Ваш «цифровой след» в интернете

2 ГЛАВА

Что такое «цифровой след»?

Каждый человек, побывав где-то – на отдыхе, в гостях, на рабочем месте, так или иначе оставляет следы своего пребывания. Так же и пользователь, заходя в интернет, каждый раз оставляет «цифровые следы».

Цифровой след (или отпечаток; англ. digital footprint) – это совокупность информации о посещениях и вкладе пользователя во время пребывания в цифровом пространстве. Может включать в себя информацию, полученную из интернета, мобильного интернета, веб-пространства и телевидения.

Принято разделять цифровые следы на **активные** и **пассивные**. Активные – это то, что люди делают сами, включая публикации в соцсетях, комментарии, фотографии и так далее. Своей активностью пользователь может управлять – например, выбирать, на какие темы писать, какие делать репосты, как себя вести в комментариях. То есть осознано формировать свой цифровой образ.

А пассивные – это то, что компьютерные системы записывают автоматически: IP-адрес, с которого вы выходите в интернет, история посещений сайтов, данные геолокации и прочее. Большинство людей и не подозревают о том, как много следов они оставляют в цифровом пространстве, даже если помалкивают и не ввязываются ни в какие холивары (бесконечные прения).

Контролировать свои пассивные следы практически невозможно. Чтобы от них полностью избавиться, нужно совсем перестать пользоваться телефоном и компьютером, и то не факт, что это поможет. Все важные вехи вашей жизни, от рождения до смерти, фиксируются в государственных информационных системах – учеба в школе и институте, служба в армии, работа, свадьба, развод, участие в выборах, получение водительских прав, покупка квартиры, выезд за границу, обращение в поликлинику – буквально каждый ваш «чих» оставляет цифровой след.

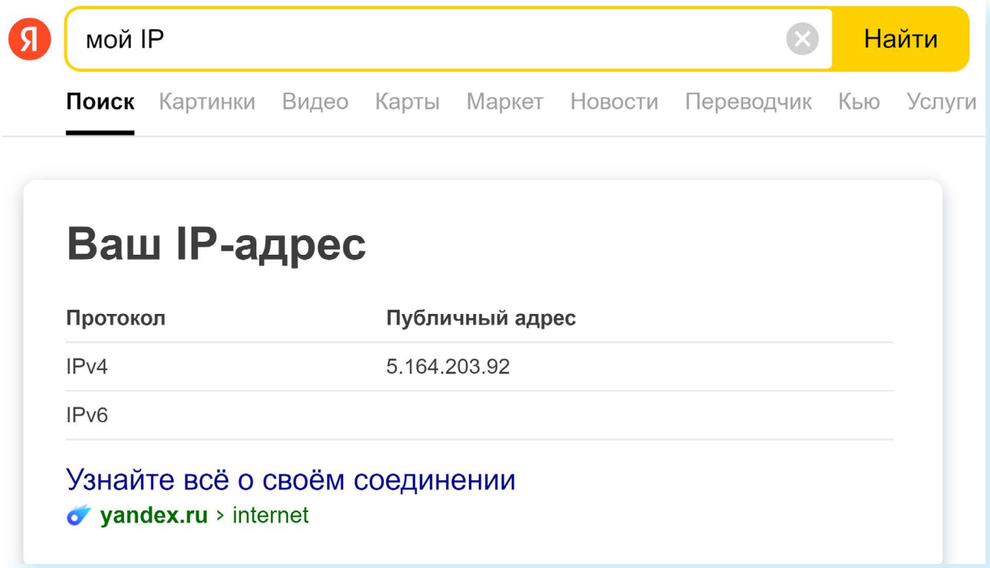
Если вы живете в большом городе, то каждый день попадаете в поле зрения камер видеонаблюдения. Например, в Москве в 2019 году их насчитывалось больше 170 тысяч, и мэрия планировала установить еще, обещая даже запустить систему распознавания лиц. Так что в скором времени все наши перемещения по городу будут известны, как минимум, властям, а , возможно, и хакерам, потому что абсолютно надежных систем не бывает.

Что значит «вычислить пользователя по IP-адресу»?

Как только вы выходите в интернет, становится виден IP-адрес (Айпи-адрес) – Internet Protocol Address вашего устройства. По сути, это цифровой идентификатор, по которому устройства могут находить друг друга в сети. Внешний IP-адрес выдает устройству провайдер. Если у вас дома стоит Wi-Fi роутер, то все устройства, которые через этот Wi-Fi получают интернет, скорее всего, будут иметь один IP-адрес.

Вы можете увидеть свой IP-адрес, просто набрав в поисковике запрос: «Мой IP» 2.1.

2.1



По сочетанию цифр в IP-адресе можно определить, где данное устройство находится вплоть до страны и города. Также можно узнать название провайдера и часовой пояс. Вот почему, узнав IP-адрес пользователя, можно узнать и его местоположение. Более подробную информацию могут предоставить провайдеры, но они имеют право это сделать только по запросу правоохранительных органов.

С одной стороны, такой внешний IP-адрес полезен. Например, если вы хотите получать доступ к файлам на домашнем компьютере с работы или, скажем, находясь в гостях, вместо того чтобы держать их в облачных хранилищах. Для этого потребуется настроить удаленный доступ. Иногда через IP-адрес настраивается камера видеонаблюдения. С другой стороны, именно возможность удаленного доступа могут использовать и кибермошенники, чтобы подключиться к вашему компьютеру и украсть конфиденциальную информацию.

Сегодня существуют инструменты, которые позволяют скрыть IP-адрес. Их используют и обычные пользователи, чтобы обеспечить безопасность информации, и мошенники, чтобы уйти от ответственности. Например, используют сайты-анонимайзеры, анонимные прокси-серверы, анонимные браузеры и соединение VPN.

Некоторые инструменты сложны для настройки неподготовленным пользователям. К тому же, обеспечивая анонимность, некоторые сервисы также становятся уязвимыми перед атаками и утечками данных. В этой главе мы разберем, как работают такие сервисы.

Какое отношение к безопасности имеют cookie(куки)-файлы

Когда вы заходите на сайты, на компьютере сохраняются кэш (cashe) и куки(cookie)-файлы. **Кэш** – это ссылки на копии веб-страниц, которые сохраняются в буфере обмена данными. Таким образом, вы можете быстрее переходить на сайты, которые уже посещали.

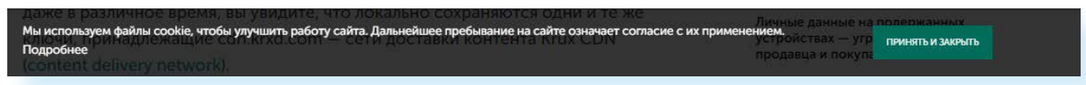
А вот **куки-файлы** хранят служебные настройки сайтов. Это они сохраняют ваши логины и пароли, индивидуальные настройки на сайтах. В них содержится информация о ваших действиях на странице ресурса. Например, если вы перешли по какой-то рекламной ссылке, куки-файлы будут способствовать тому, чтобы вам показывали рекламу именно этой тематики. Данные сохраняются у вас на компьютере, и при входе на определенный интернет-ресурс отправляются на сервер, где располагается сайт. Так сайт «узнает» вас.

Зачем это нужно? Куки – это инструмент маркетологов и рекламщиков. Они помогают собрать информацию о вашем «путешествии» по сайту. В какое время вы посетили ресурс, долго ли оставались на нем, чем интересовались, какой товар смотрели, что положили в корзину, совершили покупку или нет.

Злоумышленники также могут использовать куки-файлы для доступа к вашей личной информации и перехватить незашифрованные данные интернет-трафика.

Проблема избыточного сбора информации об интернет-пользователях начала подниматься еще в начале 2000-х. В 2018 году Европейский Союз выпустил Общий регламент защиты персональных данных. В частности, в документе были определены основы работы с куки-файлами. Использовать их теперь можно лишь с согласия пользователя. Вот откуда на сайтах стали появляться всплывающие предупреждения 2.2.

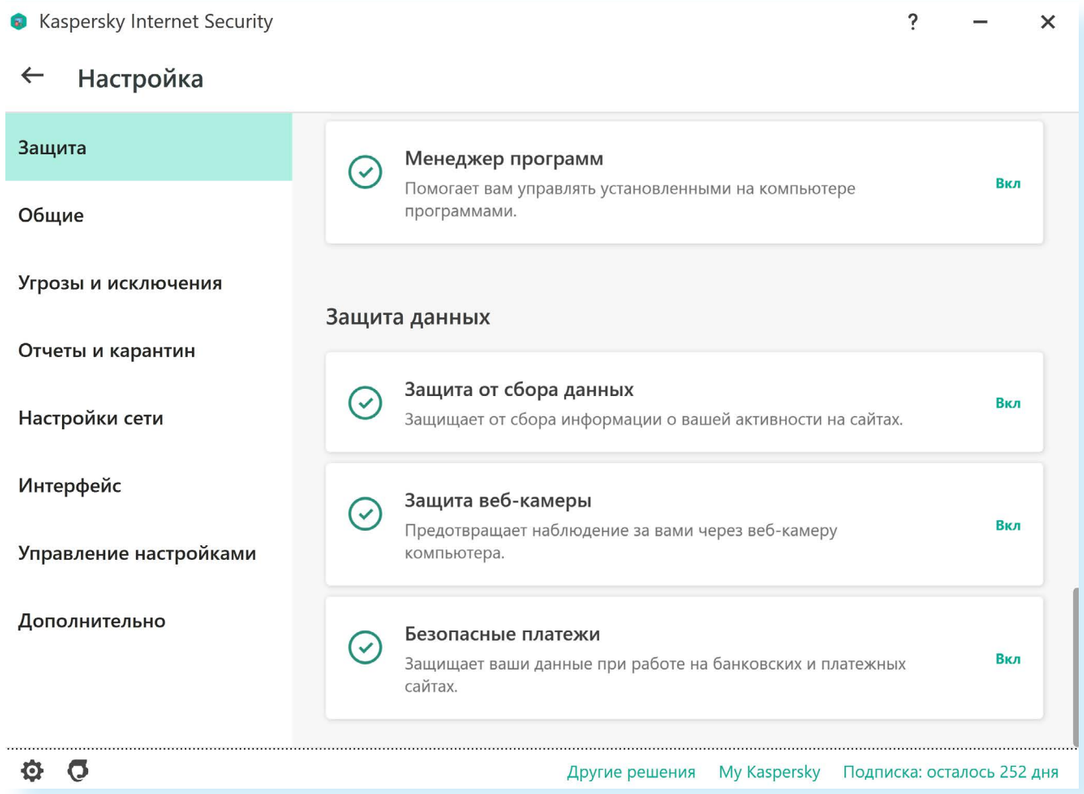
2.2



Смысл в том, что пользователь может отказаться от использования куки-файлов. Но тут тоже есть подводные камни. Иногда куки устанавливают до того, как вы ответите на баннер. Предупреждение может работать не на всех страницах, а информация об использовании таких файлов бывает неполной.

Поэтому очень важны настройка вашего браузера и антивирусной программы. Например, в антивирусе Kaspersky Internet Security (Касперский Интернет Секьюрити) нужно перейти в «Настройки», затем в раздел «Защита» и поставить в положение «Включено» функцию «Защиты от сбора данных» 2.3.

2.3

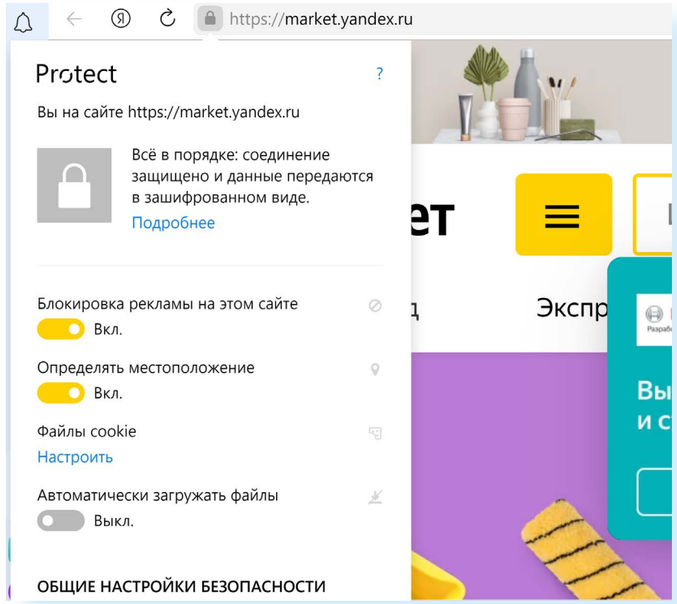


Также куки-файлы можно отключить в настройках браузера. Подробнее рассмотрим эту опцию в *главе 4 модуля «Кибербезопасность»*.

Если вы считаете куки-файлы полезными для вашей навигации по сайтам (например, не нужно каждый раз вводить пароли в личных кабинетах), то следуйте нескольким рекомендациям:

1. Используйте только защищенное соединение **https**, особенно при посещении интернет-магазинов. Это первые буквы в адресе сайта. Кликните на изображение замочка в строке браузера. Первые буквы указывают на защищенное соединение 2.4.

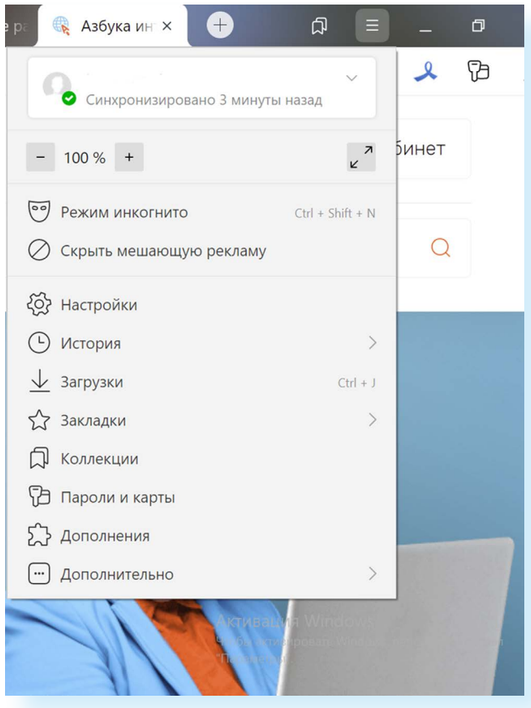
2.4



2. Не совершайте каких-либо покупок или авторизаций через общественные точки доступа Wi-Fi.

3. Если ресурс не вызывает доверия, воспользуйтесь режимом «инкогнито». Его можно выбрать в настройках браузера. В Яндекс.Браузере это изображение трех горизонтальных полосок вверху справа 2.5.

2.5



Надо отметить, что особое внимание пользователя к работе с куками снижает их эффективность. Это побудило разработчиков искать более продвинутые способы мониторинга поведения пользователей. И это направление активно развивается.

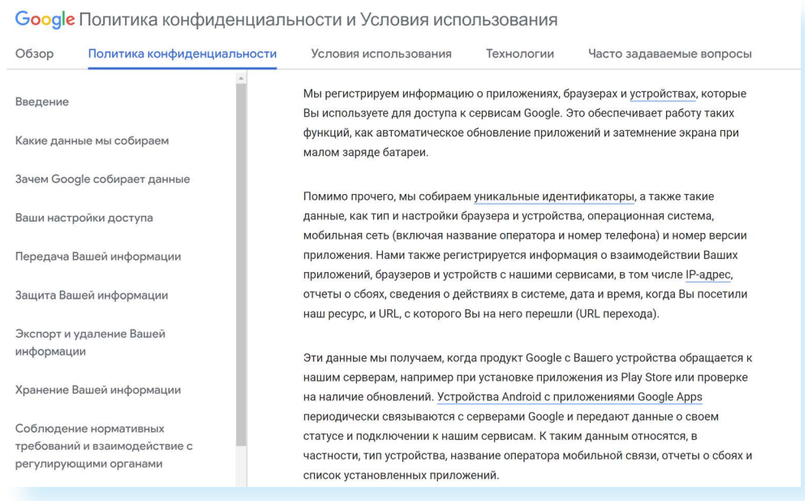
Как еще собирается и анализируется информация об интернет-пользователях

По сути, сбором информации занимается почти каждый интернет-ресурс, практикуется и межсайтовое отслеживание действий пользователя.

Большую базу данных для дальнейшего анализа собирает ваш браузер. Например, Яндекс на основе таких данных создает условный портрет пользователя. Для Яндекса мы все обезличенные пользователи, но с уникальными интересами, поведением и социально-демографическими характеристиками.

Google собирает данные в трех направлениях: личные (ФИО, телефон, логин, пароль, страна), информация о действиях (поиск, видео, сайты, объявления) и созданный контент (письма, контакты, мероприятия, фотографии). И это далеко не полный перечень. Весь список смотрите на странице «Политики конфиденциальности» 2.6.

2.6



В соцсетях собирается информация, которую пользователи указывают в анкетах, а также лайки, репосты, загрузки и даже тональность и эмоциональность сообщений. Так, Facebook собирает сведения о длительности сессий, движениях мышки, установках плагинов, доступном месте на диске, уровне заряда телефона, использовании камеры и еще много дополнительной информации, которая, на первый взгляд, не должна интересовать соцсеть.

Сбор данных периодически приводит к крупным скандалам. Уместно вспомнить историю с Facebook и Cambridge Analytica. Под видом теста они собрали информацию о пользователях, а затем использовали ее для предсказания итогов выборов Президента США, или переменную борьбу и сотрудничество Mail.Ru Group и Национального бюро кредитных историй (НБКИ), которое использует открытые данные пользователей «ВКонтакте» и «Одноклассники» для оценки платежеспособности. Последний скандал был связан с видеозаписями экрана смартфона во время оплаты заказов картой в приложении Burger King.

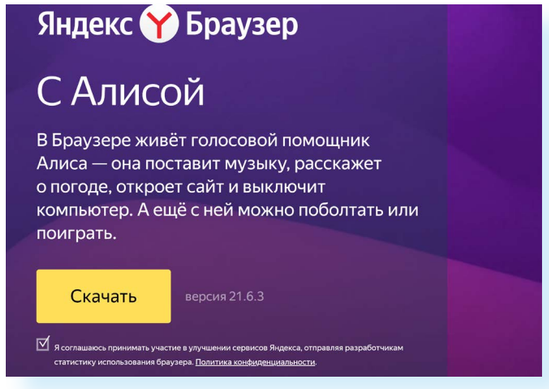
Переданные данные используют многие компании: рекламодатели, брокеры, страховые. Если все это происходит в соответствии с законом, в этом нет ничего страшного, так как информация обезличена. Это, по сути, работа ведомства статистики, которое периодически проводит перепись населения, но в случае с интернетом эти данные тут же используются для персонализированной рекламы, когда папе показывают рекламу рыболовных снастей, а маме – косметику. Теперь, чтобы понять, что искал человек до вас на компьютере, нет необходимости смотреть историю посещений сайтов, достаточно просто посмотреть, какую рекламу вам показывают на сайтах.

Наиболее активно с цифровыми данными своих граждан работает Китай. Здесь есть социальный рейтинг граждан. На основании собранных данных человек может быть отнесен к законопослушным гражданам или к нарушителям. Соответственно, тот, кто не заслужил доверия государства, имеет и меньше прав.

Почему нужно обращать внимание на Политику конфиденциальности

Наверное, вы замечали: когда скачиваешь приложение или программу на устройство или заполняешь персональные данные, сервис предлагает поставить галочку около предложения принять «Политику конфиденциальности». Большинство ставит ее, не читая и даже не задумываясь, иначе не установишь нужную программу или не зарегистрируешься на сайте 2.7.

2.7



Цель Политики конфиденциальности – проинформировать пользователя о том, как разработчики приложения используют его данные. Именно в этом документе определяется, что относится к персональным данным пользователя, как владелец приложения или сайта их собирает, обрабатывает, хранит и кому передает.

В России «Политика обработки и защиты персональных данных» регулируется федеральным законом «О защите персональных данных». Такая информация должна быть на каждом сайте, где запрашиваются ваши данные. За ее отсутствие взимается штраф.

Понять, что Политика конфиденциальности нарушена, довольно сложно, но возможно. Если в Политике говорится об обработке одних данных, а приложение или сайт требует дополнительную личную информацию – это нарушение Политики конфиденциальности. И любой пользователь может написать жалобу на такую компанию и потребовать привлечь ее к ответственности.

Достаточно сложно бывает доказать, что компания неправильно хранит ваши данные. В результате они становятся доступны третьим лицам. Хотя и в этом случае были прецеденты. Так, в 2020 году Южнокорейская комиссия по защите личной информации оштрафовала Facebook на $6,1 миллиона за нарушение закона о защите персональных данных. Как выяснилось, на протяжении шести лет, с мая 2012 года по июнь 2018 года, соцсеть передавала другим компаниям личную информацию более 3,3 миллионов человек без их на то согласия.

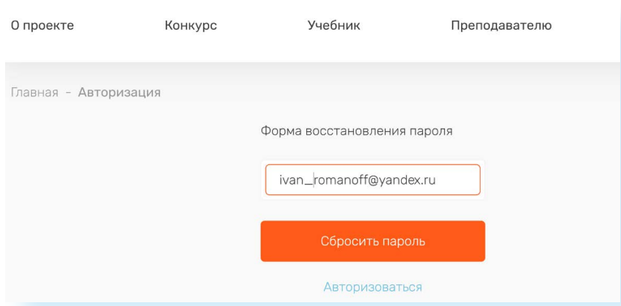
Компании часто обновляют Политику конфиденциальности. Например, в документе мессенджера WhatsApp (ВотсАп) появилась информация, что пользователи обязаны предоставлять компании Facebook доступ к номерам телефонов, именам и фото профилей, сведениям о транзакциях, диагностическим данными из приложений и IP-адресами. Недовольство и массовый уход пользователей заставили WhatsApp убрать нововведение из документа.

Прежде чем установить приложение или браузерное расширение, воспользоваться онлайн-сервисом или зарегистрироваться в социальной сети, обязательно изучите Политику конфиденциальности. Убедитесь, что приложение или сайт не получает права распоряжаться вашими личными данными – фотографиями, электронным адресом или номером телефона.

Хеширование и шифрование информации

Нужно понимать, что большие объемы информации, которые собираются в интернете, хранятся и обрабатываются не в привычном нам виде, как буквы и картинки, а в наборе символов. Информация может кодироваться, шифроваться, хешироваться. И хеширование, и шифрование имеют прямое отношение к безопасности информации.

Например, скачивая файлы из интернета, мы можем увидеть в названии ряд символов. Это и есть **хеш**. Хешируется информация для того, чтобы ее можно было быстро найти, сравнить, идентифицировать. Например, введенные вами на сайтах пароли хранятся в хешах. Когда вы используете функцию восстановления пароля, вам высылают ссылку и просят придумать новый пароль 2.8.

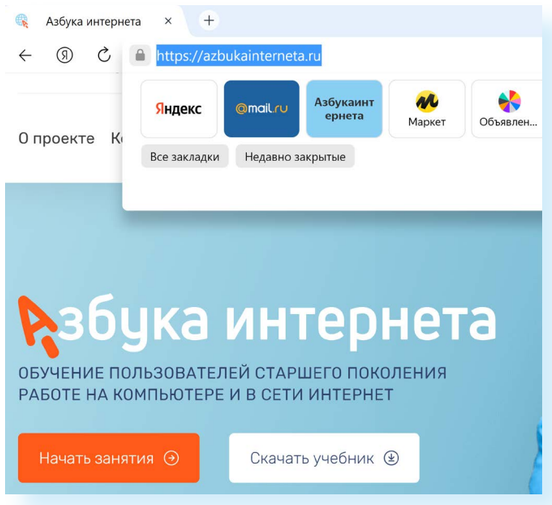


2.8

Дело в том, что сервис на самом деле не знает, каким был ваш пароль, и не может вам его подсказать. Для сайта это лишь набор символов в хеше. Столкнувшись с хэш-кодом, хакер даже время терять не будет, потому что прочитать произвольный набор символов практически невозможно. Конечно же, если это не пароль в виде «54321» или что-то подобное. А вот если, восстанавливая пароль, вы получили свой старый пароль в открытом виде – это значит, что сайт не хеширует пароли, что очень плохо.

Точно также в хеше хранится и закодированная электронная цифровая подпись, что позволяет быстро проверить ее оригинальность.

Шифрование применяется исключительно для безопасности данных. Например, когда вы заходите на сайт онлайн-банкинга или на сайт проекта «Азбука интернета», вы связываетесь с сервисом по зашифрованному каналу. Это тот самый протокол https – первые буквы, которые мы можем увидеть в адресе сайта 2.9.



2.9

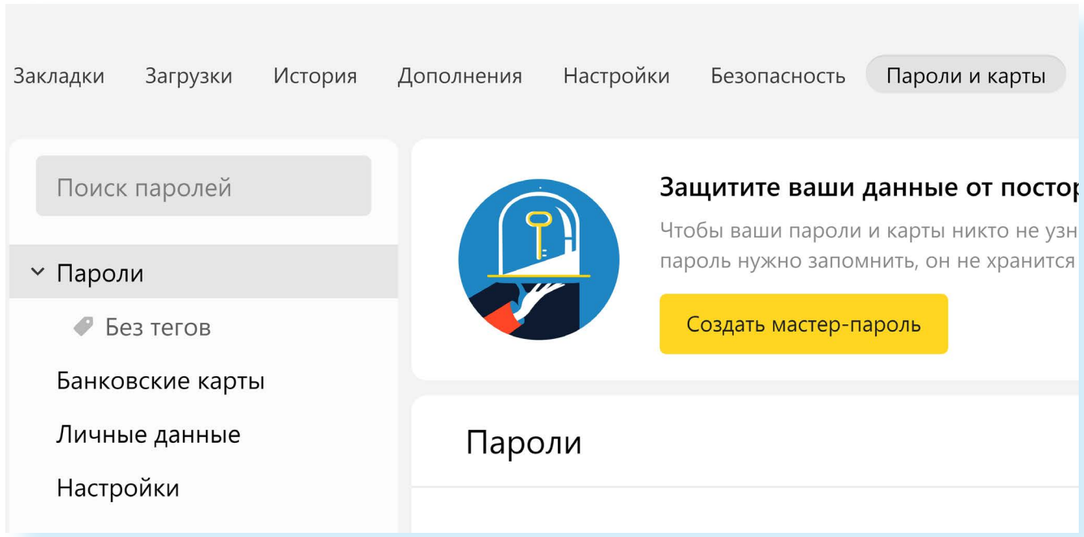
Встроено шифрование и в самый популярный сегодня стандарт сотовой связи GSM.

Также в мобильные операционные системы встроена функция шифрования. Ключевая информация в смартфоне постоянно хранится в зашифрованном виде и всякий раз расшифровывается, когда владелец вводит пароль или PIN-код для разблокировки.

Наверняка вы слышали о технологии сквозного шифрования в мессенджерах WhatsApp, Телеграм, в мессенджере Фейсбук. Это значит, что когда вы отправляете сообщение, оно уходит в зашифрованном виде. А когда поступает к адресату, расшифровывается для прочтения. В Телеграм есть функция секретного чата, где можно настроить автоматическое удаление всех сообщений.

Конечно, шифрование используется и в браузере, где хранятся ваши пароли. Доступ к ним можно зашифровать. Для этого нужно подключить мастер-пароль. По сути, вы создаете некий сейф с ключом-паролем. Данные в формы автоматически будут подставляться только после того, как вы введете основной пароль от хранилища вашей информации 2.10.

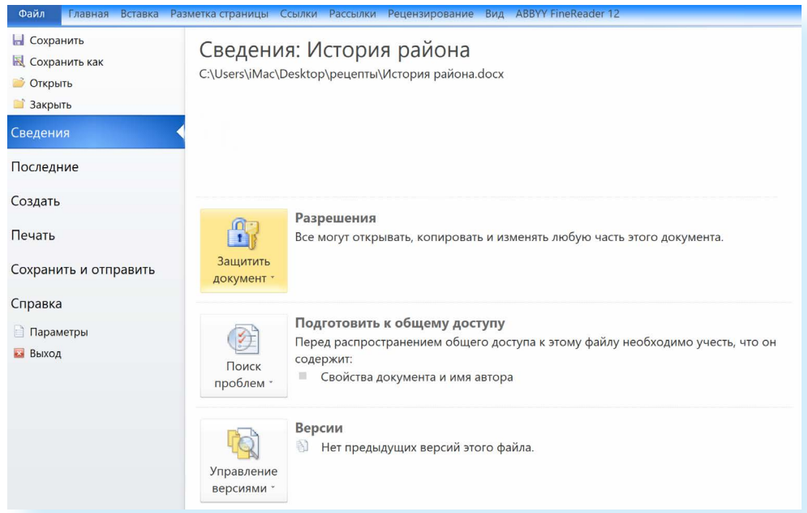
2.10



Сегодня многие компании разрабатывают «программы-менеджеры паролей». Иногда они могут быть встроены в антивирусную программу, как у Касперского, а могут быть и самостоятельным продуктом с дополнительными функциями. Все они используют технологии шифрования.

Можно зашифровать все папки и файлы, которые хранятся на компьютере. Например, в программе Microsoft Word через кнопку «Файл» можно зайти в раздел «Защитить документ» и зашифровать файл, введя пароль 2.11.

2.11



Сервис шифрования для диска и всех данных на нем встроен и в операционную систему Windows. Это программа BitLocker. Если вы решили что-то зашифровать, позаботьтесь о том, чтобы не потерять пароль к зашифрованным данным. И примите во внимание, что все возможности безопасности должны применяться разумно и адекватно ситуации.

Анонимность для «чайников»: зачем нужен VPN?

Вопрос анонимности в сети остается одним из самых актуальных. К этому стремятся и добропорядочные пользователи, чтобы обезопасить себя, и мошенники, чтобы уйти от ответственности. Поэтому в теме анонимности есть легальные и нелегальные сервисы.

Выбирая варианты защиты, нужно быть внимательными, и, прежде всего, читать отзывы о тех или иных сервисах, использовать программы надежных проверенных разработчиков.

Одна из технологий, которая работает на анонимность – это **VPN** (ВПН) – виртуальная частная сеть Virtual Private Network.

Смысл технологии в том, что соединение идет по отдельному выделенному каналу (Сеть поверх основной Сети), где сложно отследить ваши действия, поскольку ваши исходные данные изменены.

VPN-сеть может быть в любой стране и, подключаясь к ней, вы становитесь пользователем из этой страны. Вы увидите рекламу в интернете на другом языке, а отслеживающие системы будут получать некорректную информацию о ваших действиях.

Сегодня такое соединение позволяет пользователям работать в интернете по частному каналу. Ваш IP (адрес компьютера) не виден. Данные о ваших действия шифруются. Вот так на рисунке изображает суть VPN компания Касперского. Это как отдельный тоннель, который обходит все опасности интернета 2.12.

2.12

Изначально такие сети создавались для бизнеса. Это позволяло безопасно обмениваться файлами и организовывать защищенные каналы связи. А теперь VPN-соединение рекомендуют и простым пользователям, например, при подключении к Wi-Fi в общественных местах.

VPN-провайдеров, предлагающих такую услугу, немало. Вопрос в том, как выбрать, поскольку проверить честность создателя такой сети сложно. Нельзя быть уверенным, что разработчик в действительности не сохраняет пароли и логины пользователей, не торгует личными данными клиента.

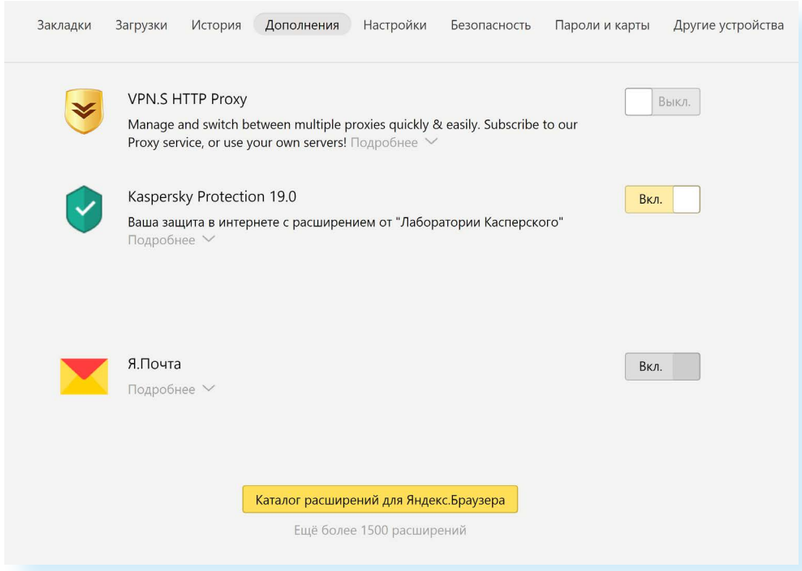
Если вы все же решили использовать анонимную сеть:

- не используйте бесплатные варианты, поскольку непонятно, за счет чего существует сеть? Как правило, VPN-сети – платная услуга;
- читайте отзывы и обращайте внимание на репутацию сервиса и компании, его создавшей. Например, Касперский создал продукт Kaspersky Secure Connection, который работает как VPN-сеть.

Стоит сказать, что браузеры сегодня также предлагают пользователям решения для VPN-соединений. Например, такое расширение есть для Яндекс.Браузера:

- зайдите в «Настройки» браузера (три горизонтальные линии справа вверху);
- выберите «Дополнения»;
- пролистните страницу вниз и перейдите в «Каталог расширений для Яндекс.Браузер» 2.13;

2.13



- на следующей странице в строке поиска наберите «VPN»;
- выберите расширение из предложенных вариантов;
- нажмите «Установить»;
- далее действуйте в соответствии с инструкциями.

Однако по мнению специалистов данные расширения не являются 100% VPN-системами. Они предлагают шифрование и анонимность трафика, но не подключают устройство к частной сети.

Также надо учесть, что любое VPN-соединение не сможет обеспечить абсолютную анонимность. Для этого нужны более сложные решения. Также сами пользователи зачастую выдают себя, например, указывая в публикациях место своего нахождения.

Можно ли удалить все ваши «следы» в интернете?

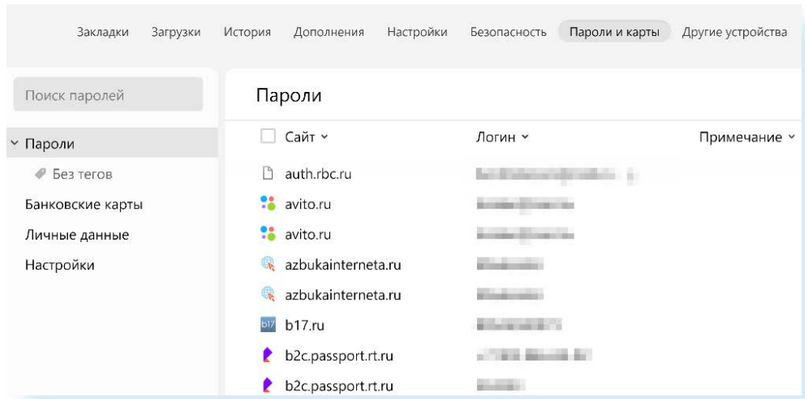
В теории можно попробовать полностью удалить свои данные из интернета. Удалить свои аккаунты в социальных сетях (не везде это легкий процесс), удалить свои аккаунты в почтовых сервисах, в мессенджерах. Если есть упоминания на каких-то сайтах, также попросить владельцев убрать ваши данные. По закону они обязаны это сделать.

Как найти все сайты, на которых вы регистрировались? Можно сделать это через сервис «Менеджер паролей» в браузере. Для этого:

- откройте меню браузера (три горизонтальные полоски вверху справа);
- выберите «Настройки»;
- в боковом меню выберите «Пароли».

Здесь вы увидите список сайтов и адреса электронных почт, номера телефонов, которые вы вводили на этих сайтах 2.14.

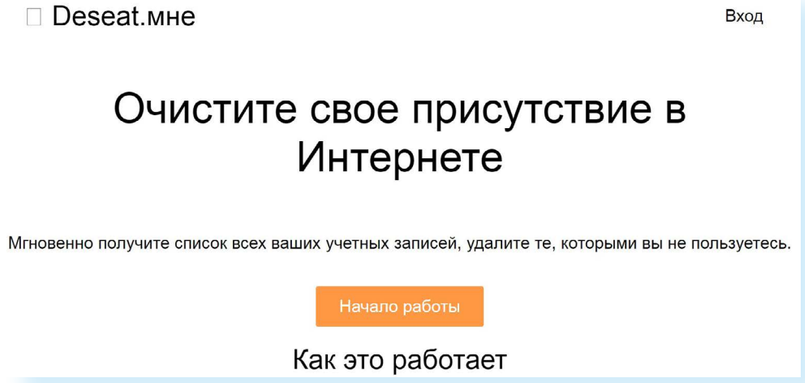
2.14



Можно перейти на каждый из них и при необходимости удалить личный кабинет.

Если у вас почтовый ящик на Gmail (аккаунт Google), то можно воспользоваться сервисом **deseat.me**, который найдет все ваши активные и давно забытые аккаунты в соцсетях и на других сайтах. Это поможет провести ревизию и решить, что оставить, а что пора списать в расход 2.15.

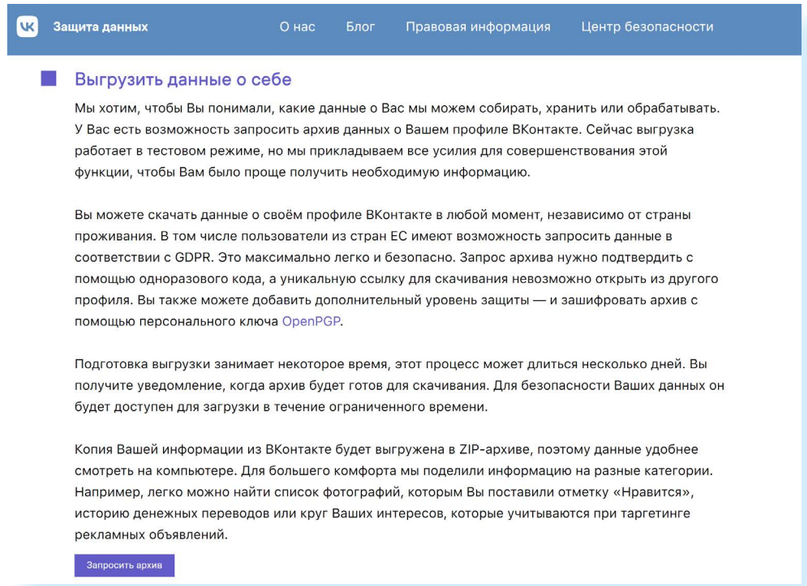
2.15



Иногда бывает, что владельцы интернет-ресурсов не хотят расставаться со своими пользователями и прячут функции удаления аккаунта куда подальше. В этом случае воспользуйтесь советом сайта Justdelete.me (**backgroundchecks.org/justdeleteme/**), который сразу перенаправит вас на нужные страницы или объяснит, почему удаление невозможно.

Многие ресурсы, например, Фейсбук, ВКонтакте, почти все сервисы Google и другие, дают возможность выгрузить все свои посты, фотографии и документы в виде архива и сохранить у себя на компьютере. Не всегда эта функция на виду, но если поискать, то найдется. Например, по этому адресу – **vk.com/data_protection?section=rules&scroll_to_archive=1** (раздел «Защита данных») – можно запросить свой архив в социальной сети в ВКонтакте 2.16.

2.16



Не рубите сгоряча. Может быть, вам еще пригодится ваша история – вдруг надумаете мемуары писать? Но помните, что если уж «рукописи не горят», то цифровая информация и подавно: где-то копия все равно останется.

Есть такой «эффект Барбары Стрейзанд» – социальный феномен, выражающийся в том, что попытка изъять определенную информацию из публичного доступа приводит лишь к ее более широкому распространению. Так было со снимками ее дома, которые попали в сеть. Их пытались убрать, а в результате эти фото стали особенно популярными и разошлись по всему интернету.

Контрольные вопросы

1. Что можно узнать по IP-адресу?
2. Зачем нужны куки-файлы?
3. Кто и зачем собирает информацию о пользователях в интернете?
4. Что прописывается в Политике конфиденциальности?
5. Какая информация в интернете хешируется и шифруется?
6. Как работают VPN-сети?