МРНТИ 81.93.29
УДК 002:004.056

https://doi.org/10.51889/2020-2.1728-7901.44

Т.Г. Плотникова

Алматинский филиал Санкт-Петербургского Гуманитарного университета профсоюзов, г. Алматы, Казахстан

СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

Аннотация

В настоящее время защита личных данных очень актуальна, хотя сбором и обработкой персональных сведений люди занимаются давно. Компании заявляют о конфиденциальности и обезличивании собираемых данных, но возникает вопрос, зачем собираются эти данные, насколько они защищены. Сейчас перевод различных баз данных в электронный вид упрощает не только законные манипуляции с персональными данными, но и незаконные, стало проще получить несанкционированный доступ к большому числу данных. Есть много рисков того, что персональные данные попадут к тем, у кого их не должно быть. Существуют различные способы защиты персональных данных, с помощью которых пользователи могут ограничить доступ посторонних к личным данным. В статье рассматриваются различные инструменты, которые используются для организации комплексной защиты персональных данных в сети Интернет.

Ключевые слова: интернет, персональные данные, браузер, социальные сети, шифрование, пароль.

Аңдатпа

Т.Г. Плотникова

Кәсіподақтардың Санкт-Петербург гуманитарлық университетінің Алматы филиалы, Алматы қ., Қазақстан

ИНТЕРНЕТТЕ ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ ЖОЛДАРЫ

Қазіргі уақытта жеке деректерді қорғау өте өзекті, дегенмен адамдар ұзақ уақыт бойы жеке ақпаратты жинап, өңдеп келеді. Компаниялар жиналған деректердің құпиялылығы мен анонимизациясын жариялайды, бірақ бұл мәліметтер не үшін жиналады, қанша қорғалады деген сұрақ туындайды. Енді әр түрлі мәліметтер базасын электронды түрге айналдыру жеке мәліметтермен заңды айла-шарғы жасауды ғана емес, сонымен бірге заңсыздықты да жеңілдетеді, үлкен көлемде деректерге рұқсатсыз қол жетімділікке қол жеткізілді. Жеке мәліметтер оған ие болмауы керек адамдарға жетуі мүмкін көптеген қауіптер бар. Жеке деректерді қорғаудың әртүрлі тәсілдері бар, олар арқылы пайдаланушылар бейтаныс адамдардың жеке мәліметтеріне кіруді шектей алады. Мақалада Интернеттегі жеке деректерді жан-жақты қорғауды ұйымдастыру үшін қолданылатын әртүрлі құралдар қарастырылады.

Түйін сөздер: интернет, жеке деректер, шолғыш, әлеуметтік желілер, шифрлау, пароль.

Abstract

WAYS TO PROTECT PERSONAL DATA ON THE INTERNET

Plotnikova T.G.

Alma-Ata branch of the St. Petersburg Humanitarian University of Trade Unions

Almaty, Kazakhstan

Currently, the protection of personal data is very relevant, although people have been collecting and processing personal information for a long time. Companies declare confidentiality and anonymization of the data collected, but the question arises as to why this data is collected, how much it is protected. Now the conversion of various databases into electronic form simplifies not only legal manipulations with personal data, but also illegal, it has become easier to gain unauthorized access to a large amount of data. There are many risks that personal data will reach those who should not have it. There are various ways to protect personal data, through which users can restrict the access of strangers to personal data. The article discusses various tools that are used to organize comprehensive protection of personal data on the Internet.

Keywords: Internet, personal data, browser, social networks, encryption, password.

Сервисами сети Интернет сейчас регулярно пользуется более пяти миллиардов человек во всём мире. Существует множество приложений и служб, облегчающих различные виды взаимодействия или предоставляющие полезные услуги.

В данное время существует проблема защиты персональных данных. Все компании заявляют о конфиденциальности и обезличивании собираемых данных, но возникает вопрос, зачем собираются эти данные, и насколько они защищены.Может показаться, что конфиденциальности в Интернете просто не существует, этой точке зрения способствуют и крупные утечки данных, и анализ лент социальных сетей, вездесущая реклама, отслеживающая каждый шаг пользователей в цифровом

мире. Тем не менее существуют различные способы защиты персональных данных, с помощью которых пользователи могут ограничить доступ посторонних к личным данным.

Рассмотрим, каким образом пользователь может сохранить и защитить персональные данные, используя различные инструменты.По умолчанию браузеры сохраняют на компьютере часть информации о посещаемых сайтах. Эти данные могут оставаться в кеше, где хранятся картинки и другие постоянные элементы интерфейса, которые в дальнейшем можно не загружать с сервера. В результате страницы открываются быстрее.Для запоминания данных о пользователе служат и cookie-файлы, которые среди прочего, позволяют сайтам запоминать устройство. Cookie-файлы подразделяются на основные и сторонние. Основные cookie-файлы действуют только в пределах своего сайта, записывают предпочтения пользователя на конкретном сайте и в большинстве случаев нужны для запоминания учетных записей.

Сторонние cookie-файлы этим не ограничиваются, они могут принадлежать рекламодателю, размещающему рекламные объявления на нескольких сайтах, которые посещает пользователь. Информация накапливается в базах данных, на основе которых злоумышленники составляют полный портрет пользователя, чтобы использовать его для собственной выгоды.Кроме этого, браузер сохраняет историю посещенных ресурсов.Значительную часть этой информации могут видеть механизмы онлайн-слежки. Ее используют, чтобы узнавать, какие сайты посещает пользователь, тем самым определять круг его интересов. Регулярно удаляя эти данные, можно сильно затруднить составление такого досье. Кстати, не обязательно избавляться от временных данных вручную. В большинстве браузеров можно настроить автоматическое удаление файлов cookies при каждом закрытии. Однако следует учесть, что при удалении временных данных можно лишиться и удобств, которые они дают. Особенно неприятна для многих необходимость каждый раз заново вводить логины и пароли на всех сайтах. К счастью, именно ее легко компенсировать – в этом поможет менеджер паролей.Если же надо, чтобы кое-что сайты помнили о пользователе, например поля длинной анкеты, которые же заполнили, можно выбрать более мягкие меры: запретить сайтам использовать сторонние или «следящие» куки – ту их разновидность, которая в подавляющем большинстве случаев нужна именно для слежки и не требуется ни для чего иного.

Если нужно скрыть от чужих глаз не всю историю браузера, а только отдельные сайты, можно воспользоваться режимом «инкогнито». В нем браузер не сохраняет информацию о просмотренных страницах, введенные пароли и другие данные. При этом вкладки «инкогнито» не мешают пользоваться обычными вкладками и не удаляют то, что браузер уже сохранил.

Необходимо учесть, что режим «инкогнито» не защищает от слежки на отдельных сайтах, не скроет IP-адрес для тех, у кого есть доступ к сети.Следует обратить особое внимание на выбор браузера. Браузеров сейчас немало, и у каждого подход к приватностисвой [1].

В частности, один из популярных браузеров Google Chromeсобирает самые разные данные о пользователе, даже символы, которые вводятся в адресную строку. Кроме того, в нем по умолчанию разрешены и «следящие» куки, и другие инструменты, помогающие составлять досье на пользователя. Однако не все известные браузеры придерживаются той же политики.

Например, компания Mozillaставит приватность во главу угла. Браузер Firefox по умолчанию блокирует известные трекеры (инструменты слежки, которыми пользуются сайты) в окнах «инкогнито» и позволяет включить эту опцию и для обычных сессий. Конечно, от всех возможных способов собрать информацию о пользователе это не защитит, но существенно уменьшит объем такой информации и заодно ускорит загрузку сайтов.

Кстати, у Mozilla есть отдельный приватный браузер для мобильных устройств FirefoxFocus. Он не только блокирует трекеры, но и позволяет удалить все данные о посещенных сайтах.

Браузер Safari демонстрирует сайтам обезличенную информацию о системе пользователя, делая данное устройство похожим на многие другие. Также браузер обладает набором инструментов для блокирования слежки через виджеты соцсетей на сайтах и другие трекеры.

Одним из самых защищенных от посторонних глаз браузеров считается Tor. Он представляет собой надстройку над целой сетью так называемых «луковых маршрутизаторов», которые маскируют IP-адрес и не дают сайтам определить, откуда их открывают. Каждый запрос проходит по меньшей мере через три таких маршрутизатора, при этом вплоть до последнего из них данные остаются зашифрованными. Существуют и другие браузеры, которые в той или иной мере защищают от онлайн-слежки, например EpicPrivacyBrowser, SRWareIronBrowser, Brave и Dooble. Однако стоит помнить, что чем менее популярен браузер, тем больше вероятность, что он окажется несовместим с сайтами, которые привык применять пользователь.

Даже при использовании надежного браузера за пользователем могут следить поисковые системы. Например, компании Google или Яндекс сохраняют запросы в своих архивах. Однако существуют альтернативные поисковики, не отслеживающие запросы.Самый известным из них является DuckDuckGo. Он не сохраняет запросы и данные об устройствах и не передает информацию рекламным сетям. За основу DuckDuckGo берет как собственную индексацию, так и результаты поиска более сотни различных систем, при этом не сообщая им, кто что искал.

Существуют также другие приватные поисковики, например Swisscows, Gibiru, использующие исключительно собственные алгоритмы. Поисковик StartPage, используя выдачу Google, предлагает анонимно открывать сайты из поисковой выдачи.Избавиться от слежки можно и при помощи специальных программ и расширений — например, популярного блокировщика рекламы AdBlockPlus, который заодно не дает соцсетям отслеживать действия (эту функцию нужно включить в настройках). Список блокируемых по умолчанию трекеров тоже можно дополнить.

Расширения Disconnect, uBlockorigin, Ghostery и uMatrix не требуют специальных настроек – они сразу блокируют трекеры и слежку соцсетей. Свое расширение, отключающее трекеры, есть и у разработчиков поисковика DuckDuckGo. Также сервис предлагает свой приватный браузер для мобильных устройств на Android и iOS. Пользователи Firefox могут установить расширение Facebook Container, мешающее Facebook собирать данные о пользователе на других сайтах.

Еще один способ скрыться от назойливой слежки – применять VPN-соединение, в котором при каждом подключении меняется IP-адрес. Однако стоит иметь в виду, что от информации, которую собирают социальные сети и поисковики, VPN полностью не защитит, поэтому им надо пользоваться вместе с другими инструментами.

В настоящее время пользователи активно пользуются социальными сетями, которые являются онлайн-сервисами, позволяющими создавать различные социальные связи, выстраивать структуру взаимоотношений, обмениваться информацией.

К основным особенностям социальных сетей можно отнести практически неограниченные возможности для обмена самой разнообразной информацией (текстовой, фото, видео; сервисы сообществ и микроблогов; возможность указывать место, отмечать фотографии и т.д.);формирование индивидуальных профилей с максимальным количеством личной информации (ФИО, вуз, место работы, фото и т.д.), добавление в «друзья» по принципу наличия реальной связи (друзья, знакомые, одноклассники-одногруппники, родственники и т.д.) и а также по схожести интересов (группы, сообщества и т.д.).Кроме того, сайт социальной сети предоставляет своим пользователям возможность отслеживать связи между своими единомышленниками, вступать в различные сообщества, создавать группы, открывать или закрывать для всеобщего доступа информацию своего профиля, комментировать контент, который выкладывают его «друзья» и многое другое.

Появление и развитие социальных сетей является большим технологическим достижением, имеющим огромные возможности. Пользователи хранят в социальных сетях немало личной информации, если использовать настройки по умолчанию, то значительную часть этих данных может видеть буквально кто угодно. Поэтому обязательно следует проверять настройки конфиденциальности, ведь решение о том, что могут видеть другие посетители сайтов, решает сам пользователь. Случайно выдать лишнюю информацию можно не только через социальные сети. Например, не стоит хранить конфиденциальные данные в онлайн-службах, предназначенных для обмена информацией. Например, Google Документы – не лучшее место для файла с паролями, а сканы паспорта не надо выкладывать на Dropbox (разве что предварительно упаковав их в зашифрованный архив). Не следует также использовать для хранения личных данных файлообменники и сервисы для совместной работы.

В наше время защита личных данных очень актуальна, хотя сбором и обработкой персональных сведений люди занимаются давно. Сейчас перевод различных баз данных в электронный вид упрощает не только законные манипуляции с персональными данными, но и незаконные, стало проще получить несанкционированный доступ к большому числу данных. Существует много рисков того, что персональные данные попадут к тем, у кого их не должно быть.

Собрав о пользователях данные из различных источников, можно сделать предположение об интересах, платежеспособности, местоположении, личности. Проанализировав данные, крупные интернет-игроки стараются показывать только ту рекламу, которая может быть интересна конкретному пользователю. Собранная конфиденциальная информация может быть использована и для шантажа, это наиболее вероятно, если информация из электронных медицинских карт попадёт злоумышленникам, которые захотят на этом заработать.

Как же минимизировать эти риски? Универсального средства нет, но можно определить некоторые рекомендации [2]. Прежде чем поделиться с кем-либо персональной информацией, будь то домашний адрес, номер мобильного телефона, номер удостоверения личности и т.п., надо подумать, а зачем это надо. Стоит ли добровольно сообщать эту информацию о себе.

Необходимо уточнять, для чего именно нужны персональные данные, каковы условия их обработки. Следует обращать внимание на запросы приложений и сайтов. Довольно часто в разных приложениях и на различных сайтах появляются всплывающие окна с запросом на разрешение доступа к тому или иному устройству (например, микрофону или камере) или к тем или иным данным (например, к геолокации). Чаще всего, не читая, пользователь дает такое разрешение. Не следует это делать машинально.

Не надо сообщать свою основную электронную почту и номер телефона всем подряд.Даже если приходится оставлять контактные данные интернет-сервисам и онлайн-магазинам, уж по крайней мере не стоит давать их случайным людям в социальных сетях. Еще лучше создать отдельный «мусорный» почтовый ящик, который не жалко будет удалить. В идеале хорошо бы иметь и отдельный номер телефона для таких случаев. Большинство современных мессенджеров использует шифрование. Но во многих из них сообщения шифруются только во время передачи на сервер – а там уже хранятся незашифрованными. Что будет, если кто-нибудь взломает такой сервер? Пусть даже этот риск не слишком велик, лучше его полностью избежать. Для этого надо пользоваться мессенджерами со сквозным (end-to-end) шифрованием, например WhatsApp. Следует обратить внимание, что некоторые мессенджеры, например, Telegram, Facebook не используют сквозное шифрование по умолчанию. Чтобы включить его, необходимо вручную начать секретный чат.Необходимо использовать надежные пароли.Среднестатистический пользователь, создавая пароль учетной записи, обычно выбирает что-то запоминающееся ему. Такой пароль легко запомнить. С другой стороны, его и легко «угадать»: подобрать перебором вручную или используя соответствующий инструментарий. Рекомендуется использовать длинные пароли – хотя бы 12 символов, а лучше еще больше. Чаще всего такие пароли люди не придумывают сами, за них это делают генераторы паролей. Такая функция есть у менеджеров паролей – специальных приложений для работы с паролями и прочей чувствительной информацией. Конечно, запомнить длинные уникальные пароли для всех многочисленных сервисов и приложений, практически невозможно. Тут на помощь приходит менеджер паролей – достаточно запомнить только одну комбинацию для доступа к нему, все остальные он сохранит.

Время от времени пароли следует менять. Надо учитывать то, что не следует вводить конфиденциальную информацию, к которой относятся реквизиты банковских карт, коды подтверждения оплаты на чужих устройствах. Мало ли что установлено из «шпионского» программного обеспечения на посторонних компьютерах и мобильных устройствах. Имеется риск, что на чужих компьютерах могут быть установлены программы, запоминающие то, что вводят пользователи с клавиатуры, может быть установлено и другое шпионское программное обеспечение. Если уж пришлось вводить пароль на чужом устройстве, надо изменить его на своём как можно скорее.

Довольно распространенный способ узнать пароли пользователей – обманным путем заставить их ввести свои данные на фальшивом сайте, который внешне может напоминать настоящий. Надо обращать особое внимание на адрес (доменное имя) сайта.

Фальшивку, обычно, присылают в письме по электронной почте или сообщении в каком-либо мессенджере, иногда даже не особо шифруясь. Фальшивка может оказаться близкой к оригиналу. Приведём пример. 29 июля2019 года в Службу реагирования на компьютерные инциденты KZ-CERT поступило сообщение о подозрительном интернет-ресурсе, который дублирует официальный интернет-ресурс Kaspi.kz, маскируясь под доменным именем kaspi-bannk.com [3]. Специалисты провели детальный анализ ресурса, по результатам которого зафиксировали наличие фишинговых форм «Отличительной чертой данной фишинговой ссылки являлось то, что при переходе на страницу первым всплывающим окном являлась регистрация/авторизация. Хотелось бы отметить, что при переходе на официальный ресурс Kaspi.kz первым всплывающим окном открывается главная страница, где отображается интернет-магазин», – отметили в KZ-CERT.

По задумке мошенников, держателям карт необходимо было ввести доверенный номер телефона и пароль, после чего пользователь, не замечая того, направлялся на страницу loading.php и при получении sms-кода, должен был ввести его, предоставляя таким образом доступ к своим счетам. Интернет-ресурс классифицирован Службой KZ-CERT как «мошеннический интернет-ресурс/Фишинг в сети Интернет». Ранее KZ-CERT выявила фишинговые формы интернет-ресурса

Homebank.kz, с аналогичной схемой мошеннических действий. Следует вводить пароли только на сайтах, использующих шифрование. В адресной строке браузера адрес сайта должен начинаться с https://. Для того, чтобы защитить себя от существующих и ещё не придуманных схем, надо быть бдительным. Никогда и никому не следует сообщать реквизиты банковских карт, коды подтверждения, пароли, конфиденциальную информацию. Необходимо использовать двухфакторную аутентификацию там, где это возможно.

Мобильные приложения часто просят дать доступ к контактам или файлам на устройстве, разрешить им использовать камеру, микрофон, геолокацию и так далее. Некоторым приложениям это действительно нужно для того, чтобы нормально работать. Но далеко не всем: многие используют полученную информацию для маркетинговой слежки. Следует учесть, что права приложений довольно легко контролировать. То же относится и к расширениям для браузеров, которые, к сожалению, также известны шпионскими наклонностями, поэтому не стоит устанавливать браузерные расширения без крайней необходимости, при этом надо следить, что же им разрешается делать.

Компьютер и телефон рекомендуется защитить паролями или кодами доступа. При этом пароль для разблокировки компьютера не обязательно должен быть очень сложным, так как чаще всего защищаются не от взлома, а от праздного любопытства. Смартфоны часто теряются, иногда их воруют – поэтому лучше дополнительно подстраховаться и использовать ПИН-код из шести цифр (или даже длиннее), а не из четырех, как это предлагает операционная система по умолчанию. Сканер отпечатка пальца и распознавание лица – это тоже неплохо. Но следует учесть, что и у биометрических технологий есть свои ограничения.

Если пользователь защитил телефон длинным надежным ПИН-кодом, но оставил всплывающие уведомления на экране блокировки. В этом случае любой сможет подсмотреть, о чем была переписка. Чтобы личная информация не появлялась на экране блокировки, необходимо правильно настроить уведомления. Следует соблюдать осторожность в общедоступных сетях Wi-Fi. Публичные сети Wi-Fi обычно не шифруют трафик. А это значит, что кто угодно может подсмотреть, что отправляет и получает пользователь, подключившись к той же точке доступа. Следует не передавать через общественные сети конфиденциальные сведения: логины, пароли, данные кредитных карт и тому подобное. Лучше всего использовать VPN, чтобы зашифровать передачу данных и защитить их от посторонних глаз.

Таким образом, для защиты личных данных можно использовать различные инструменты. Следует отметить, что только комплексная защита позволит сохранить персональные данные в сети Интернет.

Список использованной литературы:

1 Плотникова Т.Г. К вопросу о сохранности персональных данных в сети Интернет// Дистанционное обучение в высшем профессиональном образовании: опыт, проблемы и перспективы развития: XIII Всероссийская научно-практическая конференция с международным участием, 21 апреля 2020 года. — СПб.: СПбГУП, 2020. —с.98

2 Туреханов В. Цифровая гигиена: Мы и наши персональные данные. - URL: https://profit.kz/articles/14591/Cifrovaya-gigiena-Mi-i-nashi-personalnie-dannie/(дата обращения – 20.04.2020)

3 Кибер-мошенники нацелились на Kaspi. - URL: https://profit.kz/news/53536/Kiber-moshenniki-nacelilis-na-Kaspi/ (дата обращения – 20.03.2020)

References:

1 Plotnikova T.G. (2020) K voprosu o sohrannosti personal'nyh dannyh v seti Internet Distancionnoe obuchenie v vysshem professional'nom obrazovanii: opyt, problemy i perspektivy razvitija: XIII Vserossijskaja nauchno-prakticheskaja konferencija s mezhdunarodnym uchastiem, SPb.: SPbGUP, 98

2 Turehanov V. Cifrovaja gigiena: My i nashi personal'nye dannye. - URL: https://profit.kz/articles/14591/Cifrovaya-gigiena-Mi-i-nashi-personalnie-dannie/(data obrashhenija – 20.04.2020)

3 Kiber-moshenniki nacelilis' na Kaspi. - URL: https://profit.kz/news/53536/Kiber-moshenniki-nacelilis-na-Kaspi/ (data obrashhenija – 20.03.2020)