Итак, мы подключились к Интернету. Что он может нам предложить? Многое чего. Начнем по порядку и перечислим основные сервисы сети Интернет.

Хотим получить информацию о чем-либо. Пожалуйста! Для этого нам нужна в нашем ПК программа, именуемая браузер, которая умеет читать содержимое страниц Интернета.

Эти страницы размещаются на [серверах Интернета](https://www.inetgramotnost.ru/informacionnoe-obespechenie/kak-ustroeno-sovremennoe-informacionnoe-obespechenie-chast-6-a-vot-i-internet-kuda-bez-nego.html). На тех самых серверах, которые непрерывно соединены друг с другом, и могут друг другу без ограничений передавать информацию.

Каждая страница Интернета тоже имеет свой собственный адрес. Но с этими адресами пользователям работать неудобно. Попробуй, запомни множество телефонных номеров! Тоже можно сказать и про IP-адреса. Поэтому, в Интернете стало возможным давать страницам мнемонические, понятные имена. Сначала только с помощью букв латинского алфавита (ну, обогнали они нас на этом поприще, а вот в космосе… мы были  первые!). Теперь можно именовать страницы Интернет и с применением русских букв. Догоняем!..

Поэтому, если пользователь знает имя страницы Интернета, то он это имя может ввести в адресной строке браузера, и – пожалуйте. Страница будет выведена на экран ПК.

Если пользователь знает и IP-адрес этой страницы, то можно ввести и адрес. Но так обычно делают только сисадмины, когда настраивают свои серверы. Ведь именно они создают перекодировочные таблицы, которые из имени Интернет-страницы делают ее IP-адрес и наоборот. Конечно, и автоматически это делается, но совсем без ручного труда специалистов не обходится.

У каждой страницы Интернета есть не только собственный адрес и имя. У нее есть свой автор. Это очень важно. Это означает, что информация в Интернете появляется не просто так, не сама по себе. Ее туда помещают люди, целые организации (людей), которые и несут ответственность за достоверность размещаемой информации. Для пользователей ПК это значит, что **полученная через Интернет информация не может быть априори достоверна**. А вдруг автор ошибся?

Страниц в Интернете великое множество. В том числе по одним и тем же вопросам существует множество различных страниц и различных авторов. Как же можно их все найти? Для этого предназначен один из основных сервисов  в сети Интернет – **поисковые машины**.

Эти машины являются на самом деле программами, работающими на некоторых серверах Интернета. Они (эти программы, поисковые машины) непрерывно в круглосуточном режиме ищут информацию по всем страницам Интернета. И создают (автоматически) таблицы привязки.

С одной стороны, в этих таблицах записываются запросы пользователей ПК, а с другой стороны, напротив каждого такого запроса в них фиксируются имена и адреса страниц Интернета, где можно найти ответы на эти запросы.

Разработчики поисковых машин конкурируют друг с другом, поэтому алгоритмы поиска информации, алгоритмы обработки информации они держат в тайне друг от друга. Чем совершеннее поисковая машина, тем точнее она выдает перечень подходящих страниц Интернета.

Чтобы поисковые машины и браузеры могли работать, все страницы Интернет создаются по единым стандартам. Для этого был разработан специальный язык программирования. И для того, чтобы разместить информацию на странице Интернет, нужно уметь этим языком программирования пользоваться.

Для неопытных и начинающих авторов предлагаются различные программы и сервисы, которые авторские тексты (включая рисунки, видео, аудио и пр.) автоматически переводят на этот универсальный язык.

Благодаря такой стандартизации языка описания страниц удалось обеспечить доступ с любого ПК к любым страница Интернет. И благодаря этому могут работать поисковые машины, чтобы предоставлять максимально полную информацию из Интернета. А насколько точную? Это уже зависит от авторов Интернет страниц. Не ошибаются только дураки (была такая поговорка в русском языке).

По характеру размещаемой на страницах Интернет информации, эти страницы можно условно (весьма условно) разделить на сайты (на которых содержится относительно постоянная, фиксированная информации) и блоги (на которых информация постоянно пополняется авторами наподобие непрерывной ленты новостей). Но суть от этого не меняется.

Авторы сайтов и блогов оплачивают провайдерам размещение этих сайтов и блогов на серверах. Нельзя создать сайт или блог на собственном ПК. Он должен быть на сервере, иначе его никто не увидит, кроме автора.

Кроме того, авторы сайтов и блогов оплачивают право иметь имя для этого сайта, блога, то самое мнемоническое имя (**домен**), по которому сайт или блог можно найти в Интернете. Это уже оплата другому ведомству. Вроде, как оплата за авторское право на имя сайта (блога). Например, Inetgramotnost.ru является доменом для данного блога.

Что это значит для пользователя ПК? Это значит, что если сервер, на котором размещен сайт или блог, не работает в данный момент, то доступа к нему (к сайту или блогу) не будет. Сайт и блог хранятся на конкретном сервере в сети Интернет. Сайт или блог может стать временно недоступным и по другим причинам: не оплата автором сайта (блога) услуг провайдера, не оплата за имя (за домен) своего сайта (блога) и т.п.

Но зато доступ к сайту или блогу будет открыт всегда, пока работает сервер, на котором он размещен, и пока все услуги провайдера оплачены. Т.е. компьютер автора сайта или блога никакого отношения к передаче информации с сайта или блога не имеет. Автор может даже не иметь компьютера, если размещение его мыслей и идей делают за него другие люди.

Есть и бесплатные сервисы сети Интернет для размещения на них своих сайтов или блогов. Иногда начинающие блоггеры пользуются бесплатными ресурсами. Например, известный всем «Живой журнал» («ЖЖ») дает такие возможности, а также поисковики Google, Yandex.ru, Mail.ru и т.д.

С  точки зрения получателя информации (конечного пользователя ПК) никакой роли не играет, платный или бесплатный ресурс был предоставлен автору сайта (блога). Сам конечный пользователь ничего не платит за получаемую информацию, он оплачивает только своему провайдеру за услуги по подключению к Интернету.

А что делать, если пользователя ПК не интересует информация из Интернета, а он хотел бы напрямую контактировать с таким же пользователем другого ПК? Например, для обмена сообщениями. Или для совместных работ, игр и т.п. Пожалуйста! Но тогда на каждом из соединяющихся между собой ПК должно стоять специальное программное обеспечение. Простые браузеры для этого не всегда подходят.

К основным сервисам сети Интернет, например, для разговоров, подобных телефону, относится **Skype**. В нем есть не только аудио, но и даже видео связь при наличии видеокамеры на ПК пользователей.

Для обмена короткими сообщениями – пожалуйста, так называемая «аська» (название произошло от английского сокращения **ICQ** – читается «ай-си-кью»).

Для обмена электронными письмами (очень похоже на обычные письма, только доставляются они намного быстрее и точнее!) – пожалуйста, к вашим услугам почтовые ящики Google, Yandex.ru, Mail.ru, Rambler.ru, почтовые клиенты Microsoft Outlook, Outlook Express и аналогичные программы.

Про  электронную почту надо немного сказать отдельно. Этот сервис работает с участием серверов сети Интернет. Каждый пользователь ПК может на одном или на нескольких серверах сети создать свой (один) или свои (несколько) почтовые ящики.

У каждого почтового ящика есть свое уникальное имя. Так вот, после этого, как только в любом месте сети Интернет появится письмо, адресованное на этот почтовый ящик, оно обязательно будет доставлено адресату, и в этом ящике размещено. А с помощью специальных программ (например, тот же Outlook) пользователь ПК может эти письма прочитать, написать собственные письма и отправить их адресатам.

Интернет предоставляет возможности не только по поиску текстов, но и любой другой информации, которая может быть представлена в виде файлов. К основным сервисам сети Интернет относятся так называемые файлообменники, которые позволяют скачивать со специальных страниц Интернета книги, музыку, фильмы.

Тоже позволяют и так называемые Торренты, но в отличии от файлообменников скачивание производится непосредственно с компьютеров пользователей ПК, а не с серверов. Разумеется, при наличии на то согласия пользователя ПК, с которого эта информация уходит в сеть.

Возможности по скачиванию информации из Интернета породили целую проблему, известную как соблюдение авторских прав. Скачиваете фильм? Бесплатно, или пусть даже платно. Но есть ли на то разрешение автора этого фильма? А учтены ли его (автора) интересы, даже если этот фильм скачивается платным образом? Вот то-то и оно, что не известно.

В некоторых странах, например, в Германии, скачивания из Интернета запрещены. Запрещено все, кроме официальных покупок через Интернет. Но о покупках через Интернет скажу чуть позже. Ну и что же что запрещены? А если хочется? Скачаем…

Очевидцы говорят, что в Германии довольно быстро приходит к такому горе-«скачивальшику» полицейский. И – штраф. Такой, что намного дешевле бы было официально купить! А как находят? Да по тому же IP-адресу, который невозможно скрыть, так как он является обязательной частью Интернет протокола передачи данных.

В нашей стране скачивать пока можно. Но это уже к вопросам об этике и о законодательстве.

В Интернете можно **покупать информацию**. Некоторые авторы дорожат ею, и считают, что бесплатно ее отдавать нельзя. В этом случае на своих сайтах и блогах они предлагают информацию за деньги. Книги, видео, учебные пособия и другие информационные материалы.

Как оплатить? Электронными деньгами, например. Или банковской картой. Или отправив деньги по почте. А как получить оплаченную информацию? По электронной почте после оплаты. Через Почту России (очевидцы говорят, что информация доходит!). Через доступ к файлообменникам и т.п.

В Интернете можно также покупать товары и услуги. От авторучек до недвижимости, от авиабилетов до медицинских услуг.

Как? Зайти на продающий сайт, который часто называют [Интернет-магазин](https://www.inetgramotnost.ru/pokupki-v-internet/preimushhestva-internet-magazinov-vo-vremya-remonta.html). Выбрать подходящее предложение. Поместить его в собственную корзину (разумеется, виртуальную). И затем на виртуальной кассе оплатить выбранные покупки.

Как оплатить? Теми же электронными деньгами, по банковской карте и пр. Обычно в силу отсутствия платы за аренду помещений и меньшего количества персонала в интернет-магазинах товары в Интернете  стоят дешевле.

А как получить выбранные и оплаченные товары? Если Вы не попали в сети мошенников, которые берут деньги, а товары и услуги не предоставляют (такое, к сожалению, бывает, как и везде), то товары вам привезут на дом или предложат за ними прийти в офис (или пункт, терминал) по выдаче товаров. А оплаченные услуги вы получите или на дому, или в месте оказания услуг (например, в медицинском центре, если это медицинская услуга).

Интернет позволил банкам расширить комплекс предоставляемых услуг и основным сервисом сети Интернет для банков стали так называемые [Интернет-банки](https://www.inetgramotnost.ru/pokupki-v-internet/obmen-valyuty-v-internet-bankax.html).  Благодаря Интернет-банкам пользователи ПК могут получить доступ к своим счетам, открытым в банках, осуществлять контроль за ними, платежи, переводы, оплаты, обмен валют и прочее.

Только за наличными деньгами все-таки придется идти в банк или к банкомату. Интернет пока еще не может передавать ничего, кроме информации, ни товары, ни услуги, ни деньги! Только информацию. Но и это уже неплохо, не правда ли?!

**Основные правила безопасности в интернете**

Подавляющее большинство современных пользователей совершенно не заботится о своей безопасности в Интернете.

Люди просто безудержно делятся личной информацией, доверяют сохранение паролей браузерам и ошибочно полагают, что Интернет — это нечто белое и пушистое.

Современный Интернет – это некая темная улица, где вы можете столкнуться не только со случайными прохожими, но и с настоящими преступниками, которые без особого труда будут следить за вами на протяжении длительного времени, собирая личную информацию для последующей кражи или обмана.

Интернет сегодня – это гораздо больше, чем просто общение с друзьями, социальные сети, игры, онлайн-покупки. Это открытая система информации, и если кажется, что вам нечего скрывать или ваша информация никому не нужна, вы глубоко заблуждаетесь. Любая информация о вас может быть использована не теми, кому она предназначалась.

Вы когда-нибудь замечали такую интересную особенность: если вчера обсуждали на форуме котиков, то сегодня у вас обязательно промелькнет информация о новых видах корма, если обсуждали новые девайсы, то ждите рекламы с предложениями купить новый смартфон и так далее, а ведь это самый безобидный пример слежки за вами со стороны маркетинговых агентств.

Хотите заинтересовать специальные службы? Существует целый список слов и выражений, употребление которых вызовет самый недетский интерес к вашей персоне. А ваш новый смартфон (тем более яблочный) – не только быстрый, мощный и красивый, но еще и следящий за вами. Например, он может запоминать все места, в которых владелец что-то фотографировал.

Наше представление об Интернете уже в самом корне неверно. Ведь чего боятся 90 % пользователей? Вирусов, троянов, червей… Ведь так? Хотя если трезво взглянуть на это со стороны, то чем опасно большинство вирусов? Блокирующее окно с просьбой кинуть 500 рублей для разблокировки, заново поменять пароли, [переустановить windows](http://user-life.ru/kak-sdelat-samomu/kak-ustanovit-windows-7-poshagovoe-rukovodstvo.html), купить за кровно заработанные деньги [антивирус](http://user-life.ru/poleznyj-soft/besplatnaya-zashhita-kompyutera-kakoj-antivirus-vybrat.html), который, правда, можно скачать на любом [торрент-трекере](http://user-life.ru/internet/torrent-kak-polzovatsya-torrentom-piry-sidy-licher.html) – все это временные и быстро решаемые неприятности.

Гораздо страшнее то, что абсолютно любая информация, которой мы ежедневно делимся с друзьями и близкими, может в любой момент оказаться у злоумышленников. Это не паранойя, это суровая реальность или скорее дань Интернету, и однажды она может обойтись слишком дорого.

Чтобы обезопасить себя от многих ненужных проблем, я предлагаю соблюдать хотя бы основные правила безопасности в Интернете, своеобразный кодекс, в который я включил наиболее важные пункты.

**Контроль за личной информацией**

Старайтесь как можно меньше рассказывать о себе. Особенно это касается социальных сетей. Везде, где вы зарегистрированы, измените свои настройки конфиденциальности. Ваш профиль должен быть виден только вашим друзьям. Это касается и публикации статусов, и сообщений в ленте, на вашей стене и т.д.

Дружите с теми, кого знаете. Совсем не обязательно делать свои фотографии общедоступными, особенно если они сделаны из окна вашего дома. Многие люди настолько охотно любят делиться личной информацией, что даже в статусах указывают точные даты своих отпусков. Спрашивается, зачем? Осталось только приписать: «А ключ от квартиры под ковриком…».

Предположим, некий Вася Пупкин в предвкушении выходных охотно делится статусом: «Все, в субботу на рыбалку!!!». Отлично, находим в друзьях его жену Элеонору Пупкину, заходим, смотрим, нет статуса — беда! Ладно, смотрим дальше на стену, а там некая Ангелина интересуется, не смогут ли они завтра прогуляться по магазинам… «Конечно, — пишет Элеонора, — да и детей я еще вечером отвезла к бабушке…». Зайдя в свою ограбленную квартиру, Пупкины еще долго не могли понять, как же это могло произойти…

Каков главный девиз Facebook и всех социальных сетей в принципе? «Неважно, что мы хотим узнать от вас, главное, что вы сами хотите рассказать о себе».

Главная опасность социальных сетей заключается в непринужденной публикации различной информации о себе. Обратите внимание на количество информационных полей, вовсе не обязательных для заполнения: где вы работаете, куда ходите, где отдыхаете. Вы сами представляете, насколько облегчаете задачу злоумышленникам? Им и взламывать ничего не придется!

Следует изменить и настройки видимости уже опубликованных сообщений. Например, на Facebook для этого есть специальный пункт, позволяющий сделать все опубликованные сообщения доступными только для друзей.

**Надежный пароль**

Придумывайте сложные пароли, состоящие не только из букв и цифр, но и из символов. Хорошо, если ваш пароль содержит такие буквы как «Х» и «Ъ»: они плохо распознаются системой и редко используются при переборке паролей.

Не используйте один пароль на всех аккаунтах, лучше используйте вариацию пароля. Придумав и запомнив один сложный пароль, например YufG\_453@, используйте его для регистрации и на других сервисах.

Достаточно добавлять в конец пароля первые 2 буквы от названия сайта. Например, YufG453\_@vk — для ВКонтакте YufG4\_53@fa — для Facebook.

Кстати, о паролях. Этой теме я посвятил целую книгу. Книга небольшая, всего 20 страниц, где более детально рассказываю о том, каким должен быть идеальный пароль, ошибки при выборе пароля, привожу рейтинг худших паролей, описываю, как взламывают аккаунты социальных сетей и другая полезная информация. Получить книгу можно по [**этой ссылке**](http://password.user-life.ru/).

Старайтесь не переходить по ссылкам из личных сообщений. Скопируйте присланную ссылку и откройте ее в новой вкладке. Высокий процент кражи личной информации приходится и на так называемые приложения и игры соц. сетей. Будьте бдительней, особенно если приложение просит полный доступ к вашей странице.

Везде, где это можно, старайтесь не указывать свои реальные данные, и не нужно заполнять поля, не являющиеся обязательными для регистрации.

**Электронная почта — ключ к безопасности**

Это очень важный пункт в борьбе за вашу безопасность. Более того, именно взломанный почтовый ящик — это ключ к несанкционированному доступу к разным сайтам от вашего имени. Будьте очень аккуратны с вашим паролем!

Если ваш почтовый ящик будет взломан, злоумышленник в считанные секунды изменит пароль ко всем вашим сервисам, где данный адрес использовался для регистрации. Помните о важности сложного пароля и старайтесь как можно чаще менять пароль. Не разрешайте браузеру сохранять ваш пароль от почты!

Когда речь идет о секретном вопросе для восстановления пароля, будьте оригинальны. Если вас просят дать ответ на вопрос «Название улицы, на которой Вы росли», укажите, например, ответ на другой вопрос, скажем, на «Девичья фамилия вашей матери», главное — не забудьте сами, а лучше придумайте секретный вопрос самостоятельно. Вопрос получился смешным и интересным? Вот и отлично, только знать об этом больше никому не нужно!

Помните, что любой почтовый ящик, расположенный в зоне RU ( rambler.ru, mail.ru, yandex,ru ), недостаточно надежен! Как вариант, воспользуйтесь электронной почтой от Google.com (Gmail) с настройкой двухэтапной аутентификации.

Иногда ситуация требует указать почтовый ящик сервису или человеку, которому вы не слишком доверяете, в таких случаях можно воспользоваться сервисом ненастоящих электронных писем. Пример такого сервиса: Mailiпator (www.mailinator.com).

Введите любой логин (moyalevayapochta) в поле Check your Inbox, и ящик готов. Пароль не требуется. Правда, на такой ящик может зайти любой. По заявлению разработчиков, все письма бесследно удаляются через два часа.

**Защитите вашего браузера**

Большинство современных браузеров уже содержит основные средства защиты. Наиболее простой и удобный способ безопасной навигации — режим приватного просмотра (Mozilla Firefox), режим «Инкогнито» (Google Chrome), приватные вкладки и окна (Opera).

В этих режимах не сохраняются сведения о посещенных сайтах, файлы cookies, пароли и другие данные, по которым можно было бы восстановить историю работы в Интернете.

Активировать приватный просмотр в Mozilla Firefox: Ctrl + Shift + P.

А вот созданные закладки и загружаемые файлы в режиме приватного просмотра сохраняются.

Активировать режим «Инкогнито» в Chrome.

В браузере Opera аналогичный режим можно задействовать двумя способами. Первый — приватные вкладки. В этом режиме вы можете открывать приватные вкладки по одной и параллельно использовать вкладки в режиме обычного просмотра. Второй — приватное окно, где уже любые вкладки будут открываться в безопасном режиме.

Заметать следы подобным образом можно и вручную. Для этого в браузере есть соответствующий пункт.

В Mozilla Firefox: Журнал → Стереть недавнюю историю или Ctrl + Shift + Delete.

В Google Chrome: История → Очистить историю.

В Opera → Настройки → Удалить личные данные → Детальная настройка.

Но самый надежный способ — это использование [portable](http://user-life.ru/poleznyj-soft/programmy-portable-chto-eto.html)-версии браузера с вашими данными на USВ-накопителе. Правда, нужно позаботиться и о безопасности вашего USВ-накопителя. Это можно сделать с помощью программы TrueCrypt, создав зашифрованный контейнер.

**Чем опасны файлы cookies и почему за ними нужно следить.**

В далеких 1990-х, когда еще господствовал браузер Netscape Navigator, прародитель современного Firefox, появилась поддержка файлов cookies («печеньки»). Эти так называемые «печеньки» были придуманы с целью сбора информации о посетителях и их поведении в сети. Примечательно, что хранить cookie-файлы было решено не на серверах компании, а дисках посетителей.

Как это работает? Сайт, на который вы пришли, чтобы прочитать утреннюю почту, присваивает вам код (к примеру, 5yfjg847gkfdk8y5hfkdh74rguiw). Этот код в качестве текстового файла высылается и сохраняется (!) на вашем компьютере и начинает, как и вы, читать вашу драгоценную почту, которую мы как бы спрятали под семью замками надежным паролем. Будьте уверены, «печенька» обязательно запишет всю вашу интересную переписку: куда вас звали в кино, в какой ресторан, какой марки вы купили телефон, на каком самолете летали, а затем обрушит на вас поток соответствующей рекламы.

Но основная опасность в том, что этот код с легкостью можно перехватить и использовать в своих корыстных целях. Мало того, у «печенек» есть друзья, так называемые маячки (биконы), они себя не высылают, они просто находятся на просматриваемом вами сайте в качестве картинки или битого пикселя, они запоминают все введенные с клавиатуры данные, распознают, в каком месте страницы курсор мышки, и делают много других «приятных» неприятностей.

Для того, чтобы знать, какие сайты запрашивают cookie-файлы, нужно активировать соответствующую функцию в браузере и при необходимости их заблокировать. Главное — не переусердствовать. Помните, что сервисы, где нужен вход под своей учетной записью (те же соцсети), используют cookie-файлы, в противном случае нам бы пришлось вводить логин и пароль снова и снова, переходя от одной страницы этого сайта к другой.

Следует отметить, что целый ряд сайтов используют cookies с неограниченным сроком жизни, то есть ваши личные данные могут храниться на них годами, поэтому cookie-файлы иногда следует удалять.

Настройки → Показать дополнительные настройки (внизу) → Личные данные → Настройка контента.

В Opera → Настройки → Общие настройки → Расширенные → Cookies.

В браузере Mozilla Firefox → Настройки → Приватность.

Заметать следы можно и с помощью программ [CCleaneг](http://user-life.ru/poleznyj-soft/optimizaciya-windows-s-pomoshhyu-programmy-ccleaner.html). Она избавит систему от лишнего мусора: cookies, истории посещения сайтов, временных файлов, ActiveX-элементов. Старайтесь использовать программу если не ежедневно, то как можно чаще.

Будьте внимательны при установке программ и более тщательно изучайте пользовательские соглашения. Если программа обязуется от вашего имени пользоваться Интернетом, телефоном или узнавать, где вы находитесь, будьте предельно бдительны.

Для большей анонимности можно скрыть свой IР-адрес. Делается это с помощью специальных программ, так называемых анонимайзеров. При совершении запроса программа передает данные провайдеру через специальное зашифрованное соединение. После этого все ваши данные отправляются на сервер анонимайзера, где проходят расшифровку, а затем маскируются.

Будет полезным прочитать статью [Как сделать пользование интернетом более безопасным](http://user-life.ru/internet/kak-sdelat-polzovanie-internetom-bolee-bezopasnym.html)(защита путем подмены DNS-адресов).

Одна из таких программ — анонимайзер CyberGhost VPN (cyberghostvpn.com). Сервера программы, обеспечивающие подстановку IР-адресов, расположены в Германии, а это значит, что проблем с защитой не возникнет.

Думаю, о необходимости иметь надежный антивирус, корректно работающий брандмауэр и об учете контрольных записей говорить не нужно. Соблюдая эти простые правила, можно избавить себя и близких от многих неприятностей, подстерегающих нас в сети Интернет. Надеюсь, эта статья была для вас полезна.