смены используемого прокси-сервера необходимо обязательно выполнить их очистку.

При посещении нового сайта, который следует политике GDPR и просит вашего информированного согласия на установку cookies, прежде, чем согласиться, посмотрите список того, что они собираются установить. Обычно для этого есть специальная кнопка во всплывающем окне. Выбирайте только необходимые cookies, а от всех прочих можно отказаться.

С глаз долой, из браузера вон, или Блокировка рекламы

Обилие рекламы обычно раздражает людей. Она отвлекает внимание, занимает место на экране. Она маскируется под обычный

контент: броские заголовки якобы новостей на самом деле ведут на рекламные «помойки», где, кроме кричащих баннеров, ничего нет. Конечно, нормальному человеку хочется от всего этого избавиться, «развидеть», как говорят в интернете, и уж тем более убрать это подальше от детских глаз, ибо неизвестно, что в следующую секунду всплывет.

> *К сожалению, сегодня экономика мирового интернета устроена так, что провайдеры не могут отказаться от рекламы на сайтах или хотя бы существенно уменьшить ее объем. Просмотр рекламы — это часть сделки, которую мы заключаем.*

В обмен нам дают бесплатный поиск, почту, мессенджеры и соцсети, бездонное количество видео и музыки (это не про пиратов, это про легальный контент), облачные хранилища для наших фото и многое другое. Чтобы все это работало, кто-то должен заплатить. Весьма существенную часть бюджета провайдеров бесплатных сервисов, как ни крути, составляет реклама.

И это была бы честная сделка, если бы наше участие ограничивалось только просмотром. К тому же, иногда реклама и полезна. Но рекламщики сами первыми нарушили негласное соглашение, унаследованное от бумажной прессы и ТВ, — когда они показывают, мы смотрим и ничего больше. Рекламные компании научились собирать данные пользователей с помощью куки и других методов, и стали торговать ими. А такого уговора не было. Поэтому пользователи стали защищаться от чрезмерного вторжения в свою частную жизнь.

Что есть лучшая защита от назойливого продавца? Полная анонимность.

Что есть лучшая защита от назойливого продавца? Полная анонимность. Если продавец не знает, сколько денег у вас в кармане, он и напрягаться не станет. Он лучше подождет более платежеспособного клиента, поэтому главная задача правильного блокировщика рекламы не в том, чтобы скрыть от ваших глаз раздражающие картинки, а в том, чтобы не допустить в ваш браузер куки от рекламных сайтов и препятствовать другим техникам сбора личных данных.

Самые первые блокировщики имели в основе другой принцип: они скрывали от глаз пользователя рекламные элементы, которые уже были загружены на страницу. Современные же устроены гораздо сложнее. Например, они не блокируют все подряд всплывающие окна, а умеют определять, когда такое окно содержит рекламу, а когда оно необходимо для работы сайта. Как водится, если есть спрос, есть и предложение — существует большое количество блокировщиков рекламы, различающихся по возможностям настройки, платных и бесплатных, и у каждого есть свои плюсы и минусы, так что очень сложно дать на их счет однозначные рекомендации.

Современные блокировщики умеют определять, когда всплывающее окно содержит рекламу, а когда оно необходимо для работы сайта.

При поиске лучших бесплатных блокировщиков рекламы можно ориентироваться на следующие критерии:

- доступен бесплатно, без платного доступа к важным функциям;
- имеет хорошие пользовательские рейтинги;

- не требуется учетная запись для использования;
- недавно обновлен (за последние 12 месяцев);
- легко доступен в качестве плагина как минимум для одного браузера или операционной системы;
- блокирует «показы рекламы» (всплывающие окна, баннеры, видео, статические изображения, обои, текстовые объявления);
- блокирует потоковые видеообъявления (например, на YouTube).

Единого общепризнанного рейтинга блокировщиков рекламы нет, придется побыть немного самому себе аналитиком и выбрать подходящее решение, а может быть, и несколько — для разных браузеров и разных задач. Только обязательно загляните в настройки своего блокировщика, потому что далеко не всегда все нужное по умолчанию включено, придется поработать руками.

Относительно недавно в эту игру включились и сами разработчики популярных браузеров (Chrome, Firefox, Opera, Microsoft Edge) — сегодня их актуальные версии обзавелись встроенными функциями блокировки рекламы. Они тоже отличаются по своим качествам, и придется сравнивать их со специализированными решениями, которые пока сдаваться не планируют.

Эксперты высказывают сомнения, что встроенные блокировщики будут последовательно стоять на стороне пользователя. Например, говорят, что браузер Chrome, в котором эта функция

стала доступна во всех странах только с июля 2019 года, борется лишь с той рекламой, которая не соответствует стандартам, принятым Coalition for Better Ads. Фактически это означает, что встроенный блокировщик борется только с наиболее агрессивной и навязчивой рекламой, которая нарушает следующие правила:

- реклама со звуком и видеоролики, которые начинают проигрываться автоматически;
- всплывающие сообщения, закрывающие большую часть экрана;
- так называемая prestitial-реклама. Этим термином обозначают рекламу, которая имеет собственную страницу и загружается перед целевым URL, а затем пользователю демонстрируют таймер, отсчитывающий время до закрытия навязчивого объявления;
- крупные баннеры, «прилепленные» поверх окна и занимающие до 30% экрана;
- для мобильных версий сайтов не поощряется «мигающая» реклама, цвета или фон которой быстро и агрессивно меняются, пытаясь привлечь внимание и тем самым затрудняя чтение.

Тем не менее, базовый уровень защиты от рекламы и отслеживания браузеры сегодня обеспечивают. Не забудьте только их обновить и включить функцию блокировки.

«Тренд на анонимность — не новое явление для рынка, но в последнее время оно получило наибольший размах и рискует сохраниться», — печалятся мастера навязчивой онлайн-рекламы,

но сдаваться не собираются. Если нельзя будет использовать куки, то у них наготове уже есть технология следующего поколения, против которой известные технические способы защиты пока бессильны, а законодательные ограничения еще не придуманы.

Когда быть уникальным плохо: цифровой отпечаток браузера

Психологи любят говорить, что каждый человек — уникальная личность, и, как снежинки не похожи одна на другую, так и люди наделены уникальными внешними данными и обладают уникальным внутренним миром. Педагоги твердят, что каждый ребенок уникален, и к каждому нужен индивидуальный подход. Инвесторы ищут уникальные стартапы, способные изменить мир. Сколько раз я повторил слово «уникальный»? Все просто одержимы уникальностью!

Абсолютно одинаковых браузеров не существует. Точнее, они одинаковы, пока ими не начали пользоваться.

Оказалось, что браузеры тоже подвержены этому глобальному тренду — абсолютно одинаковых практически не существует. Точнее говоря, браузеры одинаковы, пока ими не начали пользоваться. Как только браузер устанавливается на конкретный компьютер, он тут же получает целый букет уникальных параметров — тип и версия операционной системы, модель устройства, язык, часовой пояс, характеристики экрана, комплект шрифтов, установленные расширения и разнообразные настройки, о которых вы, скорее всего, и не помните.

Это может показаться удивительным, но, тем не менее, факт: по комбинации нескольких параметров можно идентифицировать конкретный браузер с точностью, превышающей 99%.

На этом свойстве основана технология Browser Fingerprint[1] — «отпечатков пальцев» браузера, получившая широкое распространение после начала гонений на cookies.

Тем, кто не слишком любит математику, сейчас будет немного больно, но ничего не поделаешь — в основе метода браузерной дактилоскопии лежит математическая теория. Вы можете пропустить это объяснение и просто поверить на слово: очень вероятно, что ваш браузер уникален, что позволяет вас идентифицировать вне зависимости от наличия cookies и VPN.

Принцип метода браузерной дактилоскопии нам объяснит Питер Экерсли (Peter Eckersley), директор по исследованиям в Electronic Frontier Foundation (**eff.org**).

«Давайте начнем не с браузеров, а с людей, так будет понятнее. Представьте, что вам нужно установить личность человека, а единственное, что вы о нем знаете, это почтовый индекс, дата рождения или пол. Очевидно, что каждого из этих признаков, взятых по отдельности, будет недостаточно для идентификации.

---

1 *Фингерпринт, или «отпечаток компьютера» (браузера) — информация, собранная об удаленном устройстве для дальнейшей идентификации. Отпечатки могут быть использованы полностью или частично для идентификации, даже когда cookie выключены («Википедия»).*

Существует математическая величина, которая позволяет нам измерить, насколько данный критерий близок к полному раскрытию чьей-либо личности. Эта величина называется ***энтропией****, и ее часто измеряют в битах. Можно сказать, что энтропия — это обобщение числа различных возможностей для случайной величины: если есть две возможности, есть 1 бит энтропии; если есть четыре возможности, есть 2 бита энтропии и т.д. Добавление еще одного бита энтропии удваивает число возможностей.*

Поскольку на планете насчитывается около 7 миллиардов человек, личность случайного, неизвестного человека определяется чуть менее 33 битами энтропии (2^{33} примерно равно 8 миллиардам). Когда мы узнаем новый факт о человеке, этот факт уменьшает энтропию его личности на определенную величину. Есть формула, чтобы сказать, на сколько:

$\Delta S = -\log_2 Pr(X = x)$,

где ΔS — уменьшение энтропии, измеренное в битах, а $Pr(X = x)$ — вероятность того, что этот факт будет правдой для случайного человека. Легко догадаться, что знание пола сокращает энтропию на 1 бит, если считать, что мужчин и женщин на планете поровну. А день рождения? Применим нашу формулу и получим:

$\Delta S = -\log_2 Pr(\text{День рождения}) = -\log_2 (1/365) = 8{,}51$ *бит информации.*

То есть чем выше значение энтропии, тем более данный признак ценен для раскрытия личности. Для повышения точности при расчете вероятности надо учитывать реальную статистику.

Как известно, рождаемость неравномерна — заметно больше детей появляется на свет в сентябре, в аккурат через девять месяцев после новогодних праздников. И очень редко встречается день рождения 1 и 2 января — просто потому, что это выходной, и часто родившихся в праздники младенцев записывают следующим днем. Соответственно, сокращение энтропии нужно рассчитывать для каждой конкретной даты. Аналогично и с местом жительства: знание того, что человек живет в Москве, сокращает энтропию на 9,3 бита, а если он живет в Беверли Хиллз, то на 18,21 бита.

Таким образом, комбинация нескольких вполне обезличенных признаков может абсолютно точно указать на единственного человека. Например, если мы узнаем, что в небольшом поселке у кого-то день рождения 29 февраля (самая редкая дата), то, вполне возможно, он будет единственным. А если среди членов экипажа МКС есть только одна женщина, то этот признак становится на 100% идентифицирующим[1].

Теперь вернемся к нашим браузерам. Предположим, что есть один миллион пользователей. У 60% из них установлен Chrome, у 40% — Firefox. (Это теоретическое допущение довольно близко к правде, доля остальных браузеров невелика.) То есть мы разделили нашу выборку на две группы. Затем давайте посмотрим, какая версия браузера стоит у каждого. Для простоты будем считать, что есть три версии Firefox — тогда вторая группа делится на три подгруппы по, скажем, 15%, 15% и 10%. Эти группы все еще слишком большие, чтобы идентифицировать

1 *Peter Eckersley. A Primer on Information Theory and Privacy. // EFF.ogg, 26 января 2010.*

конкретного пользователя. Дальше посмотрим, какой у них размер экрана, часовой пояс, язык и так далее — наша выборка будет дробиться на все более мелкие группы.

*В исследовании, организованном Electronic Frontier Foundation в 2010 году, на специально созданном сайте Panopticlick (**https://panopticlick.eff.org**) было собрано более 470 тысяч цифровых отпечатков браузеров. Когда их проанализировали, то обнаружили, что в распределении отпечатков содержится, по крайней мере, 18,1 бит энтропии, а это означает, что для любого взятого наугад браузера вероятность того, что он совпадет с каким-то другим, равна 1/286 777. То есть 83,6% имели уникальный отпечаток. Среди браузеров с поддержкой Flash или Java ситуация даже хуже: 94,2% были уникальными[1]. (Вы и сейчас можете зайти на этот сайт и проверить свой браузер на уникальность.)*

Однако, 94,2% — это еще не 100%. Такая точность недостаточна, чтобы однозначно утверждать, что перед нами тот самый пользователь, который посещал сайт пару дней назад. Это, как если бы вы пытались кому-то позвонить, зная только код оператора и пытаясь набрать остальные цифры наугад. Для целей рекламы такая погрешность в принципе приемлема — подумаешь, миллионом показов больше или меньше. Казалось бы, беспокоиться не о чем, и ваша анонимность будет сохранена.

Как бы не так! Беда пришла, откуда не ждали. Вы же хотели, чтобы картинки и трехмерные изображения в браузере отрисовывались быстро и в хорошем качестве? Хотели наслаждаться дизайнерской

1 *Peter Eckersley. «How Unique Is Your Web Browser?» // Panopticlick.eff.org 2010* ***https://panopticlick.eff.org/static/browser-uniqueness.pdf***

графикой, визуальными эффектами и играть в динамичные игры, да? Для этого программисты придумали технологии WebGL и Canvas. Но чтобы порадовать вас сочной картинкой и мгновенной сменой кадров, им пришлось обращаться к низкоуровневым функциям вашего ноутбука или телефона. И тут вскрылась любопытная вещь: из-за особенностей оборудования отрисовка одних и тех же элементов происходит на разных моделях чуть-чуть по-разному — на глаз незаметно, но если взять битовый образ, то отличия легко зафиксировать. Чем не преминули воспользоваться разработчики: они тут же добавили анализ Canvas и WebGL в отпечаток браузера, и точность сразу повысилась до 99%.

В 2013 году проект исследователей INRIA (Французский национальный исследовательский институт цифровых наук) получил в целом аналогичные результаты на еще большей выборке. Ознакомиться с результатами исследования и проверить свою уникальность можно на сайте с говорящим названием «Am I Unique?» — «Уникален ли я?» (**https://amiunique.org/**). В отличие от предыдущего исследования EFF, во французском проекте задействованы новейшие технологии определения отпечатка по особенностям графики, и данные постоянно обновляются.

В отличие от отпечатка пальца, который неизменен всю жизнь, отпечаток браузера есть вещь изменчивая.

Временной фактор вообще очень важен — выходят обновления браузеров и операционных систем, люди меняют телефоны на новые модели, изменяется начинка компьютеров и прочее. То есть в отличие от обычного нашего отпечатка пальца, который неизменен всю жизнь, отпечаток браузера есть вещь изменчивая по своей природе. Как же в таком случае с его помощью можно кого-то идентифицировать? Очень просто: вы же узнаете вашего

приятеля, если он отпустил бороду, не так ли? Параметры браузера не меняются все сразу, а к небольшим изменениям можно адаптироваться — разработчики научились их учитывать. Это значит, что если изменения будут происходить постепенно, как это бывает в реальной жизни, вас все равно отследят.

Вы, конечно, можете попытаться поставить новый браузер и работать через него. Но и на эту хитрость уже есть ответ. Программисты подумали хорошенько и решили, что, собственно, браузер не так уж и необходим для отслеживания вас в интернете. Для этого достаточно знания параметров операционной системы и оборудования — прежде всего, процессора и графической карты. Так в 2017 году появилась кросс-браузерная дактилоскопия (Cross-Browser Fingerprinting — CBF), и техники CBF позволяют точно идентифицировать 99,24% всех компьютеров и смартфонов. Исследователи проводили тесты с использованием браузеров Chrome, Firefox, Edge, IE, Opera, Safari, Maxthon, UC Browser и Coconut[1].

Сам браузер не так уж необходим для отслеживания вас в интернете — достаточно знать параметры операционной системы и оборудования.

Наверное, здесь стоит остановиться и сказать о полезных применениях технологии браузерной дактилоскопии, прежде чем перейти к обсуждению методов защиты от нее. Ведь не только же ради показов рекламы все делается!

Действительно, отпечатки браузера широко используются в системах обнаружения мошенничества. Всякий раз, когда вы

1 *(Cross-)Browser Fingerprinting via OS and Hardware Level Features. // Yinzhicao.org, 2017. В более простом изложении — «Фингерпринтинг конкретного ПК с точностью 99,24%: не спасает даже смена браузера» // Habr.com, 14 января 2017.*

заходите в соцсеть с нового устройства, срабатывает двухфакторная аутентификация, а на почту приходит письмо с просьбой подтвердить, что это были именно вы. Это делается как раз на основе определения браузера. Аналогичным образом поступают банки и интернет-магазины (те, которые заботятся о безопасности). Еще эта технология применяется в игровой индустрии, чтобы обнаруживать попытки игроков «хакнуть» игру, в СМИ — чтобы контролировать пользование платными подписками, а также при продаже билетов, бронировании гостиниц и других операциях пользователя, требующих особого контроля.

> *Зачем все это сайту, который вы хотите просто посмотреть? Затем, чтобы сформировать страницу, которая будет правильно отображаться на вашем устройстве, будь то телефон или компьютер. То есть чтобы лучше вас обслужить.*

Конечно, у этой технологии есть и темная сторона. В течение нескольких лет цифровые отпечатки браузеров были подарком для поставщиков рекламы, которые отслеживали посетителей своих сайтов независимо от того, установлен следящий cookie-файл или нет. Пользуются браузерными отпечатками и вирусописатели. В 2016 году в ходе кампании по распространению вредоносного ПО для Mac OS у исследователей возникло подозрение, что злоумышленники идентифицируют цели с помощью цифровых отпечатков браузера[1].

Поэтому желание пользователей избежать слежки, осуществляемой с помощью этого механизма, вполне объяснимо. Но тут нас

---

1 *Firefox перестанет оставлять свои отпечатки на сайтах. // **TreatPost.ru**, 2 ноября 2017. Scareware Campaign Targets Mac OS X Machines. // **TreatPost.com**, 5 февраля 2016.*

поджидает парадокс, на который обратил внимание еще Петер Экерсли в статье 2010 года: чем больше вы стараетесь защититься от снятия отпечатков браузера, тем более уникальным вы становитесь, и тем легче вас обнаружить.

Чем больше вы стараетесь защититься от снятия отпечатков браузера, тем более уникальным вы становитесь, и тем легче вас обнаружить.

Профессиональные разведчики (как, впрочем, и преступники) знают, что уникальность — худший враг анонимности. Чтобы остаться неузнанным, нужно слиться с толпой, выглядеть самым средним и заурядным представителем народных масс. Одеваться неброско, вести себя как все, и тогда, может быть, удастся уйти от слежки. Но главное в стремлении стать незаметным — не переусердствовать.

> *Основной метод маскировки заключается в придании своему отпечатку максимально средних значений. Используйте популярные браузеры с настройками по умолчанию, не меняйте шрифты и язык, не ставьте разнообразных плагинов — в общем, будьте как все.*

Отдельно надо позаботиться о параметрах, снимаемых с помощью анализа вашей графической системы, поскольку настройками изменить вы их не можете. Сразу надо сказать, что идея поставить блокировщик отпечатков Canvas так себе — наличие блокировщика делает вас похожим на человека, стоящего среди толпы в маске. Никто точно не знает, кто вы, но вы единственный, кто носит маску, так что вас могут опознать. А если таких, как вы, несколько, вас немедленно сгруппируют как «людей в масках». Даже блокировщиками рекламы пользуются всего 5-10% пользователей — на их фоне ваш блокировщик отпечатков будет выглядеть вообще экзотикой.

Есть браузерные расширения, которые умеют подменять ваш истинный отпечаток на некий фиктивный. С этим тоже надо быть осторожным — нормальный человек не будет переодеваться на ходу, а частая смена отпечатка именно так и выглядит для наблюдателя. Если вы все-таки настроены заметать следы, то можно воспользоваться расширением для браузера Canvas Defender (или аналогичным), которое вы найдете в магазине приложений.

Нормальный человек не будет переодеваться на ходу, а частая смена отпечатка именно так и выглядит для наблюдателя.

Хотя сегодняшние методы не дают надежной защиты от снятия сайтами отпечатков вашего браузера, аргумент «защита от дактилоскопии бесполезна» — пример пораженческого поведения. Сталкиваясь с наплывом плохих новостей о возможностях слежки, мы проявляем склонность к выученной беспомощности и приходим к упрощенному выводу, что конфиденциальность умирает, и мы ничего не можем с этим поделать.

Однако такая позиция не подтверждается историческими свидетельствами: вместо этого мы видим постоянный пересмотр равновесия конфиденциальности и отслеживания. И хотя нарушения, затрагивающие право на тайну частной жизни, случаются постоянно, время от времени они компенсируются юридическими, технологическими и социальными механизмами.

Отпечатки браузера сегодня остаются на переднем крае битвы за конфиденциальность. GDPR усложняет их использование, приравнивая отпечаток к персональным данным. Поставщики браузеров также стали серьезно относиться к этой практике и вводят ограничения на ее использование.

В обоих упомянутых нами исследованиях опубликованы замечательные научные данные. Но время не стоит на месте, технологии развиваются, и старые гипотезы нужно регулярно проверять, чтобы подтвердить их или опровергнуть. Поэтому в 2018 году выпускник университета Братиславы провел новое исследование реальных возможностей идентификации по отпечатку браузера. Было собрано более 500 тысяч отпечатков, но, в отличие от прошлых исследований, 65% устройств составляли смартфоны — примерно пополам iPhone и Android.

Согласно полученным данным:

- *74% настольных устройств могут быть однозначно идентифицированы, в то время как то же самое можно сказать только о 45% мобильных пользователей;*
- *Только 33% отпечатков браузера, собранных на iPhone, были уникальными;*
- *Остальные 33% айфонов вряд ли можно отследить вообще, потому что 20 или более айфонов показывают тот же отпечаток браузера.*

Новые результаты кардинально отличаются от известных ранее — о точности свыше 99% речь не идет. То есть для гарантированной идентификации пользователя технология отпечатков браузера пока не доросла. Особенно интересно, что смартфоны Apple гораздо сильнее похожи друг на друга, чем устройства остальных типов, что является следствием высокого уровня стандартизации устройств и ограниченности модельного ряда.

В итоге можно сказать, что отпечатки браузера идеально подходят для таких случаев использования, как персонализация рекламы (где точность не является особо важной) или предотвращение банковского мошенничества (где паранойя вполне уместна)[1].

Срывание всех и всяческих масок: деанонимизация

Говоря формальным языком, деанонимизацией называется лишение человека анонимности, то есть установление связи между действиями пользователя на интернет-ресурсах и конкретной личностью. Естественно, власть всеми ветвями за деанонимизацию и достаточно продвинулась на этом пути, принимая все новые законы.

Плохо ли это? Ведь в отсутствие анонимности любого обидчика будет легко найти и выяснить отношения в офлайне, а полиция быстро вычислит и поймает любого преступника. В идеальном мире, наверное, так и было бы, но в реальном все не столь однозначно, и анонимность часто является главным залогом безопасности.

В реальном мире анонимность часто является главным залогом безопасности.

Посмотрим, какие последствия имела или могла бы иметь деанонимизация на примере трех историй. В двух из них анонимность была раскрыта, в третьей — нет.

---

1 *Peter Hraška. We've analysed 500,000 browser fingerprints. Here is what we found. // **Medium.com**, блог Slido, 7 февраля 2019.*

История первая

WikiLeaks — созданная в 2006 году международная некоммерческая организация, которая публикует утечки документов из государственных и коммерческих организаций, предоставленные анонимными источниками. До сентября 2018 года ее возглавлял австралийский интернет-активист Джулиан Ассанж. На счету организации много громких публикаций, вызвавших международные скандалы. Среди них материалы о коррупции в Кении, о содержании заключенных на американской базе в Гуантанамо, о незаконной деятельности швейцарского банка Julius Baer, секретные «библии» саентологии, список членов ультраправой Британской национальной партии и другие. Но настоящей бомбой стала публикация секретных документов Пентагона, касающихся войн в Ираке и Афганистане, — в частности, видео авиаудара по Багдаду, в результате которого погибли два журналиста Reuters (пилоты по ошибке приняли их видеокамеры за оружие).

WikiLeaks провозглашала в качестве одного из своих принципов обеспечение полной анонимности для информаторов и утверждала, что сайт организации обладает пуленепробиваемой защитой, однако утечка все же произошла. Чья-то глупая ошибка — список адресов всех доноров WikiLeaks в почтовой рассылке был случайно подставлен в поле CC (копия) вместо BCC (скрытая копия). Одним из якобы доноров был Адриан Ломо — хакер, работавший на правительство США, который тоже получил полный список. И он не упустил свой шанс — вычислил информатора, который слил секретные документы, вступил с ним в личную переписку в чате и спровоцировал назвать свое имя и рассказать о том, что тот сделал. Снова социальная инженерия, ничего больше!

Информатором оказался военнослужащий армии США Брэдли Мэннинг, которого осудили на 35 лет. (Позже президент Обама его помиловал, и он вышел на свободу после 7-летнего заключения, правда, уже как Челси Мэннинг — за время пребывания в тюрьме он сменил пол.)

Объем материалов, добытых Мэннингом, был огромен. Только в «Афганском архиве» было 92 тысячи документов. Конечно, общественность должна была узнать правду о войне, но многие из этих документов содержали персональные данные агентов, и после публикации архива их жизнь оказалась бы под угрозой. Несмотря на мнение своих товарищей, считавших, что документы надо обезличить, Ассанж единолично решил обнародовать весь архив как есть. «Мы не редактируем документы», — заявил он. Этот поспешный жест привел к тому, что многие из афганцев, сотрудничавших с силами антитеррористической коалиции, были казнены талибами.

Мораль этой истории:

- Будьте осторожны с электронной почтой. Довольно частая ошибка, когда секретные списки адресов случайно улетают всем;

- Будьте осторожнее с чужими тайнами. Ваши действия могут деанонимизировать других людей. Пусть это не всегда вопрос жизни и смерти, но готовы ли вы взять на себя ответственность за возможные последствия?;

- Опасайтесь социальной инженерии. В интернете этот риск выше, чем в офлайне.

История вторая

В качестве еще одного яркого примера можно привести историю с нашумевшим стартапом Find Face. Эта компания прославилась тем, что без дополнительного уведомления скачала базу фотографий всех пользователей социальной сети «ВКонтакте», что позволило ей идентифицировать буквально любого человека на улице, если в его профиле «ВКонтакте» есть фото подходящего качества. Сервис приобрел вирусную популярность после того, как петербургский фотограф Егор Цветков запустил свой фотопроект, в рамках которого находил в соцсетях профили встреченных им в метро людей. «Таким образом, я узнавал многое о жизни человека, не вступая в личный контакт, и мог сопоставить реальный образ с интернет-репрезентацией», — говорил фотограф. В принципе, это был безобидный арт-проект, ничего более.

Затем пользователи имиджборда «Двач» стали использовать Find Face для деанонимизации порноактрис. Этот кейс оказался потенциально куда более опасным: он вылился в травлю и шантаж девушек, которые действительно снимались, или могли оказаться просто похожими на героинь фильмов для взрослых. Пока шантажисты и хипстеры развлекались как могли, сами владельцы проекта делали деньги, занимаясь фактически шантажом, — требуя 459 рублей ежемесячно за возможность удалиться из поисковой выдачи сервиса.

В сентябре 2018 года общедоступный «бесплатный» сервис Find Face был закрыт, потому что компания-собственник переключилась на обслуживание заказов крупного бизнеса и государства. Но свято место пусто не бывает: в феврале 2019 года открылся Search Face —

новый сервис для поиска людей в VK по фото, аналогичный закрытому Find Face и запущенный неизвестными разработчиками.

Мораль этой истории:

- Технология распознавания лиц — очень опасная штука в руках безответственных людей с размытыми этическими принципами. Семь раз подумайте, прежде чем оставить где-то свое фото, кроме своей страницы в соцсети;

- И еще более основательно подумайте, прежде чем постить фото других людей без их явного согласия. Эффекты могут быть самые неожиданные.

История третья

Наверное, нет человека, который бы не слышал про биткойн и его загадочного создателя Сатоши Накамото. Вот уже десять лет мир будоражит криптолихорадка, а ее «виновника» никто в глаза не видел. В октябре 2008 года Накамото опубликовал статью, описывающую протокол биткойна, а 3 января 2009 года начала работать сеть, и был сгенерирован первый блок и первые 50 биткойнов.

Все это время изобретателю криптовалюты удается сохранить анонимность, несмотря на отчаянные попытки его найти. Его ищут криптоэнтузиасты, которые хотят не иначе как лично воздать ему хвалу. Наверное, не меньше почитателей заинтересованы в деанонимизации отца-основателя биткойна и спецслужбы — старый финансовый мир чувствует в криптовалюте угрозу доллару, а вызвать на ковер в Конгресс и пропесочить как следует некого, — как прикажете сражаться с пустотой?

Последнее сообщение от Сатоши датируется 23 апреля 2011 года, оно было адресовано разработчику Майку Херну: «Я сейчас занят другими проектами. Дело остается в надежных руках, есть Гэвин [Андресен] и все остальные». Сатоши всегда выходил в интернет, используя сеть Tor и прочие средства, которые обеспечивали анонимность. В своем профиле на сайте P2P Foundation он указал, что родился в 1975 году и живет в Японии, хотя, скорее всего, это легенда, и человек, пользующийся этим псевдонимом, не японец: он пишет на английском языке как на родном.

«Охота» на Сатоши идет давно, но безуспешно. Программист из Швейцарии Штефан Томас обнаружил, что между 05:00 и 11:00 (GMT) Накамото никогда ничего не публиковал. Это касалось, в том числе, и выходных. Так Томас предположил, что Накамото проживает в Великобритании. В пользу этой версии говорили и особенности почти идеального английского языка создателя биткойна — он часто использовал слова вроде «bloody», «optimise» или «colour», что свойственно именно британцам. Другие «охотники» уверены, что это лишь маскировка. Многие вообще считают, что это не один человек, а группа людей.

За это время кого только ни подозревали в том, что он и есть создатель «битка»! Однако все «кандидаты» категорически отвергли такие предположения. В 2014 году журналисты нашли американца японского происхождения по имени Дориан Сатоши Накамото, проживающего в Калифорнии. Уже тогда ему было 64 года, и он наотрез отказывался общаться с прессой, но это снова оказался не настоящий Сатоши. Были, наоборот, самозванцы, объявлявшие себя Сатоши Накамото, однако убедить сообщество в собственной подлинности они не смогли.

В каком-то смысле исчезновение Сатоши — лучшее, что произошло с первой криптовалютой за всю ее историю, поскольку оно автоматически решило проблему возникновения культа личности.

Мораль этой истории чрезвычайно проста:

- Если очень постараться, то свою анонимность можно сохранить, несмотря на активные действия людей, желающих вас найти. Будь как Сатоши!

Анонимность — не только ваше личное дело. От вашего умения соблюдать правила безопасного поведения в интернете может зависеть безопасность других людей. Иногда сохранение инкогнито становится жизненно важным. Об этом надо помнить также, как о правилах оказания первой медицинской помощи, — может быть, вам никогда не придется делать кому-то искусственное дыхание и массаж сердца, но лучше на всякий случай это уметь. Также и с анонимностью в интернете: в повседневной жизни параноиком быть ни к чему, но владеть хотя бы базовыми приемами маскировки — полезно. Или, по меньшей мере, знать об их существовании.

«Луковый» браузер Tor для повышения анонимности

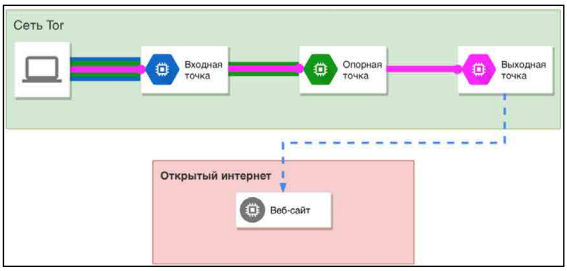
Когда речь заходит о действительно высоком уровне анонимности, то продвинутые в таких делах пользователи непременно вспоминают про браузер Tor. Его название никак не связано со скандинавским богом Тором и героем «Мстителей», не имеет оно ничего общего

и с геометрической фигурой в форме баранки. На самом деле, это сокращение от «The Onion Router» — «луковый маршрутизатор».

Причем здесь лук, спросите вы? Притом, что кроме браузера, который видит пользователь, есть еще сеть Tor Network, состоящая из нескольких тысяч серверов, раскиданных по миру. Она, собственно, и обеспечивает анонимность — ваш Tor-браузер не напрямую выходит в интернет, а через несколько ее узлов. По умолчанию через три, но узлов может быть и больше, чтобы запутать следы.

> *Для каждой страницы, которую вы намерены посетить, случайным образом формируется своя цепь узлов, причем сами узлы об этом не знают, их адреса берутся из каталога сети. Затем клиент сети Tor (в составе вашего браузера) готовит «луковый» пакет, то есть многократно шифрует исходное сообщение таким образом, что первый узел в цепи может расшифровать только верхний слой, после чего он узнает адрес следующего узла и передает пакет ему. Тот расшифровывает второй слой, видит адрес очередного получателя и передает оставшийся пакет дальше. Каждый узел видит только своих соседей, но не знает ни исходного отправителя, ни конечного получателя, ни длины цепи. Последний узел также выполняет расшифровку и в итоге передает ваше сообщение по адресу назначения в обычный интернет.*

Если все это нарисовать, то получится похоже на луковицу: каждый узел как бы снимает один ее слой, пока последний не доберется до сердцевины. Отсюда и название. Сам же браузер Tor является просто защищенной версией Firefox. Он включает в себя многочисленные модификации конфиденциальности и безопасности, встроенные в версию по умолчанию.



Если вы сейчас подумали, не стоит ли использовать совместно VPN и Tor, то вы на правильном пути. Действительно, эти методы дополняют друг друга, и эксперты именно так рекомендуют поступать, ибо у обоих способов есть свои сильные и слабые стороны.

VPN прячет вас от местного интернет-провайдера и оберегает от хакеров, способных перехватить ваши данные при работе в публичной сети, — например, если вам пришлось воспользоваться wi-fi. Но при этом самому провайдеру VPN ваши данные могут быть доступны. Как кто-то сказал: «Ни один провайдер VPN не собирается отправляться в тюрьму, чтобы защитить подписчика, приносящего 20 долларов в месяц», — и это правда.

Tor хорош в обеспечении анонимности, но ваш локальный интернет-провайдер может счесть трафик подозрительным и блокировать его. К тому же в Tor'е все-таки есть уязвимости: например, может быть скомпрометирован выходной узел. То есть кто-то может сидеть там и читать весь ваш трафик — пароли, явки, адреса, любовные послания, планы по захвату мира и все прочее. В основном Tor'ом управляют ответственные люди, но такие истории случались.

Если использовать VPN и Tor совместно, то эти риски можно снизить. Сначала запускаете VPN, потом через Tor обращаетесь к нужному сайту. Ваш локальный интернет-провайдер в этом случае видит только подключение к VPN, но не видит, что вы используете Tor. Затем сервер VPN на другом конце туннеля отправляет ваши зашифрованные данные первому узлу Tor, который, однако, не знает вашего настоящего местоположения и IP. А тот уже по цепочке передает запрос нужному сайту. То есть ваш провайдер VPN видит, что вы используете Tor, но не знает, куда и зачем вы обращаетесь по сети.

Из минусов этой схемы можно назвать только замедление работы, но с безопасностью всегда так[1].

Сложилось мнение, что Tor'ом пользуются в основном хакеры и преступные элементы, что там процветает торговля оружием и наркотиками, детская порнография и экстремизм, и что нормальному человеку там делать нечего. Это мнение подогревается не слишком компетентными публикациями в СМИ, в которых Tor прочно ассоциируется с даркнетом[2] — темной стороной интернета. В ответ на это можно только еще раз повторить: проблема не в технологиях, а в людях. Tor — это технология обеспечения анонимности, а уже люди ее используют в разных целях.

Tor — технология обеспечения анонимности, а уже люди используют ее в разных целях.

1 *Tor vs. VPN — A 2020 Comparison. // **Blokt.com**, 11 июня 2020.*

2 *Даркнет (англ. DarkNet) — это собирательное название компьютерных сетей, предназначенных для анонимной передачи информации. Там тоже есть сервисы для торговли, общения и обмена контентом, но их нельзя открыть через стандартный браузер или найти в обычном поисковике.*

Например, на основе Tor реализован проект Secure Drop — платформа для безопасной коммуникации журналистов с их информаторами, желающими сохранить анонимность. По сути, проект продолжает дело, начатое WikiLeaks. Этой платформой пользуются многие уважаемые издания — Forbes, The New Yorker, The Guardian, Associated Press, Bloomberg, The Wall Street Journal, Aftenposten и другие.

> *Неправительственные организации пользуются сетью Tor, чтобы их сотрудники могли посещать веб-сайт организации во время пребывания в чужой стране, не оповещая при этом всех вокруг о том, что они к ней принадлежат.*
>
> *Частные лица пользуются Tor'ом для того, чтобы сайты не отслеживали их активность в Сети, или чтобы подсоединяться к новостным сайтам, сервисам мгновенных сообщений и прочим подобным услугам, заблокированным местными интернет-провайдерами. Скрытые сервисы Tor дают пользователям возможность публиковать информацию, не раскрывая своего местонахождения. Отдельные лица также пользуются сетью Tor для обсуждения конфиденциальных тем — например, на форумах поддержки жертв изнасилования или домашнего насилия, или людей с определенными болезнями.*
>
> *Подразделение ВМФ США использует Tor для передачи разведывательной информации, в том числе с Ближнего Востока. Правоохранительные органы пользуются сетью Tor, чтобы посещать или наблюдать за веб-сайтами, не оставляя в их логах запросов с правительственных IP-адресов, а также для безопасности операций внедрения и контрольных закупок*[1].

1 *Краткий обзор Tor. // Сайт* ***pf.team.***

Когда мы говорим, что Tor — защищенный браузер, это не значит, что можно расслабиться и гулять по всем сайтам, по которым вздумается. Tor оберегает только вашу анонимность, но не может защитить вас от собственной глупости: если вы зайдете на какой-то вредоносный сайт, то точно также можете подцепить вирус или шпионское ПО, которое будет использовано для деанонимизации. Или банально для того, чтобы просто украсть у вас деньги.

Злоумышленники знают, что среди пользователей Tor много новичков, которые прибегли к нему из-за роста ограничений в интернете, изобретаемых правительствами различных стран. Злоумышленникам грех этим не воспользоваться.

Заходя в Tor, надо удвоить осторожность. И также следует быть осторожным с настройками самого Tor'а.

Значит, заходя в Tor, надо, наоборот, удвоить осторожность. И также следует быть осторожным с настройками самого Tor'а, чтобы случайно не превратить свой компьютер в выходной узел сети. В таком случае запущенный Tor-браузером ретранслятор Tor-сети может трактоваться как программа, участвующая в предоставлении доступа к запрещенным в РФ ресурсам кому-то, кроме вас, а это уже влечет ответственность по закону.

13 августа 2014 года французский студент Жюльен Вуазен обнаружил поддельный ресурс, в точности имитирующий официальный сайт The Tor Project, Inc. Через него под видом пакета Tor Browser распространялось вредоносное программное обеспечение, и похищались пожертвования пользователей. Согласно информации, которую

удалось добыть Вуазену, за созданием фальшивого сайта стояла группа хакеров из Китая[1].

В апреле 2017 года в России был арестован математик Дмитрий Богатов. Его обвинили в призывах к терроризму и организации массовых беспорядков в сообщениях, размещенных на форуме **sysadmins.ru**. *Единственной уликой против Богатова является то, что ему принадлежит IP-адрес, с которого было размещено сообщение. Богатов поддерживал на своем компьютере выходной узел сети Tor, которым мог воспользоваться любой. По словам защиты Богатова, его невиновность подтверждается записями камер наблюдения, которые доказывают, что в момент публикации он возвращался домой из магазина. Арест Богатова широко обозревался в российских СМИ и вызвал широкий интерес россиян к работе анонимайзера*[2].

Бдительный читатель обязательно должен спросить: а как у Tor'а с отпечатками браузера? Мы тут усложняем себе жизнь, громоздя Tor поверх VPN, а нас, может быть, все равно идентифицируют в два счета. Или нет? Ситуацию разъясняет Пьер Лаперди (Pierre Laperdrix), один из ключевых участников проекта **amiunique.org**.

«Tor Browser был первым браузером, который решал проблемы, связанные с дактилоскопией, еще в 2007 году, до того, как появился термин «дактилоскопия в браузере» — в Tor была добавлена функция перехвата Javascript для маскировки часового пояса.

---

1 *Закон об анонимайзерах вступил в силу. Что о нем нужно знать? // Русская служба BBC, 1 ноября 2017.*

2 *Следствие по делу Дмитрия Богатова через год было прекращено, и он уехал в США.*

Подход, выбранный разработчиками Tor, прост: все его пользователи должны иметь одинаковые отпечатки браузера. Независимо от того, какое устройство или операционную систему вы используете, отпечаток вашего браузера должен совпадать с любым устройством, на котором запущен Tor.

Кроме того, вы, возможно, задавались вопросом, почему при развертывании окна браузера появляется следующее сообщение: "Максимизация Tor Browser позволяет веб-сайтам определять размер вашего монитора, это может быть использовано для отслеживания вас. Мы рекомендуем оставить окна браузера Tor в их исходном размере по умолчанию".

Это из-за дактилоскопии. Поскольку пользователи имеют разные размеры экрана, один из способов убедиться в том, что различий не наблюдается, состоит в том, чтобы все использовали один и тот же размер окна. Если вы развернете окно браузера до максимума, ваш браузер может оказаться единственным, использующим Tor с этим конкретным разрешением, — таким образом повышается риск вашей идентификации в интернете.

На самом деле, «под капотом» было сделано еще множество доработок, призванных уменьшить различия между пользователями. Были введены резервные шрифты по умолчанию для минимизации отпечатков шрифтов. WebGL и Canvas API по умолчанию заблокированы, чтобы предотвратить скрытый сбор параметров графики. Проделано было и много другой работы[1].

1 *Browser Fingerprinting: An Introduction and the Challenges Ahead. // Блог Tor Project, 4 сентября 2019.*

По состоянию на сегодняшний день можно сказать, что Tor довольно неплохо противостоит попыткам идентификации пользователей с помощью технологии снятия цифровых отпечатков браузера. Его разработчики считают эту задачу одной из приоритетных и намерены продолжить борьбу за анонимность.

Учтите, что сказанное выше о противодействии фингерпринтингу верно при условии, что в Tor выбран наивысший уровень безопасности (Safest).

Итак, подумайте еще раз хорошенько: вам действительно нужен Tor? Пользование им выделит вас из общей массы ежедневной аудитории интернета. В мире ежедневно Tor используют 2-3 миллиона человек, среди которых из России — порядка 500 тысяч. То есть порядка 0,7% от общего числа российских пользователей. Трафик Tor заметен, а это значит, что вы сразу привлечете к себе внимание. Ради того только, чтобы получить доступ к заблокированным ресурсам. Не избыточно ли это?

Трафик Tor заметен, а это значит, что вы сразу привлечете к себе внимание.

Тем не менее, если все же по каким-то причинам Tor вам нужен, соблюдайте следующие правила:

- Никогда не входите в свои обычные аккаунты почты и соцсетей через Tor;
- Не пользуйтесь онлайн-банкингом. (Тем более что банк, скорее всего, посчитает это подозрительным и заблокирует ваш счет;)

- Используйте VPN. (Об этом уже говорили, но не лишне напомнить;)
- Никому не сообщайте никаких личных сведений, остерегайтесь «социальных инженеров»;
- Не смешивайте анонимный режим с обычным. Лучше вообще иметь для Tor отдельный компьютер или хотя бы виртуальную машину.

Контрольные вопросы

1. Как обеспечивали анонимность в реальном мире?
2. Зачем нужна анонимность в интернете? Ваши версии.
3. Что понимается под анонимностью в интернете?
4. Что такое псевдоним (в обычной жизни и в интернете)?
5. Что такое IP-адрес? Опишите своими словами.
6. Как найти человека по IP-адресу?
7. Что такое прокси?
8. Почему могут быть опасны бесплатные анонимайзеры?
9. Что такое VPN? Опишите своими словами, как это работает.

10. Что на самом деле запрещает закон о запрете анонимайзеров?

11. Что значит «ответственное поведение в интернете» и почему это важно?

12. Что такое куки и где они хранятся?

13. Чем куки опасны? Назовите два основных риска.

14. В чем слабые места позиции «мне нечего скрывать»?

15. Для чего нужен блокировщик рекламы помимо блокировки рекламы?

16. Что такое отпечаток браузера?

17. Что такое Tor?

18. С какими целями люди используют Tor?

19. Зачем использовать VPN и Tor совместно?