Цифровые ценности

1 ГЛАВА

Сегодня многие считают себя «цифровыми бедняками» — красть у них нечего, потому и замки не нужны. Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными. Однако «цифровые богатства» есть у каждого. Их условно можно разделить на три категории:

- «**Измененные цифрой**» — то, что существовало и раньше, но под воздействием новых технологий имеет теперь и цифровой аналог. Например, деньги;

- «**Рожденные в цифре**» — это различные цифровые объекты, которые мы создаем сами, покупаем их или пользуемся. Например, виртуальный танк или персональная страница в соцсети;

- «**Кибервещи**» — сейчас каждая кофеварка норовит выйти в интернет. То есть обычные физические вещи становятся цифровыми.

Давайте просто перечислим, что это может быть.

Деньги. Кроме наличных в кошельке, они все электронные.

Бонусы — «как бы деньги» — мили, баллы лояльности и прочее.

Персональные данные, включая медицинские.

Аккаунты в соцсетях, страницы и каналы — иногда это очень дорогой актив.

Тайна частной жизни. Когда вокруг камеры и микрофоны, это становится роскошью.

Репутация. Интернет помнит все, что написано о вас, и все, что вы написали сами.

Переписка — деловая и личная, в электронной почте и мессенджерах.

Контакты и заметки. Никто уже не держит записных книжек, не так ли?

Цифровые авторские права на сайты, блоги, фото, видео и другой контент.

Домены (сайты). В наше время бывает так, что имя ребенку выбирают «в соответствии со свободным доменом».

Цифровые коллекции — музыка, кино, файлы, фотографии.

Виртуальные вещи. Пока в играх.

Цифровые ресурсы — Wi-Fi, место в облачном хранилище, виртуальные машины и прочее.

Цифровая техника — телефон, компьютер и прочая «умная» электроника.

Автомобиль — все больше превращается в компьютер на колесах со всеми вытекающими рисками.

Умный дом. Эта тема только набирает популярность и пока не слишком волнует киберпреступников, но угрозы будут расти.

Естественно, найдутся люди, которые могут захотеть это украсть или уничтожить.

Три категории цифровых богатств:

- измененные цифрой;
- рожденные в цифре;
- кибервещи.

Деньги и бонусы

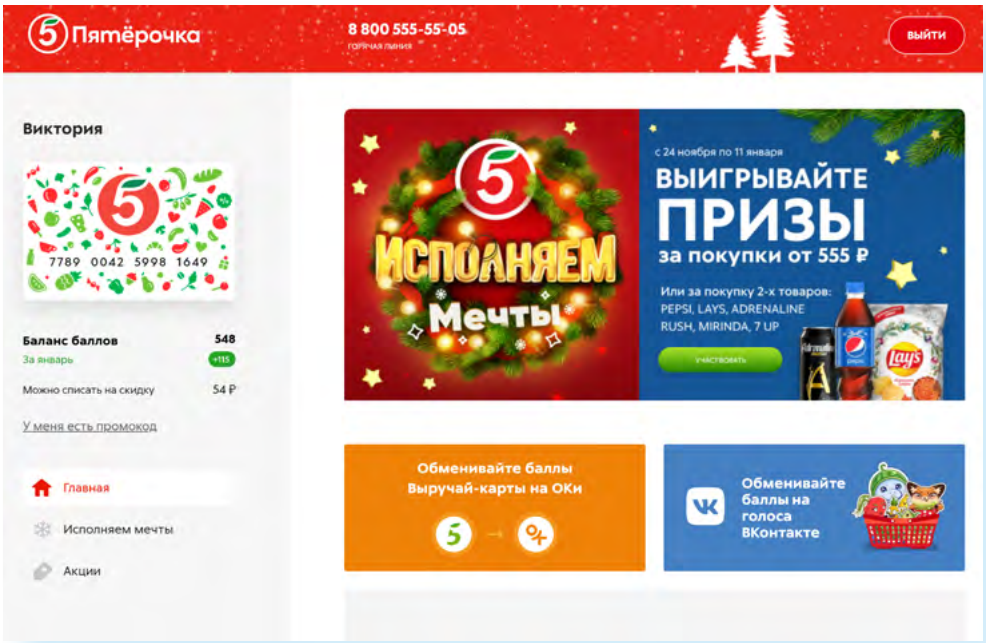
Кроме наличных, которые лежат у вас в кармане, все остальные ваши деньги существуют в цифровом виде. Пенсия на карточке, депозит в банке, баланс на счете мобильного телефона и пр. Это не более чем цифры в какой-то базе данных, но точно также их можно потерять или стать жертвой грабителей.

Более подробно о безналичных формах оплаты, электронных деньгах в модуле 4 «Оплата товаров и услуг через интернет: полезные сервисы и платежные устройства».

Финансовые системы являются одними из наиболее защищенных, но они же — лакомый кусок и для киберпреступников. При этом мошенники используют технические механики (взломы систем, вирусы, фишинг, фарминг), социальную инженерию (психологическое манипулирование), когда пользователи сами сообщают мошенникам нужные пароли. Увы, на удочку таких жуликов попадаются даже специалисты по информационной безопасности. Все мы живые люди, и у нас есть эмоции, которые могут отключить наше критическое мышление.

Главное — не поддаваться эмоциям, когда вам сказали, что ваши деньги вот-вот украдут, или позвонили, чтобы поздравить с небывалым выигрышем. Спокойно проанализируйте ситуацию и возьмите инициативу в свои руки.

Кроме банковских карт у вас в кошельке наверняка найдутся бонусные и скидочные карты, карты лояльности от различных компаний. Бонусы копятся в ваших личных кабинетах на сайтах магазинов 1.1.



1.1

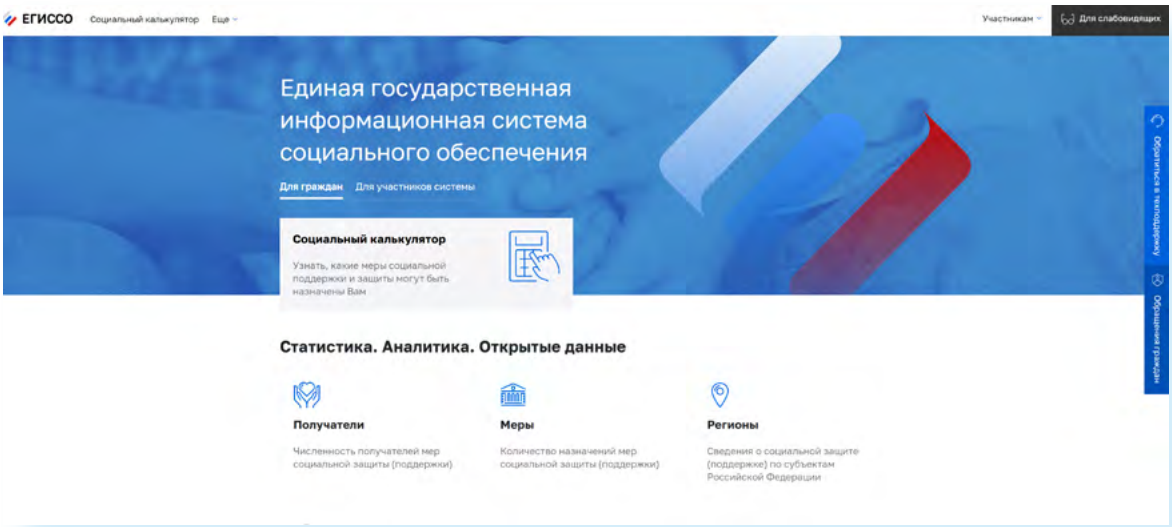
Формально все эти баллы и бонусы деньгами не являются, но с практической стороны они равнозначны настоящим деньгам. Если вы потеряете саму карточку, то это нестрашно — попро́сите новую. А вот если кто-то получит доступ к вашему аккаунту, то этот кто-то, скорее всего, найдет способ, как использовать ваши бонусные баллы.

Примеры «цифровых денег»:

- зарплата на карточке;
- депозит в банке;
- баланс на счете мобильного телефона.

Персональные данные

Ваши фотографии, имя, фамилия, номер мобильного телефона, адрес электронной почты, данные ваших документов (паспорта, СНИЛСа), данные о состоянии вашего здоровья — все это **персональные данные**. Благодаря развитию информационных технологий стала возможной массовая обработка персональных данных. Например, есть система **ЕСИА** (Единая система идентификации и аутентификации), на которой основан портал Госуслуг, **ЕГИССО** (Единая государственная информационная система социального обеспечения), хранящая данные ваших личных документов 1.2.



1.2

Конечно, базы данных являются и целью для мошенников. Можно поставить на поток схемы по краже денег с банковских карт, вести незаконные рекламные кампании или даже пытаться влиять на исход выборов. Одна из иностранных социальных сетей поплатилась именно за это — соцсеть передала данные клиентов компании, которая якобы помогла победить на выборах определенному политику.

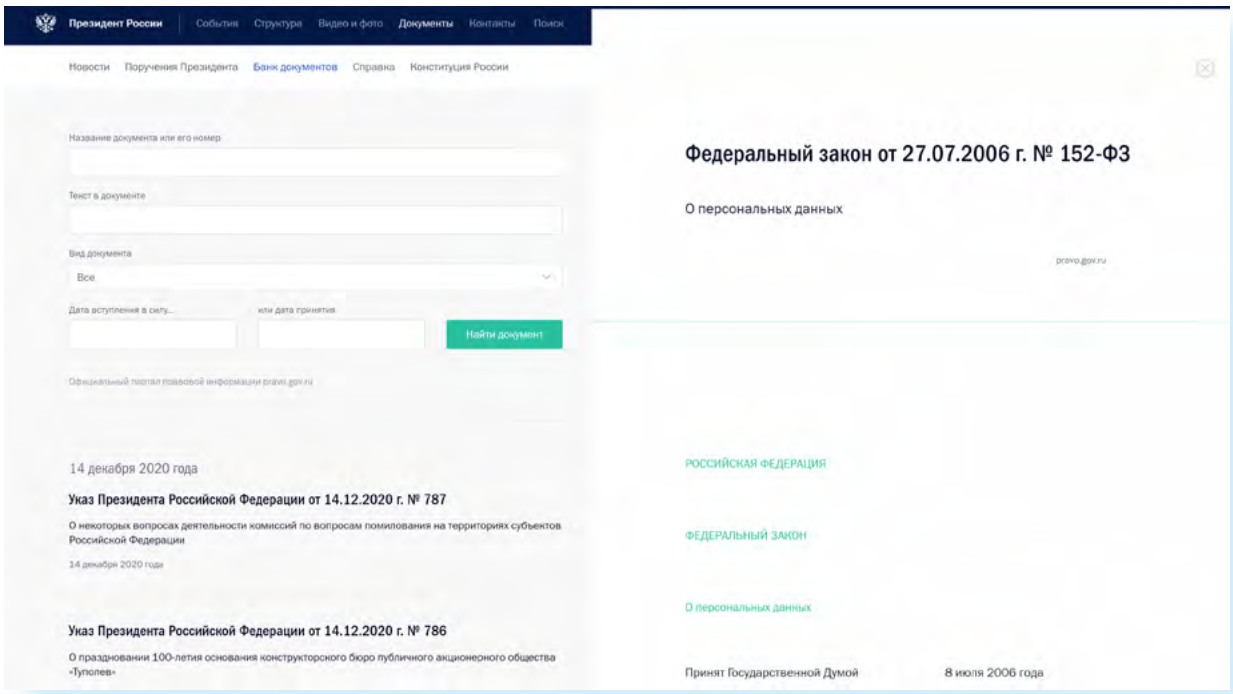
Среди персональных данных особо выделяются данные о состоянии здоровья: о перенесенных заболеваниях, диагнозах, обследованиях, результаты анализов и даже сам факт обращения к врачу. Люди обеспокоены рисками разглашения их истории болезни в основном из-за возможных социальных последствий: например, есть «стыдные» болезни, которые никто не хотел бы афишировать.

Однако здесь есть и риск, связанный с рекламой или попытками мошенничества: узнав ваши медицинские данные, некто может попытаться продать вам лекарственные препараты или медуслуги, в том числе поддельные или сомнительного качества.

Поэтому законодательством предусмотрена строгая ответственность за распространение персональных данных граждан.

Закон 152-ФЗ можно найти на официальном сайте президента **kremlin.ru** 1.3.

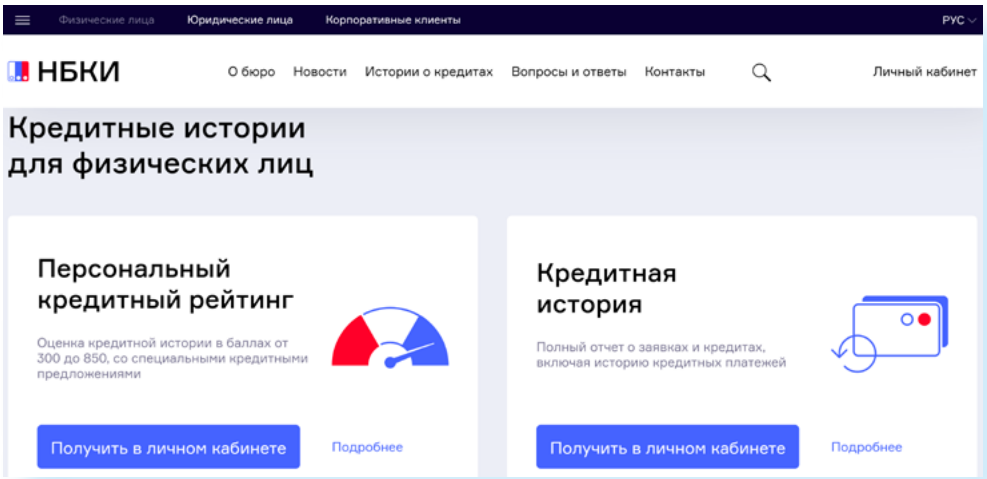
1.3



Если посмотреть на вещи реально, то у человека нет возможности управлять данными о себе. Конечно, следует проявлять разумную осторожность и не оставлять лишней информации на совсем уж «левых» сайтах. Но в паранойю тоже впадать не следует. Достаточно задать себе вопрос: для чего кому-то нужны ваши данные? Например, если вы не скажете адрес таксисту, он вас не довезет до дома. Однако совершенно необязательно сообщать ему, с кем вы живете и сколько денег у вас на счете.

Еще говорят, что если кто-то завладеет копией вашего паспорта, то сможет оформить на него кредит. Да, такое случается, и полностью уберечься от этого риска невозможно, но можно периодически проверять, есть ли кредиты, взятые на ваше имя. Необходимо отправить запрос в **Бюро кредитных историй** — один раз в год это можно сделать бесплатно прямо на сайте. Обратите внимание, что таких кредитных бюро несколько. Одно из крупнейших — **nbki.ru** 1.4.

1.4

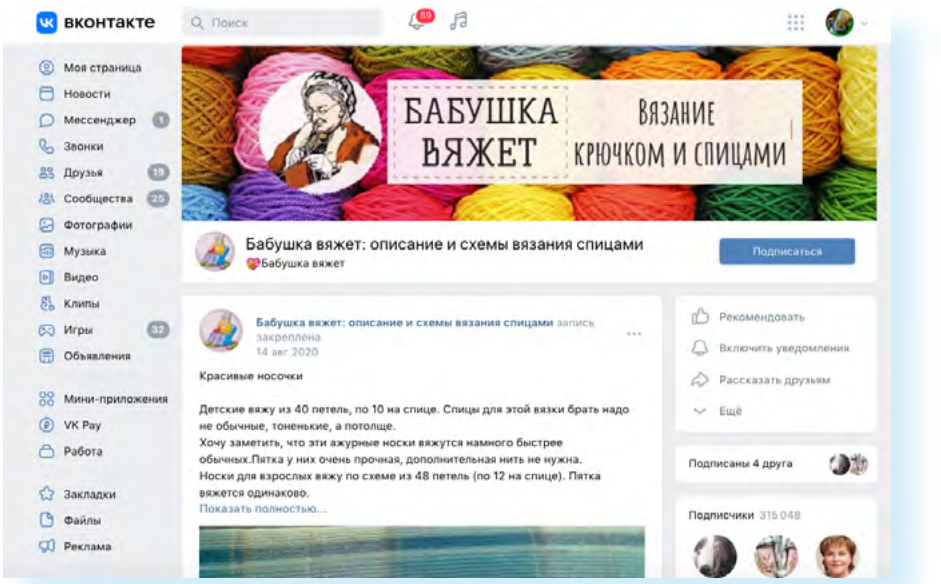


Считайте такой ежегодный запрос одним из элементов цифровой «гигиены», даже если вы не теряли паспорт.

Аккаунты в социальных сетях, репутация и тайна частной жизни

Миллиарды людей имеют аккаунты в соцсетях. Для многих это очень важная ценность, так как там содержатся контакты, личная информация или коллекции цифровых фото и видео. Потерять свой аккаунт в социальных сетях может быть очень болезненно психологически, а иногда и финансово. Есть люди, для которых ведение аккаунта — это уже работа 1.5.

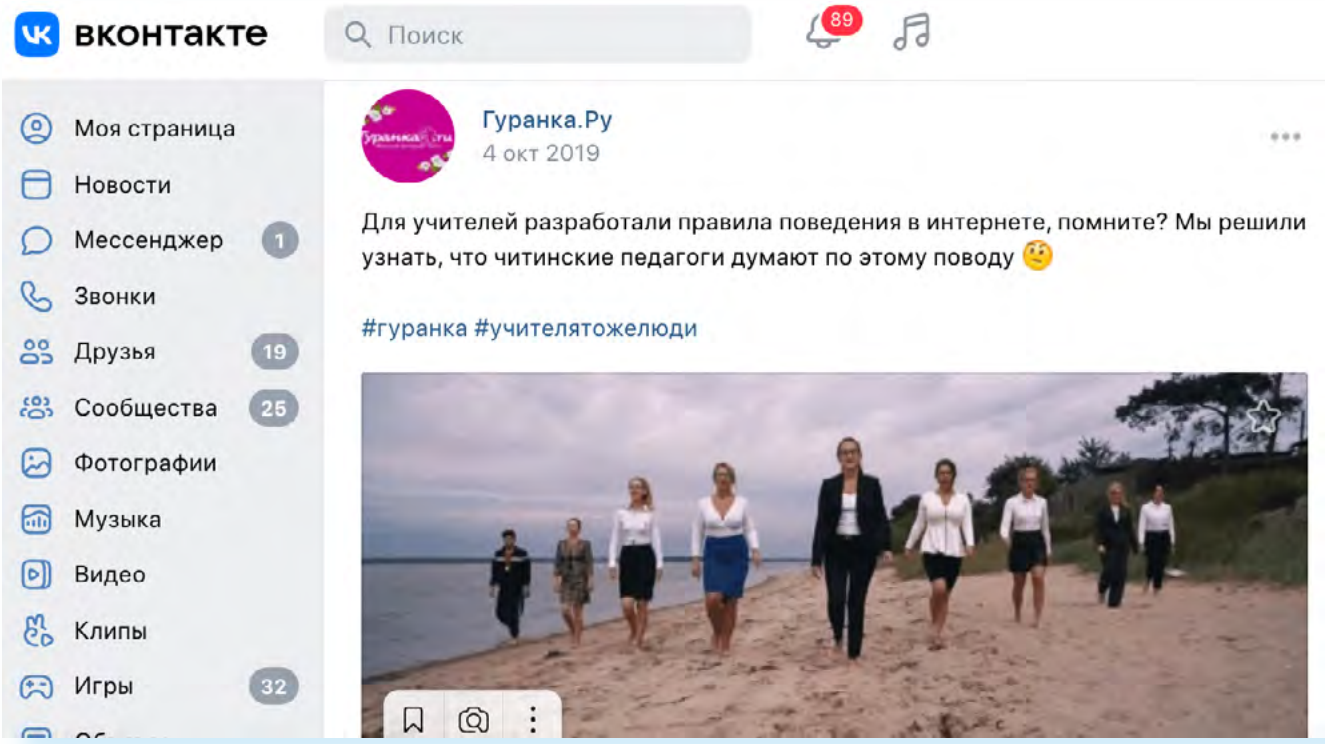
1.5



Набрав нужное количество подписчиков, автор может монетизировать свой труд. Аккаунт работает как рекламная площадка. И в тот момент, когда страничка в социальных сетях начинает интересовать рекламодателей, к ней появляется интерес и у мошенников, которые могут завладеть вашим аккаунтом. Поэтому, начиная карьеру блогера, нужно побеспокоиться о цифровой безопасности.

Не менее важная тема — репутация. Интернет и социальные сети дают возможность заглянуть в частную жизнь буквально каждого человека. При этом интернет помнит все. Теперь даже одно неудачное фото или резкая фраза могут если не сломать жизнь, то заставить изрядно понервничать, потому что люди очень по-разному понимают правила приличия и готовы затравить тех, кто, по их мнению, в них не вписывается.

В январе 2019 года учительница из Барнаула, разместившая у себя в соцсети фото в купальнике после заплыва в честь Универсиады в Красноярске, где она демонстрировала свои медали и грамоту за участие в соревнованиях, неожиданно получила от директора школы настойчивое предложение уволиться, потому что на нее пожаловалась мать одного из учеников, которой эта фотография показалась вызывающей. Эта история завершилась в целом благополучно — учителя по всей стране устроили флешмоб в поддержку коллеги и выложили фото в купальниках с хештегом #УчителяТожеЛюди. Министр образования Алтайского края лично вступился за нее и предложил подыскать ей достойное место, но учительница в школу не вернулась 1.6.



Вероятно, вы слышали про эксперименты с социальным рейтингом в Китае, когда человеку за определенные проступки снижают баллы и, наоборот, поощряют за социально одобряемое поведение. Можно

по-разному относиться к такому эксперименту, но тенденцию он отражает точно: когда вся информация прозрачна, человеку надо осознанно относиться к управлению своей репутацией, и не важно, следит за ним какая-то государственная система или пока нет.

Мы ежедневно попадаем в поле зрения сотен видеокамер, наши разговоры записываются, перемещения фиксируются. Мы добровольно променяли наши маленькие секреты на удобства, которые предоставляют цифровые технологии.

Стоит ли этого опасаться? Спор на эту тему идет давно. Во многих европейских странах не принято иметь шторы на окнах, люди так и живут у всех на виду. Есть мнение, что именно открытость и прозрачность дает возможность привлекать к ответственности тех, кто нарушает законы. Пожалуй, в нашем прозрачном мире это будет самое благоразумное решение — поменьше беспокоиться о том, что за вами наблюдают, и всегда вести себя так, чтобы не было причин чего-то стыдиться.

При этом не надо путать приватность (конфиденциальность) и анонимность. **Анонимность** — это желание скрыть свою личность при контактах с другими людьми. Помните, что анонимщиков и анонимки всегда не очень жаловали в обществе.

Переписка: почта и мессенджеры, контакты, заметки, цифровые коллекции

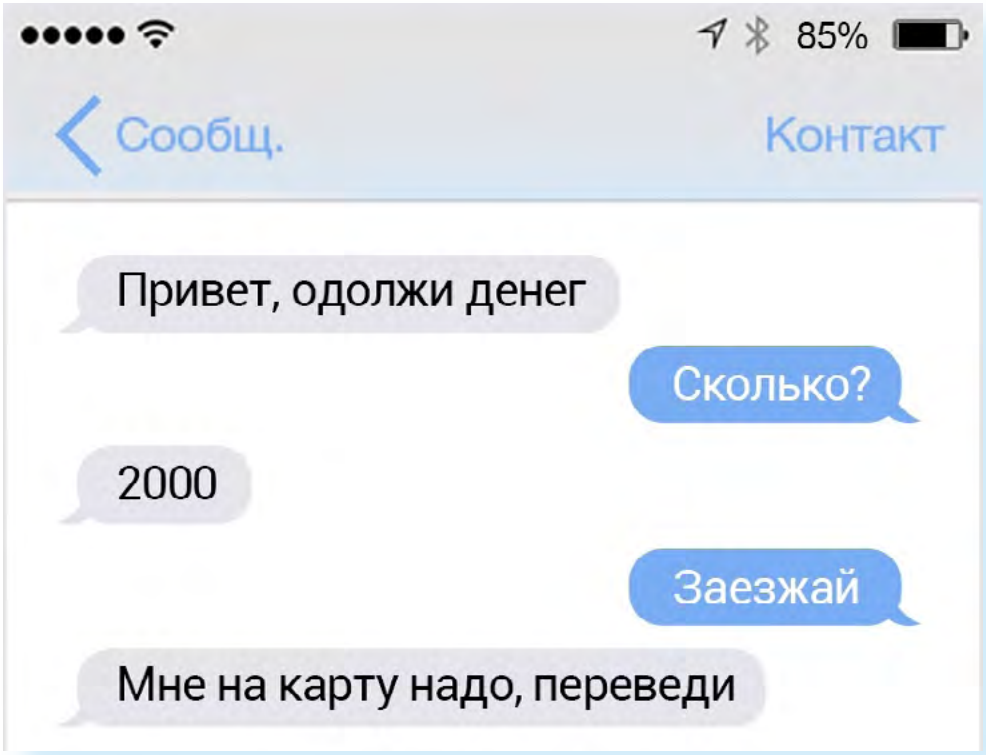
Из тридцати томов полного собрания сочинений и писем Антона Чехова письма составляют двенадцать томов. По объему переписки мы сегодня, пожалуй, превосходим Антона Павловича.

Личная переписка ведется в электронной почте, в социальных сетях, в мессенджерах (Вайбер, Вотсап и т.д.). А еще адрес электронной почты активно используется для восстановления паролей к различным сервисам. Для хакеров это возможность взломать адрес вашей электронной почты, получить доступ к другим ресурсам, найти ваши персональные данные, пароли. Поэтому к защите почтовых ящиков, как своих, так и своих детей и внуков, надо относиться со всей серьезностью.

За реальными почтовыми адресами, которые еще не засветились в спам-рассылках, охотятся и рекламщики. Если им удастся заполучить ваш пароль, они с удовольствием будут рассылать от вашего имени свой мусор на адреса ваших друзей, да и просто случайным людям. Потом кто-нибудь пожалуется на спам, и ваш ящик будет заблокирован.

С мессенджерами история аналогичная. Здесь чаще срабатывают банальные «разводки», когда со взломанного аккаунта вашего знакомого просят срочно перевести деньги на какое-то важное дело 1.7.

1.7



Такими же ценными для мошенников являются и контакты или заметки, которые хранит ваш мобильный телефон, ведь уже никто не ведет рукописных телефонных книжек. Вся информация, которая есть в телефоне, сегодня копируется в облачные хранилища, и через них легко восстанавливается, если, конечно, вы специально не отключите опции резервного копирования на устройстве.

Но тут появляется другой риск — можно потерять контроль над своим аккаунтом, и тогда это будет большой проблемой, потому что все контакты тоже будут потеряны. Заполучив его, хакеры могут делать рассылки вашим знакомым от вашего имени, что сразу повышает их уровень доверия к полученной информации, и человек кликает на присланную ссылку или открывает вредоносный файл. Или того хуже: мошенники начинают просить помощи от вашего имени, а ваши доверчивые друзья переводят им деньги. Чаще всего это срабатывает с самыми близкими людьми.

Также нужно подумать о ваших цифровых коллекциях. Раньше фотографии хранили в альбомах. Теперь на компьютерах, флешках или облачных хранилищах. И всегда есть риск, что на флешку, в компьютер или любой другой гаджет попадет вирус, а, может, кто-то получит доступ к вашему гаджету и будет вас шантажировать, угрожая уничтожить дорогие сердцу коллекции. Хранить коллекции фотографий и видео в облачных хранилищах удобно. Главное при этом — внимательно относиться к своим цифровым ценностям и не забывать самим заботиться об их безопасности.

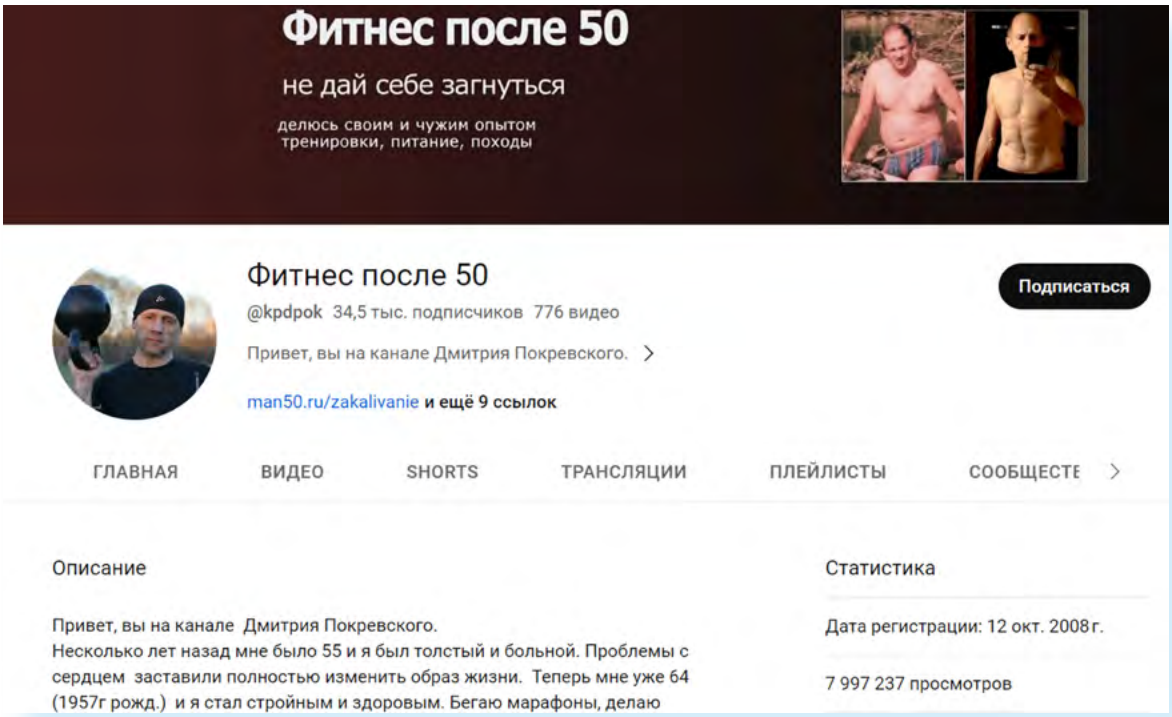
Если ваш знакомый в личном сообщении просит одолжить ему денег:

- не торопитесь переводить деньги;
- попробуйте списаться или созвониться с этим человеком;
- если это мошенники, выделите сообщение и укажите, что это спам. Это поможет заблокировать взломанный аккаунт.

Авторские права на цифровые произведения

Обычные пользователи интернета редко задумываются об авторских правах на свои произведения, а зря.

Например, 66-летний Дмитрий Покревский из Калуги по использованию современных технологий опережает многих молодых коллег. Уже 15 лет он снимает видео о здоровом образе жизни и выкладывает их на YouTube. Сейчас их смотрят русскоязычные зрители во всем мире: у канала учителя более 34 тысяч подписчиков, а общее число просмотров перевалило за 7 миллионов 1.8.



1.8

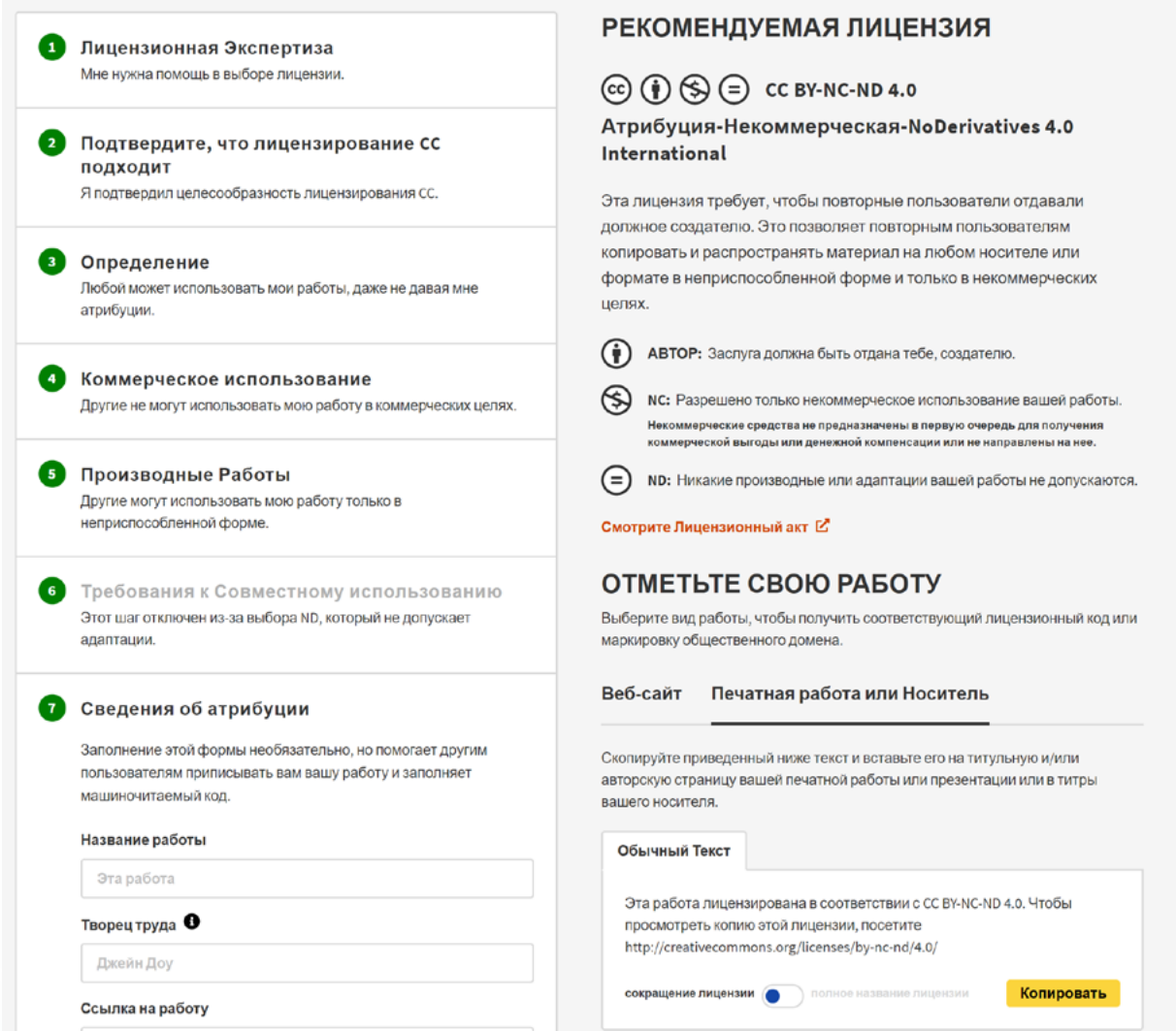
Если вы тоже решите сделать свой контент всеобщим достоянием, то это необходимо специальным образом обозначить, потому что могут найтись люди, желающие заработать на ваших произведениях вместо вас. Есть такие владельцы аккаунтов, которые не делают свой контент, а скачивают и выставляют от своего имени самые популярные видео.

Например, вы можете публиковать свои произведения под открытой лицензией Creative Commons (Креатив Коммонс), которая используется, когда автор хочет дать другим людям право делиться и использовать произведение, созданное им. Лицензии применяются ко всем работам, на которые распространяется авторское право, включая книги, пьесы, фильмы, музыку, статьи, фотографии, блоги и веб-сайты. Для ее использования нужно перейти на сайт **chooser-beta.creativecommons.org**, слева ответить на вопросы анкеты и справа отобразится рекомендуемая вам лицензия. Ее название нужно будет указать в описании к вашей работе 1.9.

Чтобы выбрать лицензию Creative Commons:

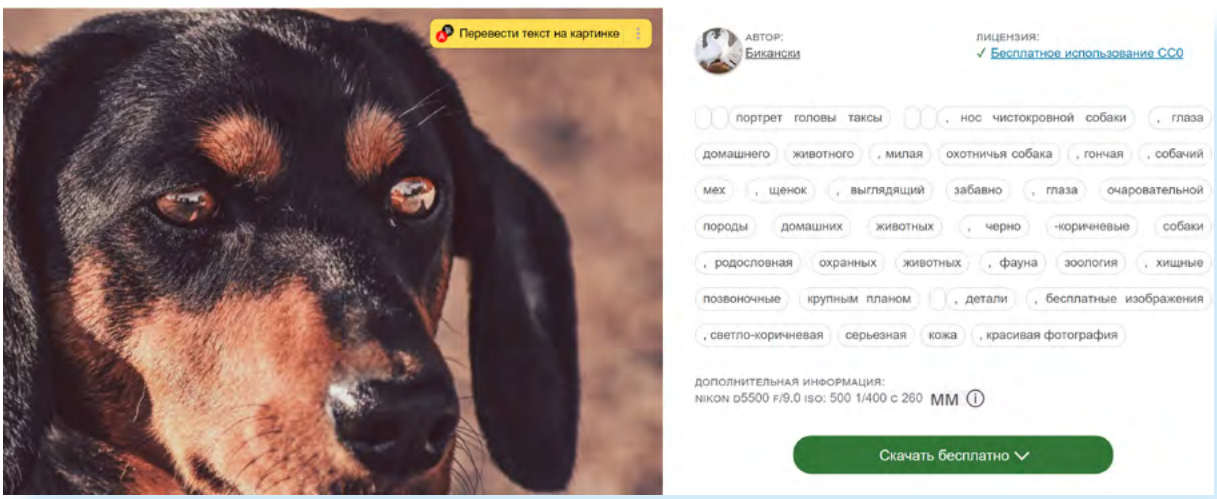
1. Зайдите на сайт **chooser-beta.creativecommons.org/**.
2. Слева заполните анкету.
3. Справа отобразится рекомендуемая лицензия.
4. Внизу в блоке **«Печатная работа»** вы сможете скопировать текст и вставить его в описание к своей работе.

1.9



Внизу, выбрав блок **«Печатная работа»**, вы можете скопировать текст о выбранной лицензии и вставить его в описание к своему произведению. Есть разного вида лицензии Creative Commons. Обычная — CC0 — позволяет всем размещать и редактировать авторскую работу. Лицензии CC CC BY-ND запрещают коммерческое использование и изменение авторского материала. Вот так выглядит упоминание лицензии на сайте. В данном случае фото в свободном доступе 1.10.

1.10



Заботясь о своих авторских правах, нужно уважительно относиться и к чужим, и помнить, что пиратский контент — это еще и источник вирусов.

Цифровые ресурсы и виртуальные вещи

В больших городах почти у каждого в квартире есть Wi-Fi-роутер 1.11.

1.11

Сегодня мы пользуемся безлимитным высокоскоростным интернетом, а ведь еще не так давно трафик был достаточно дорогим и каждый мегабайт был на счету. В то время процветал вид мошенничества, связанный с воровством трафика, — кто-то из технически продвинутых соседей взламывал ваш роутер и за ваш счет пользовался интернетом. Сейчас едва ли будет актуально ломать чужую сеть, чтобы сэкономить 300-500 рублей в месяц, но у хакера могут быть и другие мотивы. Например, чтобы совершить какие-то противоправные действия: если он делает это через ваш роутер, то полиция и ФСБ придут к вам, когда начнут разыскивать преступника. Поэтому свои цифровые ресурсы нужно защищать.

Кроме канала доступа в интернет к цифровым ресурсам можно отнести место на дисках в облачных хранилищах, пакеты минут и SMS на телефоне, подписки на кино и ТВ и так далее. В результате взлома ваших аккаунтов все это вы рискуете потерять. Допустим, некто может получить доступ к вашему личному кабинету мобильного телефона и продать ваши накопленные гигабайты интернета на бирже, как это позволяет делать Tele2.

Также внимательно теперь нужно относиться и к виртуальным вещам. Пока они распространены в игровых мирах, где, например, могут похитить танк или экипировку. На данный момент с точки зрения российского законодательства виртуальные вещи, используемые в игровых мирах, имуществом не считаются. Тем не менее, иногда пострадавшие все-таки обращаются в полицию. И даже бывает такое, что виртуальных воров находят и возвращают украденное владельцу. Для нарушителя наступает ответственность по ст. 272 УК РФ за неправомерный доступ к компьютерной информации как за деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, и грозит ему за это крупный штраф или даже реальный срок.

«Умная» техника и «умный» дом

Сегодня вокруг нас появляется все больше «умных» вещей. Например, бортовой компьютер есть во всех современных моделях машин. Пройдет немного времени, и все автомобили, находящиеся на дорогах, окажутся подключенными к интернету. Зачем? Прежде всего, для повышения безопасности движения. В авиации это делается уже повсеместно, теперь очередь за автотранспортом.

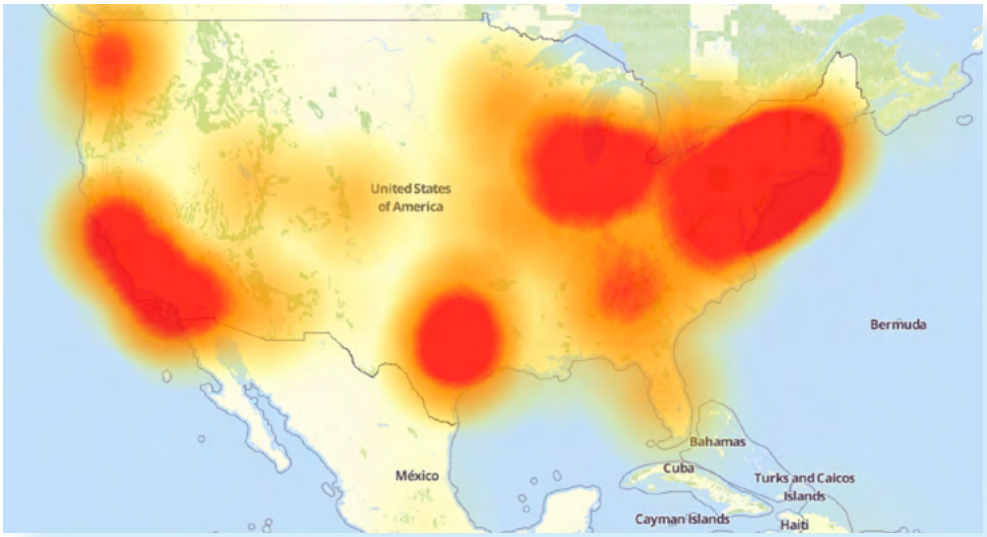
Но у этого есть и обратная сторона — наличие компьютера, управляющего всеми системами, да еще и подключенного к сети, делает такой автомобиль хорошей возможностью для хакеров. Взлом машины — это прямая угроза для жизни его владельца. Если злоумышленник получил удаленный доступ к автомобилю, это означает, что он может включить или выключить любую систему в любое время: повернуть руль, нажать на газ или тормоза, выключить фары. Таким способом можно добраться до машины, несущейся по шоссе где-то по стране, далеко от взломщика. Таким образом, автомобили дружно вошли в семью кибервещей со всеми вытекающими отсюда плюсами и минусами 1.12.

1.12

Наши дома все больше наполняются разнообразными «умными» устройствами. Уже сейчас система безопасности позволяет отслеживать появление посторонних людей и предметов, обеспечивает ваше спокойствие, а также позволяет вести удаленный видеоконтроль за маленькими детьми. На случай длительного отъезда может включаться режим симуляции присутствия хозяина, чтобы не давать ворам повода нанести вам визит. Пока настоящий «умный дом» — это дорогая игрушка для обеспеченных людей, но революция в домашнем хозяйстве пройдет очень быстро.

К сожалению, при разработке систем «умного дома» их авторы больше думают о комфорте, чем о безопасности, поэтому взламываются такие системы относительно легко по сравнению, например, с банковскими. Кроме того, получив контроль над устройствами «умного дома», злоумышленники формируют из них ботнет.

Ботнет — это набор компьютеров или «умных» устройств, подключенных к интернету, «ботов», которые находятся под удаленным управлением какой-либо внешней стороны. Так, в октябре 2016 года без доступа в интернет осталась большая часть пользователей на Восточном побережье США 1.13.



1.13

В атаке участвовали миллионы устройств — она была столь масштабной, что власти даже подумали, что это действия враждебного государства, но, как потом выяснилось, на самом деле это была работа гигантского ботнета Mirai (по-японски «будущее»). В отличие от других ботнетов, которые обычно состоят из компьютеров, ботнет Mirai в значительной степени состоял из так называемых устройств «Интернета вещей», таких как цифровые камеры и видеопроигрыватели.

Потом появились ботнеты, в состав которых вошли роутеры, «умные» лампочки, розетки, датчики движения, выключатели, камеры наблюдения и другие гаджеты. К 2017 году в интернете было 8,4 миллиарда таких «вещей», и большинство из них может стать легкой добычей хакеров.

Также есть камеры видеонаблюдения. Шалости хакеров могут быть не столь безобидны, если они получат доступ к видеопотоку из вашего дома 1.14.

1.14

Как защитить от взлома видеокамеру:

- устанавливать сложные пароли и менять их раз в месяц;
- отключать неиспользуемые функции, например, работу с облачными хранилищами.

В самом простом случае они выкладывают ролики со взломанных камер в соцсети в интернете, чтобы получить свою минуту славы. Но если взломщик будет располагать вашими персональными данными, то у него может появиться желание шантажировать вас под угрозой публикации видео. Этому риску чаще подвергаются известные люди, хотя и обычные граждане от него не застрахованы.

К сожалению, на текущий момент риск взлома видеокамер остается высоким. Чтобы свести его к минимуму, нужно следовать довольно простым правилам:

- во-первых, всегда надо обновлять прошивки таких камер и ставить сложные пароли для доступа к ним, а заодно почаще менять их. Как это сделать, обычно описывается в руководстве пользователя каждой такой камеры. Это минимально необходимые меры по защите;
- во-вторых, всегда надо отключать неиспользуемые функции. В первую очередь это касается разнообразных «облачных» сервисов, которыми оснащается все большее число камер.

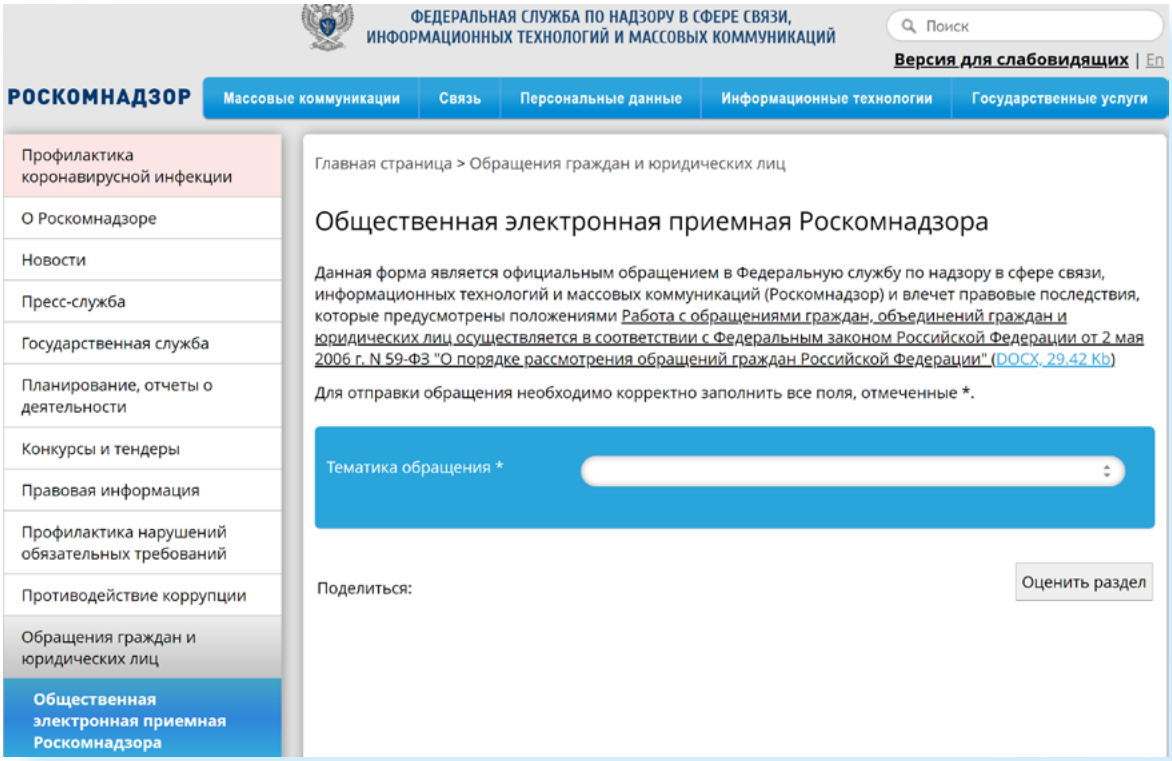
Тайна частной жизни в цифровом мире

Итак, мы живем в мире, где сохранить секретность чрезвычайно сложно. Само понятие «конфиденциальность» становится размытым, ведь мы же передаем свои данные третьим лицам.

Сегодня безопасностью становится прозрачность. Каждый должен понимать, как хранятся и используются эти данные. Именно по этому пути идет формирование новых законодательных норм и правил. Это и есть прозрачность.

Стоит ли паниковать, если произошла утечка паспортных данных? Вообще наши паспортные данные давно растекаются направо и налево. Как отмечают специалисты в НИУ ВШЭ, сегодня многие организации (например, гостиницы) требуют их предоставить, сканы документа остаются в салонах, где делаются копии. Паспортные данные можно найти даже в интернете в свободном доступе. Понятно, что часто срабатывает и человеческий фактор, и данные утекают из банков или государственных организаций через сотрудников.

Если вы нашли свои паспортные данные в открытом доступе, можно написать жалобу в **Роскомнадзор** — этот орган занимается в России контролем за защитой персональных данных и правильностью их передачи. Ссылка на форму обращения — **rkn.gov.ru/treatments/ask-question/**. На сайте **rkn.gov.ru** нужно перейти на главную страницу и слева в разделах выбрать **«Обращения граждан и юридических лиц»**, затем подраздел **«Общественная электронная приемная»** 1.15.



1.15

На данный момент подозрения об утечке данных — это не повод, чтобы менять паспорт. Такое условие не является основанием для замены документа, в МВД вам откажут.

Контрольные вопросы

1. Чем хакеры могут угрожать «умному» дому?
2. Как заботиться о своей цифровой репутации?
3. В чем разница между конфиденциальностью и анонимностью?
4. Почему нам так дороги наши аккаунты в соцсетях?
5. Чем опасны утечки персональных данных?
6. Почему списки контактов для нас ценны? Зачем они хакерам?
7. Почему надо защищать свой Wi-Fi?
8. Как защитить свои авторские права в интернете?
9. Назовите, что ценного у вас хранится в цифровом виде?
10. Какими способами преступники крадут цифровые деньги?