

Азбука интернета

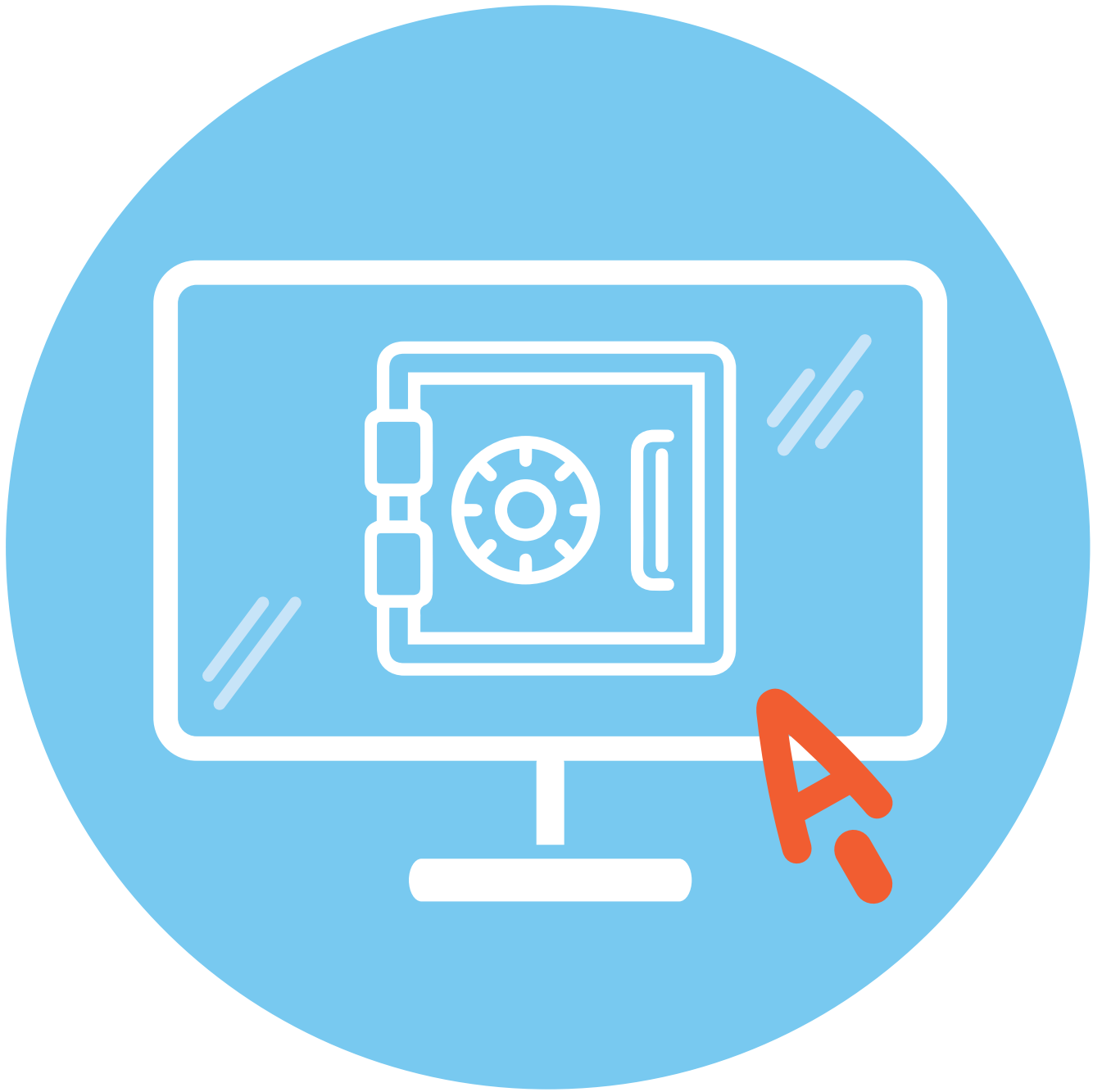
УЧЕБНОЕ ПОСОБИЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СТАРШЕГО ПОКОЛЕНИЯ:
КИБЕРБЕЗОПАСНОСТЬ



Оглавление

Глава 1. Цифровые ценности	5
Деньги и бонусы	6
Персональные данные	7
Аккаунты в социальных сетях, репутация и тайна частной жизни	9
Переписка: почта и мессенджеры, контакты, заметки, цифровые коллекции	11
Авторские права на цифровые произведения	13
Цифровые ресурсы и виртуальные вещи	15
«Умная» техника и «умный» дом	15
Тайна частной жизни в цифровом мире	18
Глава 2. Ваш «цифровой след» в интернете	21
Что такое «цифровой след»?	21
Что значит «вычислить пользователя по IP-адресу»?	22
Какое отношение к безопасности имеют cookie(куки)-файлы?	23
Как еще собирается и анализируется информация об интернет-пользователях	26
Почему нужно обращать внимание на Политику конфиденциальности?	27
Хеширование и шифрование информации	28
Анонимность для «чайников»: зачем нужен VPN?	31
Можно ли удалить все ваши «следы» в интернете?	33
Глава 3. Как действуют мошенники в интернете, способы защиты	37
Вредоносные программы	37
Как выбрать антивирус	41
Социальная инженерия. Примеры мошеннических схем	43
Безопасность на сайтах объявлений	45
Безопасность в социальных сетях и электронной почте	46
Безопасность в финансовых вопросах	47
Безопасность при интернет-покупках и интернет-заработке	48
Куда сообщить о мошенниках?	49
Риски публичных Wi-Fi сетей	51
Внешние носители	52
Какую информацию нельзя доверять интернету	53

Глава 4. Настройка безопасности компьютера	55
Зачем нужен Firewall (Файервол)/Брандмауэр	55
Безопасная настройка браузера	56
Настройки личного аккаунта в браузере	62
Нужно ли очищать кэш и куки	66
Блокировщики рекламы	67
Безопасный поиск в интернете	68
Глава 5. Система надежных паролей	71
Как работает цифровой пароль	71
Как работает сервис восстановления паролей	71
Как мошенники получают доступ к паролям	73
Двухфакторная аутентификация, биометрия, QR-коды	75
Пароли для финансовых приложений	79
Как придумать надежный пароль	79
Как и где хранить пароли, менеджер паролей	81
Глава 6. Сохранность личной информации	85
Несем устройство в ремонт	85
Шифрование жесткого диска	86
Копирование и удаление важной информации вручную	88
Резервное копирование и облачные сервисы для сохранения ваших данных	91
Что делать, если взломали аккаунт	95
Глава 7. Безопасность мобильного устройства	99
Особенность мобильных гаджетов с точки зрения киберугроз	99
Основные рекомендации безопасной работы на мобильном устройстве	100
Биометрия для телефона	101
Работа в публичных точках доступа Wi-Fi	102
Работа в Bluetooth	103
Феномен и риски селфи	104
Чьи в семье сим-карты?	105
Безопасная работа смартфона в режиме «Точки доступа»	106
Глава 8. Как защитить детей в интернете	109
Смартфон для ребенка. Настройки	109
Опция «Родительский контроль»	112
Телефон в школе	116
Как противостоять кибербуллингу и онлайн-грумингу	116
Как оградить ребенка от деструктивных подростковых сообществ	118
Пароли и дети	119



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

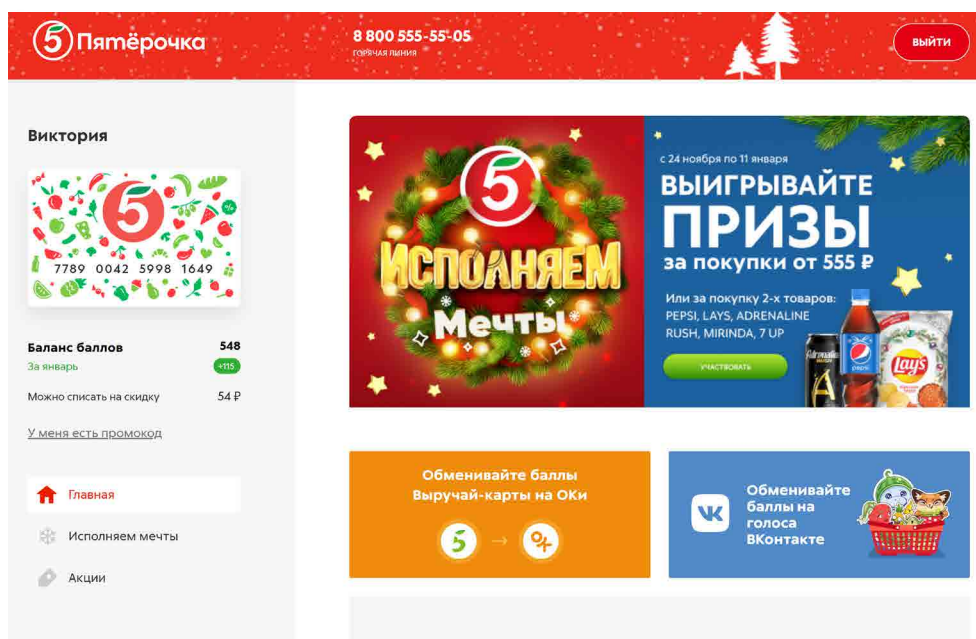
Кроме наличных, которые лежат у вас в кармане, все остальные ваши деньги существуют в цифровом виде. Пенсия на карточке, депозит в банке, баланс на счете мобильного телефона и пр. Это не более чем цифры в какой-то базе данных, но точно так же их можно потерять или стать жертвой грабителей.

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 попадают 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

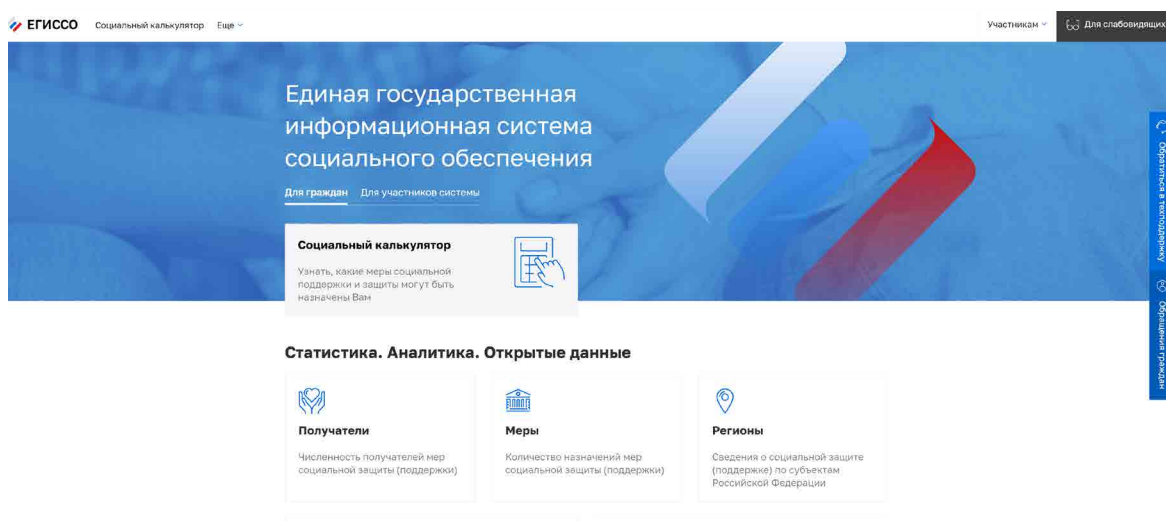
Формально все эти баллы и бонусы деньгами не являются, но с практической стороны они равнозначны настоящим деньгам. Если вы потеряете саму карточку, то это нестрашно – попросите новую. А вот если кто-то получит доступ к вашему аккаунту, то этот кто-то, скорее всего, найдет способ, как использовать ваши 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. Facebook поплатился именно за это – соцсеть передала данные пользователей компании Cambridge Analytica, которая якобы помогла победить на выборах президенту США.

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

The screenshot shows the official website of the President of Russia. The search results for the Federal Law No. 152-FZ of July 27, 2006, are displayed. The page includes a search bar, navigation menu, and a list of related documents.

Президент России | События | Структура | Видео и фото | **Документы** | Контакты | Поиск

Новости | Поручения Президента | **Банк документов** | Справка | Конституция России

Название документа или его номер
Текст в документе
Вид документа
Все
Дата вступления в силу... или дата принятия
Найти документ

Официальный портал правовой информации pravo.gov.ru

14 декабря 2020 года
Указ Президента Российской Федерации от 14.12.2020 г. № 787
О некоторых вопросах деятельности комиссий по вопросам помилования на территориях субъектов Российской Федерации
14 декабря 2020 года

Указ Президента Российской Федерации от 14.12.2020 г. № 786
О праздновании 100-летия основания конструкторского бюро публичного акционерного общества «Туполев»

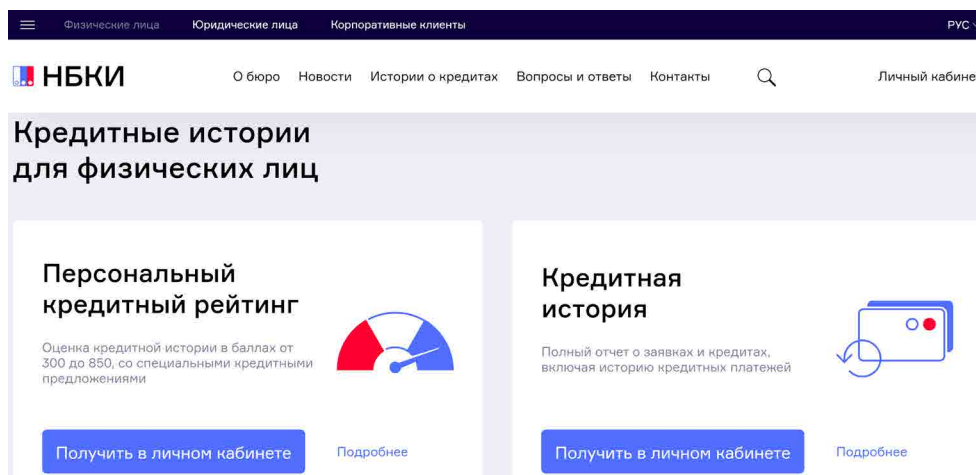
Федеральный закон от 27.07.2006 г. № 152-ФЗ
О персональных данных
pravo.gov.ru

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О персональных данных
Принят Государственной Думой 8 июля 2006 года

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 убе- речься 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 бес- платно прямо на сайте. Обратите внимание, что таких кредитных бюро несколько. Одно из крупнейших — nbki.ru 1.4.

1.4

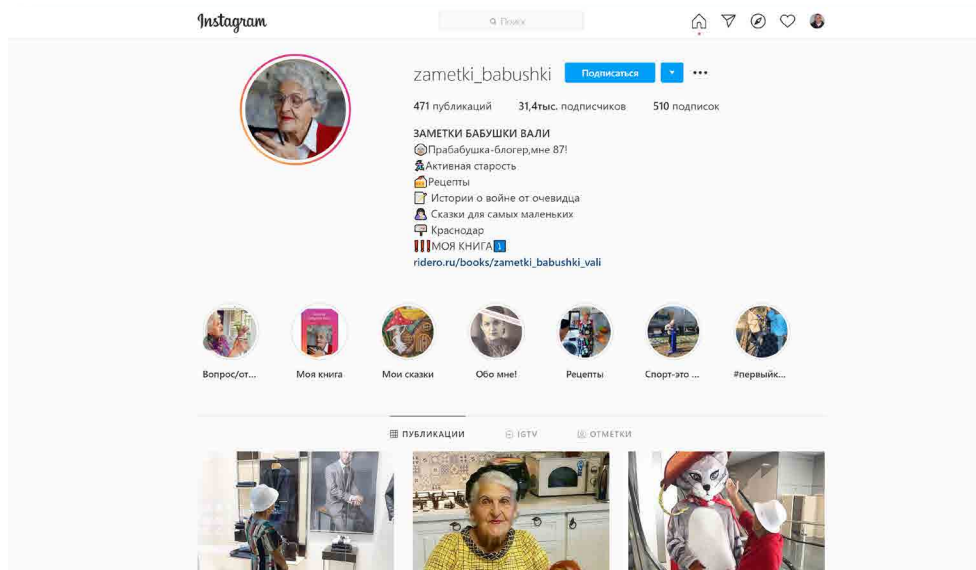


Считайте такой ежегодный запрос одним из элементов цифровой «гигиены», даже если вы не теряли паспорт.

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 соци- альных сетях может быть очень болезненно психологически, а иногда и финансово. Есть люди, для которых ведение аккаунта – это уже работа 1.5.

1.5

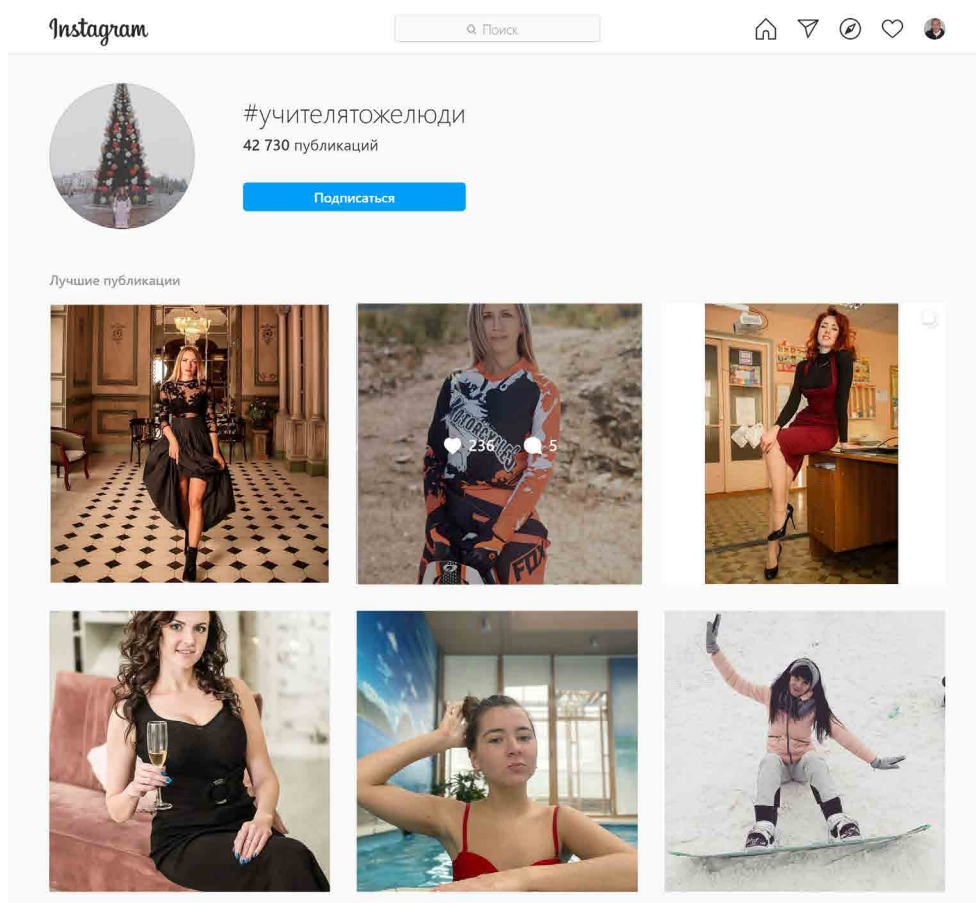


Набрав нужное количество подписчиков, автор может монетизировать свой труд. Аккаунт работает как рекламная площадка. И в тот момент, когда страничка в социальных сетях начинает интересовать рекламодателей, к ней появляется интерес и у мошенников, которые могут завладеть вашим аккаунтом. Поэтому, начиная 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](#).

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

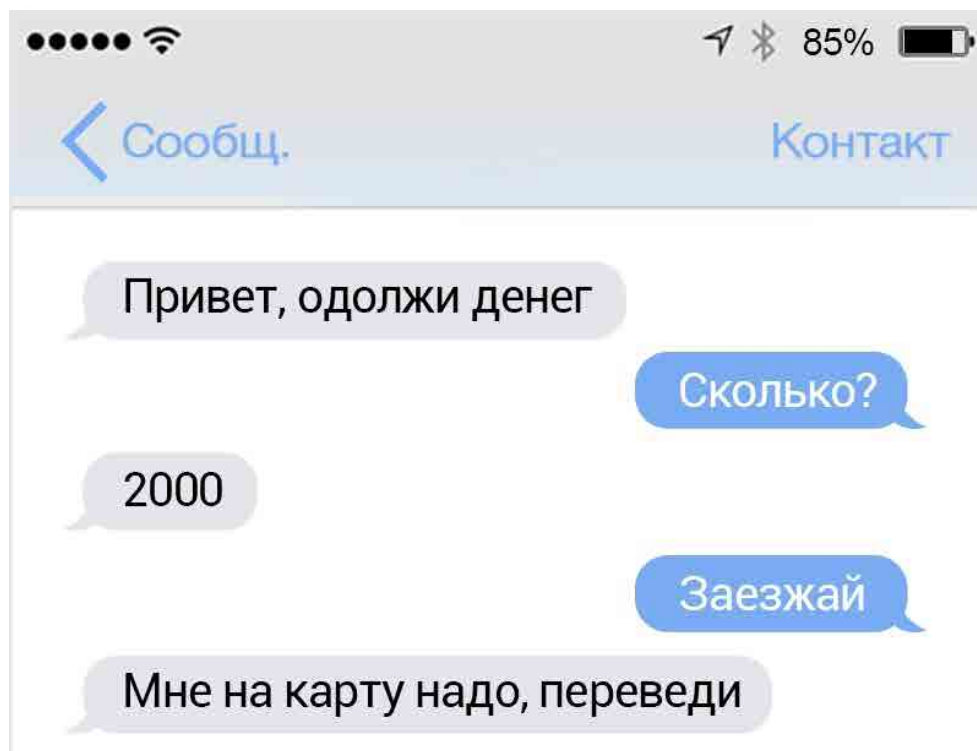
Из тридцати томов полного собрания сочинений и писем Антона Чехова письма составляют двенадцать томов. По объему переписки мы сегодня, пожалуй, превосходим Антона Павловича.

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



Таковыми 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.

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.

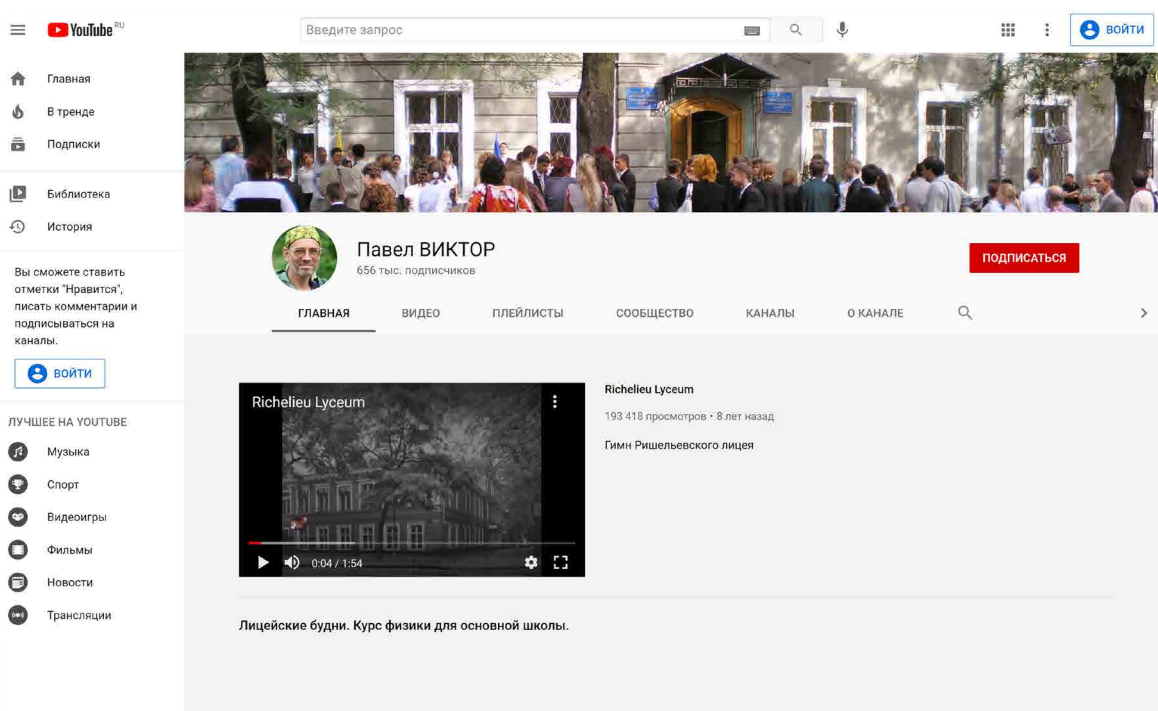
Но тут появляется другой риск – можно потерять контроль над своим аккаунтом, и тогда это будет большой проблемой, потому что все контакты тоже будут потеряны. Заполучив его, хакеры могут делать рассылки вашим знакомым от вашего имени, что сразу повышает их уровень доверия к полученной информации, и человек 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.

Авторские права на цифровые произведения

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

Например, 64-летний учитель физики из Одессы Павел Андреевич Виктор по использованию современных технологий опережает многих молодых коллег. Уже пять лет он снимает свои уроки для учеников 7-11-х классов и выкладывает их на YouTube. Сейчас их смотрят русскоязычные зрители во всем мире: у канала учителя более 650 тысяч подписчиков, а общее число просмотров перевалило за 8 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. 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

1 Лицензионная Экспертиза
Мне нужна помощь в выборе лицензии.

2 Подтвердите, что лицензирование CC подходит
Я подтвердил целесообразность лицензирования CC.

3 Определение
Любой может использовать мои работы, даже не давая мне атрибуции.

4 Коммерческое использование
Другие не могут использовать мою работу в коммерческих целях.

5 Производные Работы
Другие могут использовать мою работу только в неприкосновенной форме.

6 Требования к Совместному использованию
Этот шаг отключен из-за выбора ND, который не допускает адаптации.

7 Сведения об атрибуции
Заполнение этой формы необязательно, но помогает другим пользователям приписывать вам вашу работу и заполняет машиночитаемый код.

Название работы

Творец труда **!**

Ссылка на работу

РЕКОМЕНДУЕМАЯ ЛИЦЕНЗИЯ

CC BY-NC-ND 4.0
Атрибуция-Некоммерческая-NoDerivatives 4.0 International

Эта лицензия требует, чтобы повторные пользователи отдавали должное создателю. Это позволяет повторным пользователям копировать и распространять материал на любом носителе или формате в неприкосновенной форме и только в некоммерческих целях.

! **АВТОР:** Заслуга должна быть отдана тебе, создателю.

NC: Разрешено только некоммерческое использование вашей работы. Некоммерческие средства не предназначены в первую очередь для получения коммерческой выгоды или денежной компенсации или не направлены на нее.

ND: Никакие производные или адаптации вашей работы не допускаются.

[Смотрите Лицензионный акт](#)

ОТМЕТЬТЕ СВОЮ РАБОТУ

Выберите вид работы, чтобы получить соответствующий лицензионный код или маркировку общественного домена.

Веб-сайт **Печатная работа или Носитель**

Скопируйте приведенный ниже текст и вставьте его на титульную и/или авторскую страницу вашей печатной работы или презентации или в титры вашего носителя.

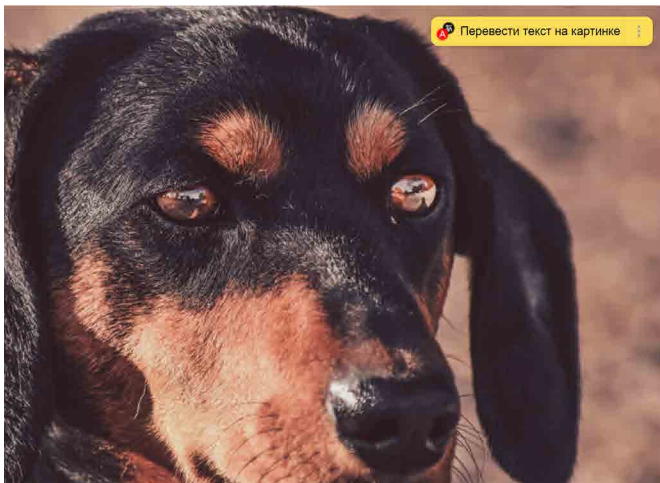
Обычный Текст

Эта работа лицензирована в соответствии с CC BY-NC-ND 4.0. Чтобы просмотреть копию этой лицензии, посетите <http://creativecommons.org/licenses/by-nc-nd/4.0/>

сокращение лицензии **ПОЛНОЕ НАЗВАНИЕ ЛИЦЕНЗИИ** **Копировать**

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 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



Перевести текст на картинке

АВТОР: Бикански

ЛИЦЕНЗИЯ: ✓ Бесплатное использование CC0

портрет головы таксы, нос чистокровной собаки, глаза домашнего животного, милая охотничья собака, гончая, собачий мех, щенок, выглядящий забавно, глаза очаровательной породы домашних животных, черно-коричневые собаки, родословная охранных животных, фауна зоология, хищные позвоночные крупным планом, детали, бесплатные изображения, светло-коричневая серьезная кожа, красивая фотография

дополнительная информация:
NIKON D5500 F/9.0 ISO: 500 1/400 c 260 MM **!**

Скачать бесплатно

Забываясь 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.

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.

Так же 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.



1.11

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.

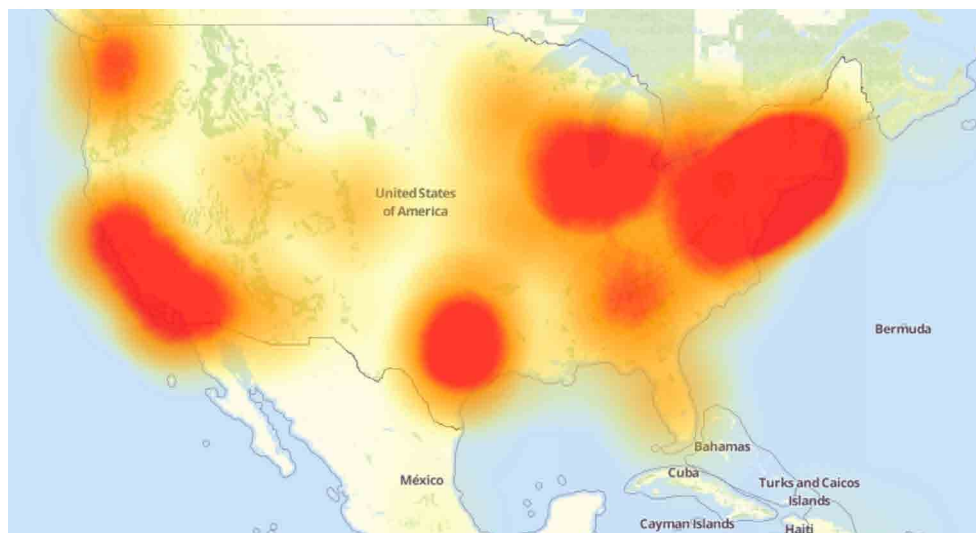
1.12



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 вору 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 видео-проигрыватели.

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 получают 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 на YouTube, 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.

The screenshot shows the website of the Federal Service for Supervision of Communications, Information Technologies, and Mass Communications (Roskomnadzor). The page is titled "Общественная электронная приемная Роскомнадзора" (Public Electronic Reception of Roskomnadzor). It includes a search bar, navigation tabs for "Массовые коммуникации", "Связь", "Персональные данные", "Информационные технологии", and "Государственные услуги". A left sidebar contains various service categories, with "Общественная электронная приемная Роскомнадзора" highlighted. The main content area explains that this is an official form for submitting complaints to Roskomnadzor and provides instructions on how to use it, including a dropdown menu for "Тематика обращения *" (Topic of the appeal).

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





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.

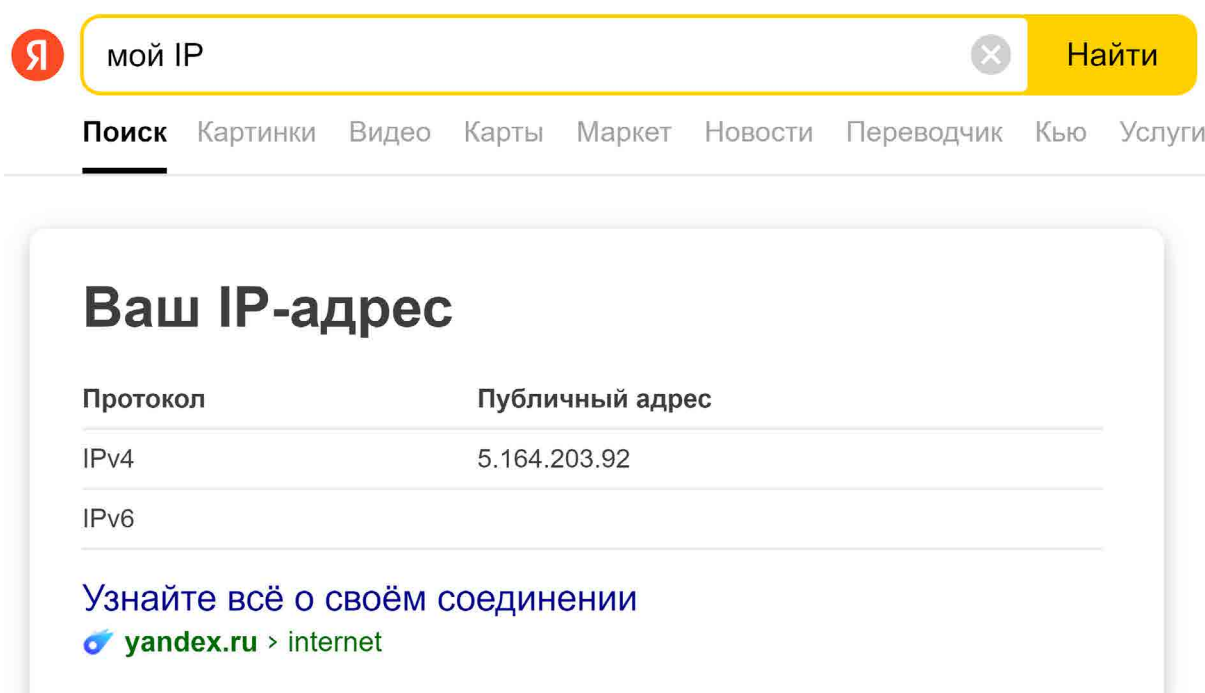
Если вы живете в большом городе, то каждый день попадаете в поле зрения камер видеонаблюдения. Например, в Москве в 2019 году их насчитывалось больше 170 тысяч, и мэрия планировала установить еще, обещая даже запустить систему распознавания лиц. Так что в скором времени все наши перемещения по городу 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



The screenshot shows a search engine interface with a search bar containing the text "мой IP". Below the search bar, there are navigation tabs: "Поиск", "Картинки", "Видео", "Карты", "Маркет", "Новости", "Переводчик", "Кью", and "Услуги". The search results display the heading "Ваш IP-адрес" followed by a table with two columns: "Протокол" and "Публичный адрес". The table lists the IPv4 address as 5.164.203.92 and the IPv6 address as empty. Below the table, there is a link "Узнайте всё о своём соединении" and a breadcrumb trail "yandex.ru > internet".

Протокол	Публичный адрес
IPv4	5.164.203.92
IPv6	

[Узнайте всё о своём соединении](#)
[yandex.ru](#) > [internet](#)

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 (cache) 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

Мы используем файлы cookie, чтобы улучшить работу сайта. Дальнейшее пребывание на сайте означает согласие с их применением.
Подробнее

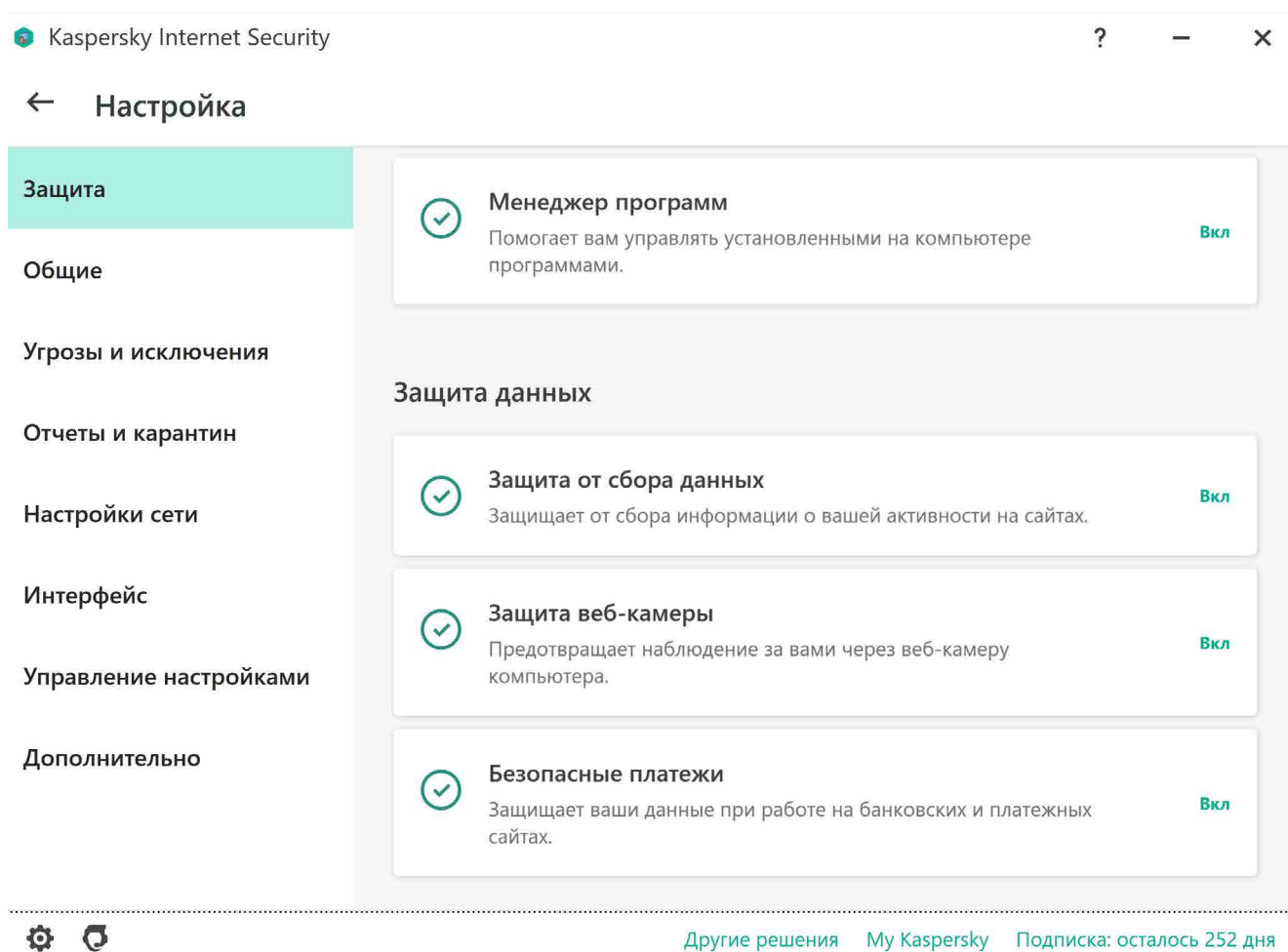
Данные данные на...
Услуга — УП
продавца и покуп

Принять и закрыть

Смысл в том, что пользователь может отказаться от использования куки-файлов. Но тут тоже есть подводные камни. Иногда куки устанавливаются 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 Секьюрети) нужно перейти в «Настройки», затем в раздел «Защита» и поставить в положение «Включено» функцию «Защиты от сбора данных» 2.3.

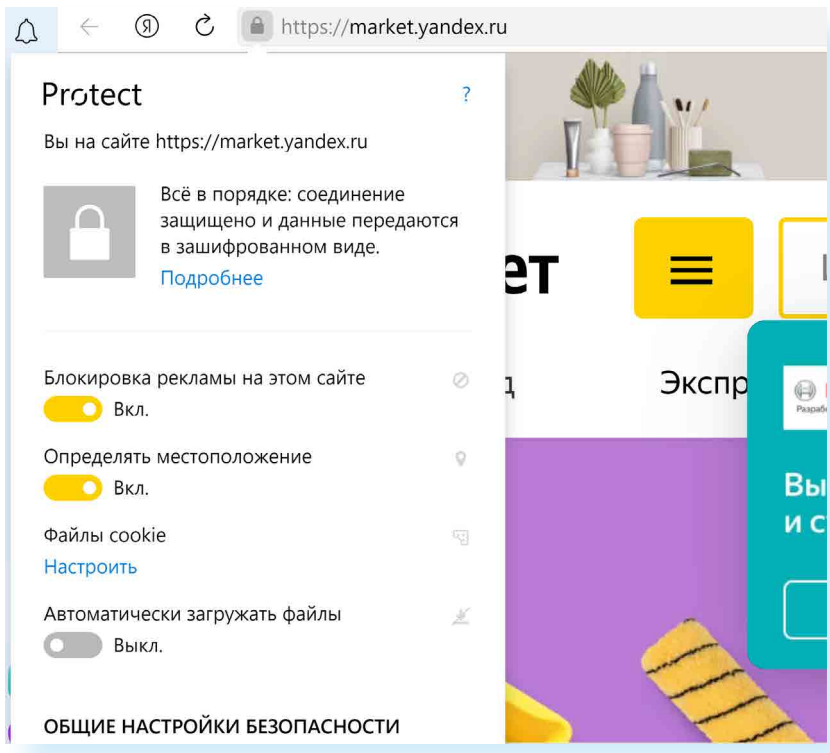
2.3



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:

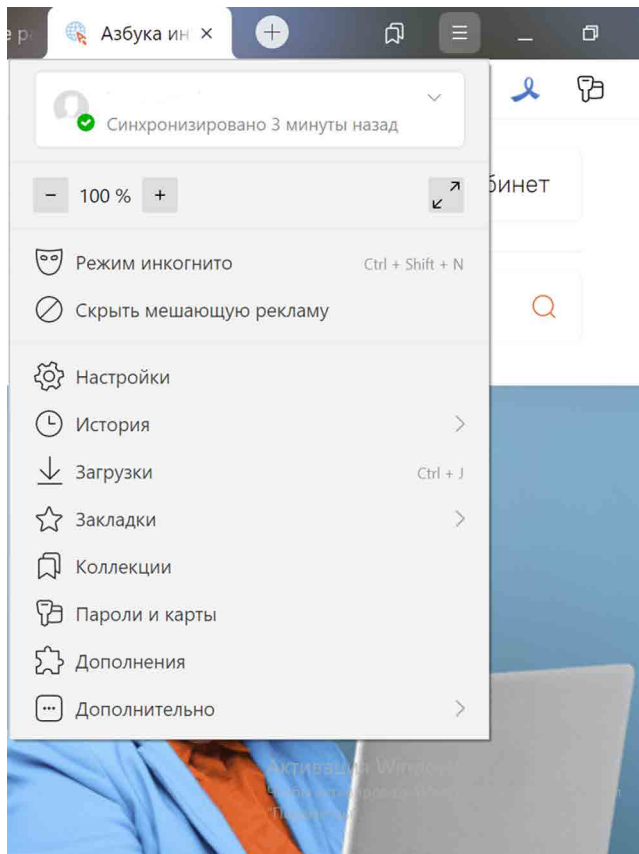
1. Используйте только защищенное соединение **https**, особенно при посещении интернет-магазинов. Это первые буквы в адресе сайта. Кликните на изображение замочка в строке браузера. Первые буквы указывают на защищенное соединение 2.4.



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

Google Политика конфиденциальности и Условия использования

Обзор	Политика конфиденциальности	Условия использования	Технологии	Часто задаваемые вопросы
Введение				
Какие данные мы собираем				
Зачем Google собирает данные				
Ваши настройки доступа				
Передача Вашей информации				
Защита Вашей информации				
Экспорт и удаление Вашей информации				
Хранение Вашей информации				
Соблюдение нормативных требований и взаимодействие с регулирующими органами				

Мы регистрируем информацию о приложениях, браузерах и устройствах, которые Вы используете для доступа к сервисам Google. Это обеспечивает работу таких функций, как автоматическое обновление приложений и затемнение экрана при малом заряде батареи.

Помимо прочего, мы собираем уникальные идентификаторы, а также такие данные, как тип и настройки браузера и устройства, операционная система, мобильная сеть (включая название оператора и номер телефона) и номер версии приложения. Нами также регистрируется информация о взаимодействии Ваших приложений, браузеров и устройств с нашими сервисами, в том числе IP-адрес, отчеты о сбоях, сведения о действиях в системе, дата и время, когда Вы посетили наш ресурс, и URL, с которого Вы на него перешли (URL перехода).

Эти данные мы получаем, когда продукт Google с Вашего устройства обращается к нашим серверам, например при установке приложения из Play Store или проверке на наличие обновлений. Устройства Android с приложениями Google Apps периодически связываются с серверами Google и передают данные о своем статусе и подключении к нашим сервисам. К таким данным относятся, в частности, тип устройства, название оператора мобильной связи, отчеты о сбоях и список установленных приложений.

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.

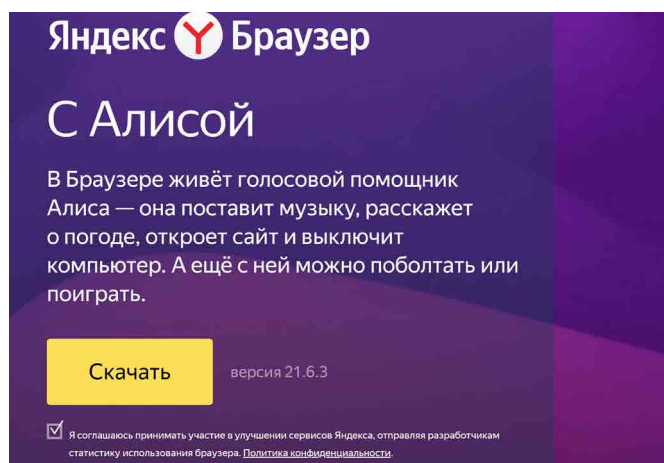
Сбор данных периодически приводит к крупным скандалам. Уместно вспомнить историю с Facebook и Cambridge Analytica. Под видом теста они собрали информацию о пользователях, а затем использовали ее для предсказания итогов выборов Президента США, или переменную борьбу и сотрудничество Mail.Ru Group и Национального 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 посещения 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.

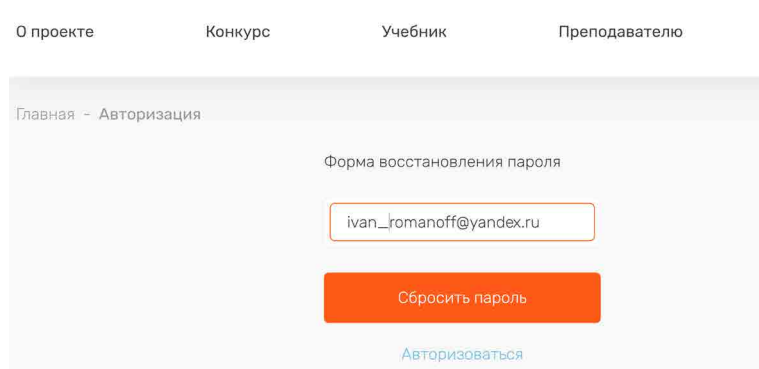
Компании часто обновляют Политику конфиденциальности. Например, в документе мессенджера WhatsApp (ВотсАп) появилась информация, что пользователи обязаны предоставлять компании Facebook доступ к номерам телефонов, именам и фото профилей, сведениям о транзакциях, диагностическим данными из приложений и 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](#).

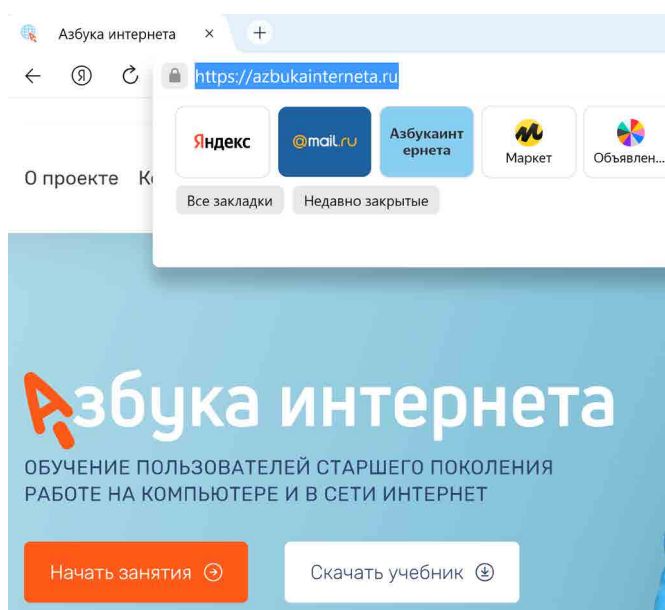


2.8

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

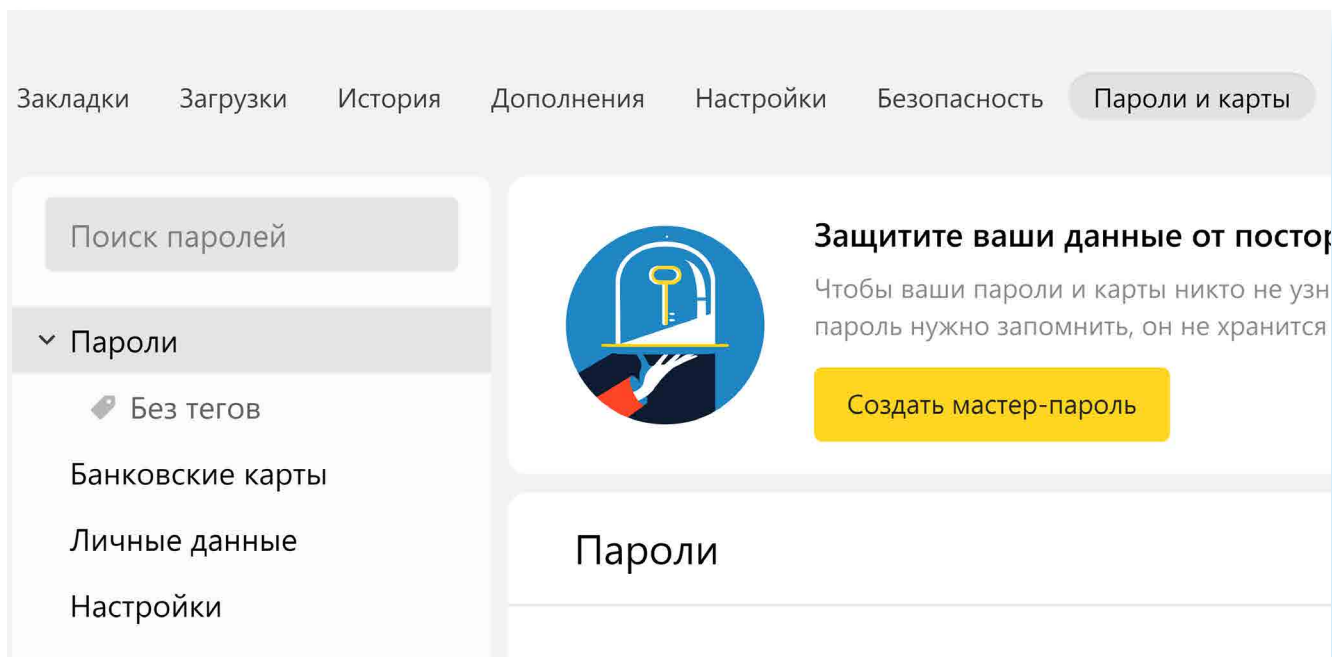
Встроено шифрование и в самый популярный сегодня стандарт сотовой связи GSM.

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](#).

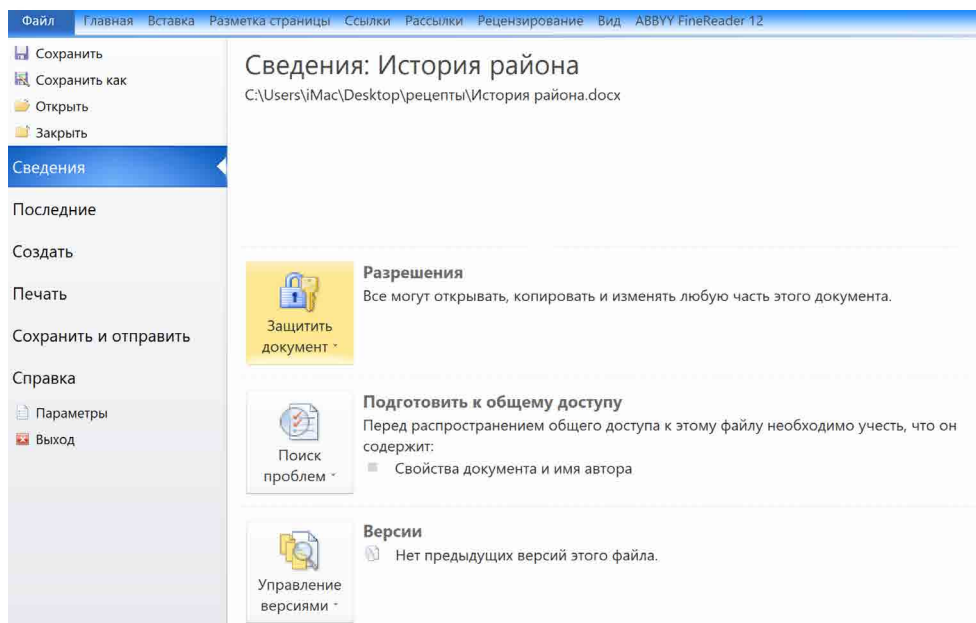
2.10



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 действиях 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.

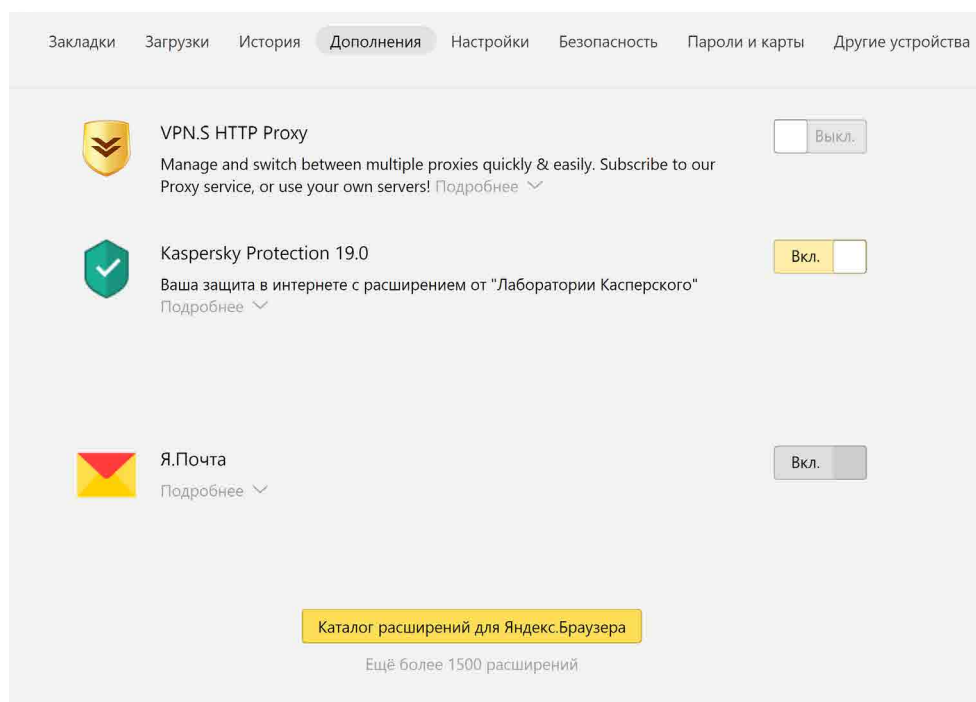
Если вы все же решили использовать анонимную сеть:

- 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 сверху);
- 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?

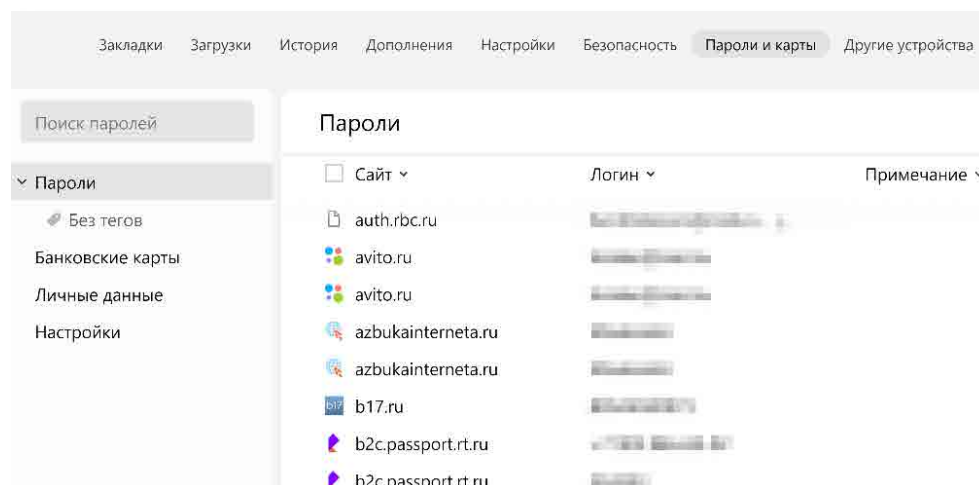
В теории можно попробовать полностью удалить свои данные из интернета. Удалить свои аккаунты в социальных сетях (не везде это легкий процесс), удалить свои аккаунты в почтовых сервисах, в мессенджерах. Если есть упоминания на каких-то сайтах, также попросить владельцев убрать ваши данные. По закону они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

Deseat.мне

Вход

Очистите свое присутствие в Интернете

Мгновенно получите список всех ваших учетных записей, удалите те, которыми вы не пользуетесь.

Начало работы

Как это работает

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.



■ Выгрузить данные о себе

Мы хотим, чтобы Вы понимали, какие данные о Вас мы можем собирать, хранить или обрабатывать. У Вас есть возможность запросить архив данных о Вашем профиле ВКонтакте. Сейчас выгрузка работает в тестовом режиме, но мы прикладываем все усилия для совершенствования этой функции, чтобы Вам было проще получить необходимую информацию.

Вы можете скачать данные о своём профиле ВКонтакте в любой момент, независимо от страны проживания. В том числе пользователи из стран ЕС имеют возможность запросить данные в соответствии с GDPR. Это максимально легко и безопасно. Запрос архива нужно подтвердить с помощью одноразового кода, а уникальную ссылку для скачивания невозможно открыть из другого профиля. Вы также можете добавить дополнительный уровень защиты — и зашифровать архив с помощью персонального ключа [OpenPGP](#).

Подготовка выгрузки занимает некоторое время, этот процесс может длиться несколько дней. Вы получите уведомление, когда архив будет готов для скачивания. Для безопасности Ваших данных он будет доступен для загрузки в течение ограниченного времени.

Копия Вашей информации из ВКонтакте будет выгружена в ZIP-архиве, поэтому данные удобнее смотреть на компьютере. Для большего комфорта мы поделили информацию на разные категории. Например, легко можно найти список фотографий, которым Вы поставили отметку «Нравится», историю денежных переводов или круг Ваших интересов, которые учитываются при таргетинге рекламных объявлений.

[Запросить архив](#)

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?





Как действуют мошенники в интернете, способы защиты

3

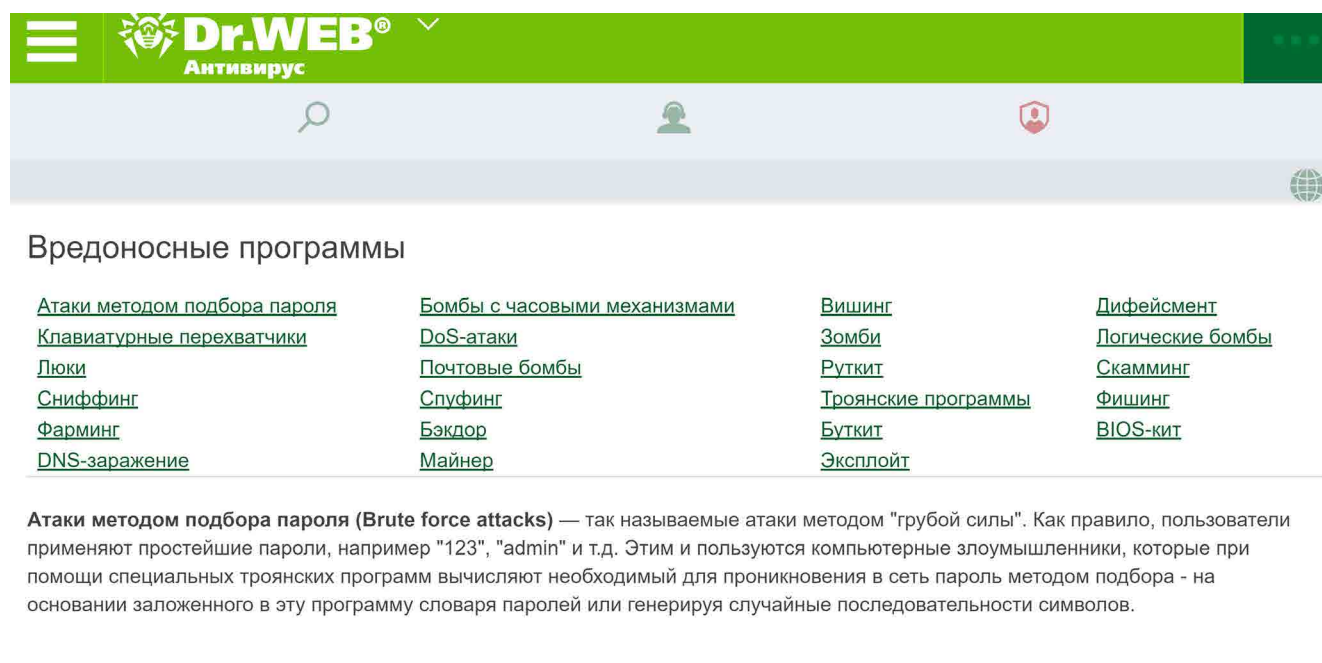
ГЛАВА

Мошенники в интернете преследуют главную цель – получить деньги либо заработав на продаже личных данных, либо просто украв ваши деньги. Для этого есть технологические способы, когда, используя уязвимость вашего устройства, мошенники с помощью вредоносных программ получают доступ к вашим данным и счетам, а есть то, что называют «социальной инженерией», когда используют психологические способы влияния на пользователей для кражи личных средств.

Вредоносные программы

Один из самых распространенных способов перехватить у вас информацию – запуск на ваше устройство вредоносных программ. Развиваются цифровые технологии, совершенствуются шпионские IT-инструменты. Вот, например, какой список вредоносных программ можно увидеть на сайте антивирусной программы «Доктор Web» 3.1.

3.1



The screenshot shows the Dr.Web Antivirus interface. At the top, there is a green header with the Dr.Web logo and the text 'Антивирус'. Below the header, there is a search bar and a user profile icon. The main content area is titled 'Вредоносные программы' (Malware) and displays a grid of 16 categories of malware, each with a link to more information:

Атаки методом подбора пароля	Бомбы с часовыми механизмами	Вишинг	Дифейсмент
Клавиатурные перехватчики	DoS-атаки	Зомби	Логические бомбы
Люки	Почтовые бомбы	Руткит	Скамминг
Сниффинг	Слуффинг	Троянские программы	Фишинг
Фарминг	Бэкдор	Буткит	BIOS-кит
DNS-заражение	Майнер	Эксплойт	

Below the list, there is a paragraph explaining Brute force attacks:

Атаки методом подбора пароля (Brute force attacks) — так называемые атаки методом "грубой силы". Как правило, пользователи применяют простейшие пароли, например "123", "admin" и т.д. Этим и пользуются компьютерные злоумышленники, которые при помощи специальных троянских программ вычисляют необходимый для проникновения в сеть пароль методом подбора - на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.

Остановимся на основных разновидностях.

Вирус – это программа, которая внедряется в установленные программы и приложения на компьютере. Вирус начинает работать тогда, когда вы запускаете данную программу или приложение.

Подцепить вирус можно на зараженном сайте, нажав на ссылку или файл в подозрительном сообщении или письме, или кликнув на всплывающее окно, призывающее вас обязательно перейти на какой-то ресурс.

Правда, сейчас вирусов становится меньше. Их быстро распознают и блокируют и настройки браузера, и операционной системы, и антивирусной программы.

Червь – тоже вирус, но действует по-другому: распространяет сам себя по компьютеру. Его также можно «занести» через ссылки или файлы в переписке.

Руткит – это особая часть вредоносных программ, которая разработана так, чтобы скрыть свое присутствие в операционной системе от защитного программного обеспечения.

Однако сложные современные антивирусные программы в состоянии обнаружить и обезвредить практически все существующие разновидности руткитов.

Троян, как правило, загружается на устройство под видом законного приложения, но на самом деле делает то, что нужно злоумышленникам. Это одна из распространенных вредоносных программ.

С годами трояны становятся все сложнее: есть трояны-бэкдоры, которые пытаются взять на себя управление компьютером, трояны-загрузчики, устанавливающие вредоносные коды, или трояны-вымогатели.

Подцепить трояна можно легко при скачивании программ, приложений или даже просто картинок.

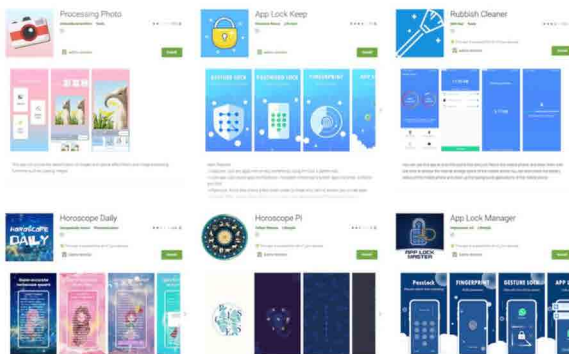
Вот как действовал «скайповский» троян. Он отправлял слово «Привет» всем пользователям в списке контактов жертвы каждый раз, когда она выходила в онлайн. На самом деле троян вместе с «приветом» отправлял еще и фишинговую ссылку (ссылку, которая вела на подставной сайт).

Достаточно много троянов антивирусные программы находят и в мобильных приложениях, в том числе даже в тех, которые можно найти в официальном магазине Google Play [3.2](#).

2021

«Доктор Веб» обнаружил в каталоге Google Play вредоносные приложения

1 июля 2021 года компания «Доктор Веб» сообщила, что обнаружила в каталоге Google Play вредоносные приложения, ворующие логины и пароли пользователей Facebook. Эти трояны-стилеры распространялись под видом безобидных программ, общее число установок которых превысило 5 856 010.



3.2

Один из самых опасных троянов – вымогатель, или шифровальщик. «Поселившись» в устройстве, он шифрует файлы, а иногда и всю систему, и требует деньги за расшифровку.

Даже если вы найдете и удалите с помощью антивирусной программы вредоносного шифровальщика, файлы могут так и остаться зашифрованными.

Чтобы не стать жертвой вредоносного программного обеспечения, нужно соблюдать простые правила:

- не открывать подозрительные письма или сообщения от незнакомых пользователей в электронной почте и мессенджерах;
- не переходить по рекламным баннерам, сулящим выигрыши или слишком дешевые предложения покупки;

Например, мошенники часто ловят пользователей на любопытстве. Вы можете увидеть громкие сообщения типа «Секретные подробности из жизни Аллы Пугачевой». Вы нажимаете на ссылку, а там вас просят скачать последнюю версию Adobe Flash, но вместо программы Adobe Flash вы получаете вредоносную программу на ваш компьютер.

- устанавливать программы и приложения только с официальных сайтов;
- обращать внимание на настройки безопасности в мобильных приложениях, ограничивать доступ приложения к вашим данным;
- проверять на безопасность подключенные к вашему устройству переносные USB-накопители;
- по возможности делать резервные копии данных со своего компьютера.

Как могут быть занесены вредоносные программы на устройство?

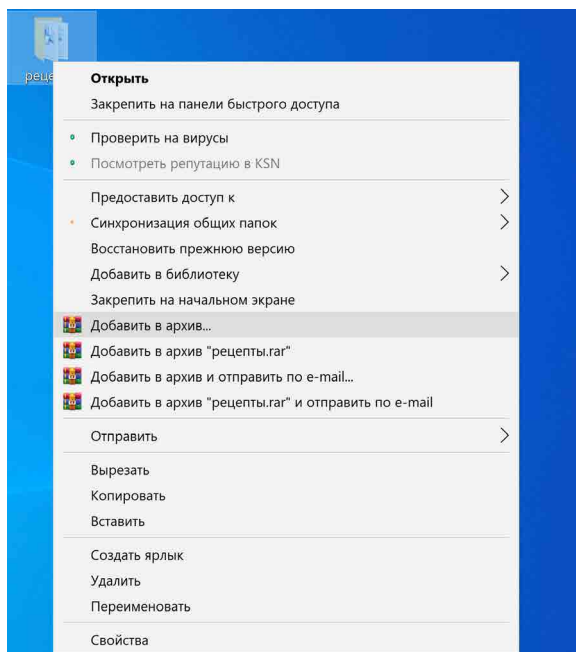
- Через ссылки и файлы, присланные в подозрительных письмах или сообщениях.
- При нажатии на рекламный баннер, обещающий большой выигрыш или выгодную покупку.
- Через USB-накопитель.
- При установке программы или приложения с неофициального сайта.

Например, копии важных файлов можно хранить на USB-накопителях или в облачном хранилище.

Чтобы разместить папку с фотографиями в облачном хранилище Яндекс. Диска, нужно:

1. Подготовить папку с фотографиями. Вы можете ее сжать, тогда она займет меньше места в облачном хранилище. Наведите на нее курсор и кликните правой кнопкой мыши. В открывшемся меню выберите программу для архивирования файлов. В нашем примере WinRAR 3.3.

3.3



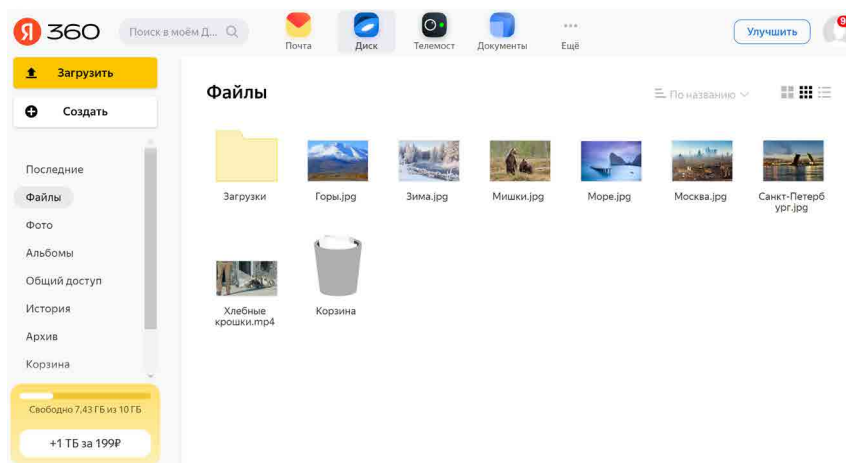
2. Завести аккаунт в системе Яндекс. Можно просто зарегистрировать электронную почту на Яндексе.

Подробнее как завести электронную почту можно увидеть в главе 7 «Электронная почта» базового курса «Азбука интернета».

3. Затем зайдите в свою электронную почту, выберите вверху вкладку «Диск».

4. Выберите «Загрузить файлы» 3.4.

3.4



5. В открывшемся окне найдите на компьютере вашу заархивированную (сжатую) папку. Выделите ее. Нажмите «Открыть». Папка загрузится.

Теперь папка будет храниться в облачном хранилище, которое привязано к вашей Яндекс.Почте. Зная логин и пароль от электронной почты, вы всегда сможете получить доступ к данной папке с любого компьютера. А, значит, восстановить ваши фотографии, если вдруг они будут удалены на компьютере трояном.

Как выбрать антивирус

Самой надежной защитой для компьютера, конечно, станет установка антивирусной программы.

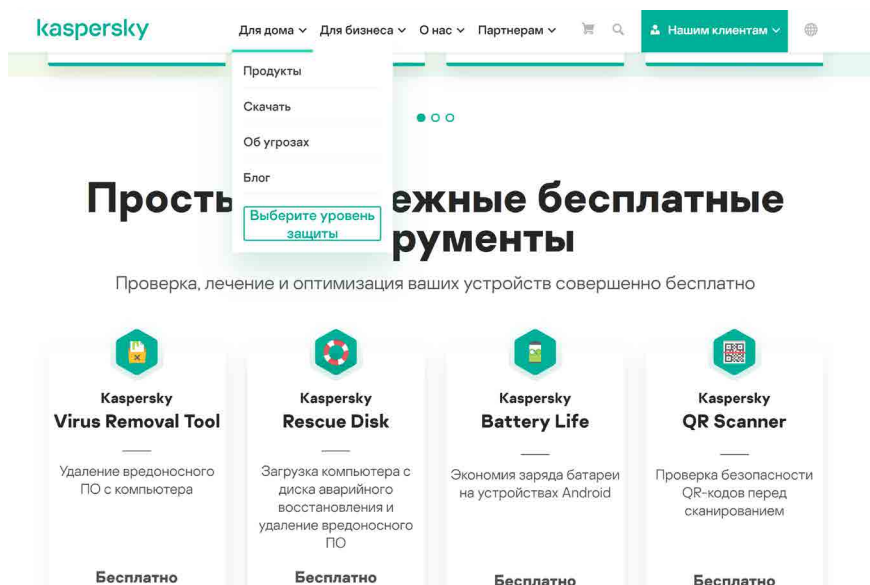
Если на компьютере не установлена антивирусная программа, мы не советуем выходить в интернет, так как в этом случае очень высок риск заражения устройства вредоносными программами.



Антивирусные программы могут быть бесплатными и платными. Как правило, в бесплатных версиях их функционал ограничен.

Но часто крупные известные компании именно бесплатно предоставляют доступ к небольшим программам, которые сканируют и помогают удалить различные зловредные программы в ситуации, когда вы видите, что компьютер, скорее всего, «заражен».

Например, на сайте Лаборатории Касперского, чтобы скачать такую программу (утилиту), нужно вверху выбрать раздел «Для Дома», а затем нажать на пункт «Скачать». Откроется страница, где внизу вы найдете блок «Простые и надежные бесплатные инструменты». Как видите, две из них для мобильных телефонов, в том числе на проверку QR-кодов, которые тоже могут перенаправлять на вредоносные ссылки, и две программы для компьютеров с возможностью «лечения» компьютера 3.5.



3.5

Как установить антивирусные программы?

- С официального сайта разработчика программы.
- Включить услугу установки антивирусной программы в тариф интернет-провайдера.

Они абсолютно бесплатны и, если вы не уверены в защите своего устройства, можно скачать такую программу и периодически ее запускать. Сама она не отслеживает вашу активность в отличие от серьезных антивирусных программ.

Обратите внимание, что антивирусы часто предлагают и провайдеры при подключении вас к интернету. Они могут входить в пакетное предложение. Можно сразу выбрать эту услугу, подключая интернет и выбирая тариф. Так, на сайте «Ростелекома», если мы перейдем к предлагаемым тарифам и нажмем около любого предложения строчку «Подробнее о тарифе», откроется список услуг, который входит в тариф 3.6.

3.6

Отправьте заявку на подключение в г. Москва

Комбо 2в1	Домашний интернет	Комбо 3в1	Комбо 4в1	Видеонаблюдение
2 в 1 Апгрейд 3.0 500 Мбит/с Безлимитный интернет 139 каналов посмотреть Интерактивное ТВ Wink Акция Оборудование > Скоростной интернет и Интерактивное ТВ Wink по выгодной цене 650 руб./мес. Подключить по акции Подробнее о тарифе	2 в 1 Экспресс 200 Оптимальный 2.0 200 Мбит/с Безлимитный интернет 143 канала посмотреть Цифровое ТВ Оборудование Роутер + 30 руб./мес. 719 руб./мес. Подключить Подробнее о тарифе	2 в 1 Экспресс 100 Продвинутой 2.0 100 Мбит/с Безлимитный интернет 164 канала посмотреть Цифровое ТВ Оборудование Роутер + 30 руб./мес. 789 руб./мес. Подключить Подробнее о тарифе		

Здесь есть и дополнительные услуги, которые можно добавить к тарифу, в том числе, подключение антивирусной программы. Можно выбрать приемлемую стоимость и подключить, заполнив ниже заявку 3.7.

3.7

Заявка на подключение

Ваш город **Москва**

Улица

необходимо заполнить

Дом Подъезд Этаж Квартира

Как вас зовут?

Контактный телефон

+7 () - - -

Наши менеджеры свяжутся с Вами в ближайший час

Я принимаю условия обработки данных

Отправить заявку

2 в 1 Апгрейд 3.0

500 Мбит/с
Безлимитный интернет

139 каналов
Интерактивное ТВ Wink

Просмотр на 5 устройствах
ТВ на смартфоне, планшете и ноутбуке

Стоимость тарифа

650 руб./мес.

С рекомендуемыми опциями

740 руб./мес.

Подробнее

подключение бесплатно

Дополнительные опции. Вы можете заказать у оператора. Он быстро добавит их к вашему тарифу.

Все крупные производители антивирусных программ обычно предлагают качественные продукты.

Сравнивайте их по стоимости и по функционалу, можно также установить антивирус сразу на несколько устройств. Как правило, программу скачивают на компьютер и затем оплачивают онлайн ее стоимость.

Скачивайте антивирусные программы с официальных сайтов производителей или включайте данную услугу в тарифах интернет-провайдеров.

Социальная инженерия. Примеры мошеннических схем

Слабое звено любой системы защиты – это люди. Для мошенников иногда бывает проще использовать психологическое воздействие, чем какие-то сложные технологические решения.

Фишинг – один из самых распространенных методов обмана. Главная задача мошенника заставить пользователя перейти на поддельный сайт. Поддельный сайт выглядит также, как настоящий официальный, но вот в адресе может быть изменена всего одна буква. Например, это может быть заново созданная страница оплаты якобы какой-то крупной сети, где вы совершаете покупку.

Переход на такой сайт предполагает оплату покупки. Ввод пароля, логина и затем данных банковской карты для оплаты. Таким образом, деньги получает мошенник и в придачу ваши личные данные, которые вы используете для онлайн оплаты покупок.

В 2021 году аналитики «Доктор Веб» обнаружили множество фишинговых сайтов. В числе прочего злоумышленники подделывали веб-страницы магазинов бытовой техники. Например, мошеннические сайты были замаскированы под официальные ресурсы «М.Видео». После нажатия кнопки «Перейти на сайт» пользователи оказывались в фальшивом интернет-магазине. Здесь они, в надежде получить товар дешевле, активировали некий промокод и совершали покупку, вводя свои банковские данные. Зафиксированы случаи, когда для оплаты товара пользователь перенаправлялся на сайт поддельной платежной банковской системы. Там покупатель вводил данные банковской карты, подтверждал платеж, но товар не получал.

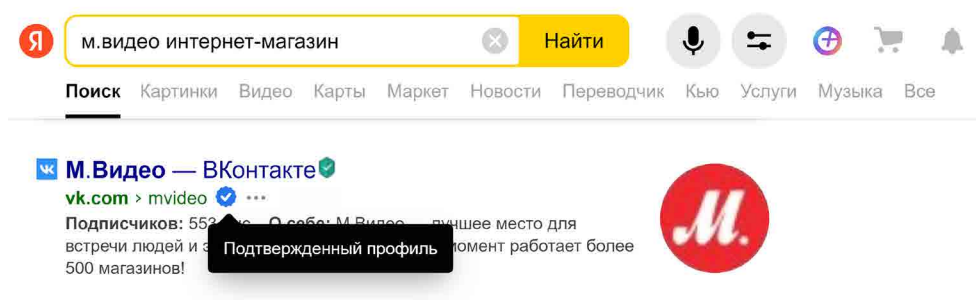
Вишинг – это обман по телефону. Мошенник представляется сотрудником банка, службы охраны или покупателем вашего товара и пытается узнать у вас всю информацию о платежной карте: номер, имя и фамилию владельца, код CVV и код для подтверждения транзакции.

Помните, что для перевода средств на вашу карту не нужно сообщать все ее данные. Деньги могут быть переведены только по номеру телефона или по номеру вашей карты. Если вас просят назвать код CVV с карты или проверочный код совершенной оплаты, это 100% мошенники.

Как пользователи попадают на фишинговые сайты?

При поиске в интернете конкретного товара пользователь может перейти на поддельный сайт. Всегда обращайте внимание на адрес сайта, прежде чем проводить оплату. Вас должны насторожить слишком низкие цены. На карточке настоящей компании должен быть значок (галочка на синем фоне), подтверждающий данные компании 3.8.

3.8



Это могут быть также письма, пришедшие в электронную почту. Среди коммерческих спам-рассылок попадают и письма от мошенников, причем это может быть письмо якобы от известного банка с просьбой подтвердить свои данные или от известного магазина, предлагающего вам как постоянному покупателю получить большой бонус. Всегда смотрите, кто отправитель. Если это известная компания, то, прежде чем переходить по ссылке, зайдите на ее официальный сайт или свяжитесь с их службой поддержки, чтобы уточнить информацию. А подозрительное письмо удалите из своей электронной почты.

Особенно часто ссылки на фальшивые сайты мошенники присылают через сайты объявлений или в социальных сетях и мессенджерах. Например, на Авито покупатель может написать вам, что готов купить товар, но через другую службу доставки. Просит перейти для разговора в другой мессенджер и присылает ссылку на страницу доставки, например, Яндекс.Доставка, но это оказывается поддельная страница, на которой продавцу, чтобы получить деньги, нужно ввести все данные своей карты, в том числе срок ее действия и код ССV. В результате продавец остается без денег. Мошенники могут использовать и вишинг. Свяжутся с продавцом по телефону, представляются покупателем, который хочет немедленно приобрести товар. И также «выуживают» данные платежной карты.

Никогда не переходите для общения из чата Авито в другие мессенджеры. Не переходите по присланным ссылкам. Используйте на сайтах объявлений функцию безопасной сделки.

Схемы обмана постоянно совершенствуются. Приведем несколько примеров того, как работают мошенники.

Безопасность на сайтах объявлений

Некоторые схемы обмана.

Продается техника по низкой цене якобы через менеджера крупного магазина. Если с ним связаться, он присылает ссылку для оплаты. Ссылка ведет на сайт, который очень похож на сайт магазина, но минимальные отличия все же есть, потому что этот сайт создали мошенники. Продавец предлагает внести залог или предоплату в 50%. В результате ни денег, ни товара.

Продавец настаивает на курьерской доставке и предлагает передать оплату курьеру. Перед приездом курьера продавец говорит, что курьеру не доверяет и просит сбросить деньги на карту. Курьер действительно приезжает. Покупатель переводит деньги, но затем оказывается, что продавец, предлагавший вам товар, не имеет никакого отношения ни к курьеру, ни к продаваемому товару. Это мошенник, который просто заказал на ваш адрес доставку нужного вам товара. В результате вы перевели деньги мошеннику, а курьер, так и не получив оплаты, товар вам не отдает.

Приходит СМС от банка, что покупатель перевел сумму за товар 2 или 3 раза. Скажем, вместо 5 тысяч переводит 20 тысяч рублей. Говорит, что это ошибка и просит вернуть деньги. Здесь большая вероятность того, что это поддельное СМС. Нужно посмотреть, с какого номера отправлено сообщение. Иногда используют, например, ненастоящий номер Сбера – девятка и две буквы «0» вместо номера 900 (девять, ноль, ноль).

Мошенники предлагают обмен товара с доплатой, для чего нужно перейти по ссылке в сообщении. Когда продавец переходит по ней, на устройство автоматически скачивается вредоносная программа, которая может зашифровать файлы или перехватить ваши личные данные.

При сделке с техникой Apple покупатель при осмотре меняет Apple ID или ставит блокировку по отпечатку пальца/паролю и затем возвращает товар. А за разблокировку потом просит деньги с продающего товар.

В любом случае будьте внимательны на сайтах купли/продажи:

- старайтесь не переводить предоплату или залог. Если это не сайт крупной торговой сети, то в 99% случаях это мошенники;
- не переходите по ссылкам, присланным в сообщениях от незнакомцев;
- сами выбирайте службу доставки или используйте сервисы безопасной оплаты;
- если вы выступаете продавцом, внимательно проверяйте сообщения об оплате, которые пришли вам от покупателя. Перепроверьте в интернет-банкинге, точно ли ваш счет пополнился на нужную сумму;

Как распознать поддельный сайт?

1. Проверить адрес, сравнить его с официальным адресом магазина.
2. Сравнить цены с другими сайтами, продающими аналогичные товары; если цены значительно ниже, это может быть признаком мошеннической схемы.
3. Связаться с представителями магазина по телефону или через официальные соцсети и проверить информацию, представленную на сайте.

- никому не сообщайте все данные вашей платежной карты. Для перевода денег вам достаточно номера вашего телефона или номера карты;
- скрывайте свой номер телефона в объявлениях.

Безопасность в социальных сетях и электронной почте

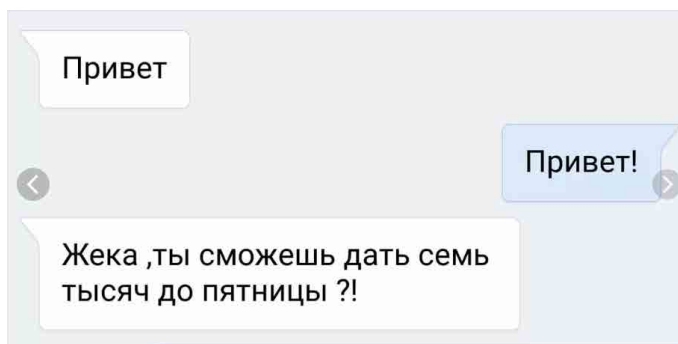
Одна из самых активных площадок для мошеннических схем – социальные сети. Многие аферы мошенников могут быть похожи, но подаются по-разному.

Например, приходит личное сообщение о раздаче бесплатных подарочных карт или о выигрыше как тысячного участника одной из групп. Мошенники предлагают перейти по ссылке. На самом деле она ведет на подставной сайт, где вас попросят ввести личные данные и данные банковской карты для перечисления выигрыша.

Мошенничество через знакомство в интернете: незнакомец входит в доверие, ведет с вами долгую переписку и затем пытается выманить деньги. Это может быть просьба оплатить какой-то подарок или его пересылку, премиум-показ фильма и т.д. В любом случае просьба невидимого собеседника о платежах должна вас насторожить. Никаких платежей делать не нужно. Должно насторожить, что новый знакомый не спешит встречаться, слишком хорошо выглядит на фотографии и тому подобные любые несоответствия в аккаунте. При знакомстве по интернету на той стороне может быть совсем другой человек, не такой, каким он вам стремится представиться.

Внезапно от знакомого вам человека приходит сообщение с просьбой выручить деньгами. Не нужно тут же переводить средства, можно предположить, что, скорее всего, его аккаунт был взломан. Нужно созвониться с ним и выяснить, действительно ли это он писал и просил о помощи. Точно такое же письмо может прийти и на электронную почту. Проще всего защититься от такого способа мошенничества, сделав телефонный звонок [3.9](#).

3.9



В электронную почту или соцсети могут приходиться сообщения, призывающие вас перейти по некой ссылке: «Ты видела эту свою фотку?», «Тут такое про тебя написано». Ссылка ведет на поддельные сайты социальных сетей, где предложат ввести свои логин и пароль от аккаунта. Так мошенники смогут завладеть вашей страничкой.

Точно также работают и другие сообщения с предложением перейти по ссылке и «Узнать свой IQ» или «Увидеть, кто зашел на твою страничку». Это сбор данных, которые можно будет перепродать или использовать против пользователя.

На электронную почту или в смс пришла информация о том, что ваш аккаунт на Фейсбуке или платежная карта заблокирована. И нужно перейти по ссылке, чтобы подтвердить данные. Конечно, ссылка ведет на подставной сайт, а ваши личные данные получают мошенники.

Предлагают редкий товар со 100% предоплатой. Однако по указанному адресу, где можно забрать товар, живут люди, которые вообще не имеют отношения к данному предложению.

На электронную почту или сообщением в социальных сетях приходит информация о выигрыше или наследстве из-за границы. Чтобы получить солидную сумму, нужно сделать перевод или предоставить банковские данные, перейдя по ссылке. Игнорируйте такие сообщения. Это обман.

Какие правила безопасности нужно соблюдать:

- не переходить по подозрительным ссылкам, пришедшим от незнакомых адресатов. Даже если кажется, что информация пришла от известной компании. Если сомневаетесь, сделайте звонок, уточните информацию;
- не доверяйте и не рассказывайте все о себе в переписке с собеседниками, с которыми познакомились в интернете. Вы не можете быть уверены, что это не мошенники;
- не переводите деньги в ответ на просьбы, которые пришли в разного рода сообщениях. Сначала уточняйте ситуацию;
- периодически меняйте пароль в аккаунтах в социальных сетях;
- откорректируйте настройки безопасности. В ВКонтакте перейдите в «Настройки», в раздел «Приватность». Поставьте разрешение на отправку сообщений только своим друзьям. Вы также можете сделать вашу страничку закрытой. Аналогичная функция есть и в других социальных сетях;
- включите двухфакторную аутентификацию для входа на электронную почту. *(Подробнее в главе 5 модуля 10 «Кибербезопасность» расширенного курса «Азбука интернета»).*

Безопасность в финансовых вопросах

Наиболее привлекательными сайтами для мошенников являются банковские и финансовые сервисы. Как правило, банки формируют надежную защиту хранящихся данных. Авантюристам проще ввести в заблуждение клиентов банка, чем взламывать существующие банковские системы защиты.

Мошенник звонит клиенту банка, представившись службой безопасности, и сообщает, что на телефоне, где установлено интернет-приложение

банка, выявлен вирус, и поэтому счет клиента под угрозой. Он предлагает немедленно установить на телефон приложение. Объясняет, как это сделать. Обманщик через установленное приложение получает удаленный доступ к устройству и снимает все деньги со счета клиента банка.

Другой вариант. Злоумышленник представляется клиенту службой безопасности банка и сообщает, что кто-то пытается снять деньги с его банковского счета. На телефон с поддельного номера действительно приходят сообщения с кодами подтверждения для проведения транзакции. Мошенник предлагает перейти к банкомату и срочно снять все деньги. Когда деньги сняты, лжесотрудник банка предлагает положить их на страховочный счет с хорошим бонусом и процентами. Это счет злоумышленника.

Еще вариант: на ваш счет приходит большая сумма денег. Звонит сотрудник банка и сообщает, что на ваше имя взят кредит. Конечно, держатель карты сообщает, что он не брал кредит. Тогда сотрудник банка предлагает срочно вернуть деньги. Для этого нужно ввести комбинацию цифр на номер 900. Деньги уходят на другой счет другого банка, то есть мошеннику. Впоследствии оказывается, что кредит на ваше имя действительно был взят. Если вы попали в такую ситуацию, не выполняйте никаких операций по переводу средств. Звоните или идите в банк и решайте вопрос с сотрудниками организации.

Мошенник звонит держателю банковской карты и, представляясь сотрудником банка, сообщает, что в ваш личный кабинет интернет-банка пытались войти из другого города. Для обеспечения безопасности необходимо подтвердить все данные платежной карты. Человек сообщает все данные, в том числе секретный код подтверждения транзакции. И деньги у мошенника.

Какие правила безопасности нужно соблюдать:

- никому и никогда не сообщайте все платежные данные вашей банковской карты;
- не проводите никаких платежей по просьбе якобы сотрудников банка;
- не общайтесь с мошенниками, кладите трубку и перезванивайте в банк.

Безопасность при интернет-покупках и интернет-заработке

При выборе вариантов заработка или покупки товара в интернете нужно быть очень внимательным.

Часто в интернете предлагают заработать деньги на опросах. Как правило, это небольшие суммы. Если вы встретите подобное предложение с высокой оплатой, стоит обойти его стороной.

Чаще всего в таких случаях после прохождения опроса и сбора ваших личных данных злоумышленники просят заплатить комиссию, прежде чем заплатить вам деньги. Она небольшая по сравнению с суммой вознаграждения, поэтому человек соглашается ее заплатить. Но после оплаты обещанная за прохождение опроса сумма так и не поступит на счет пользователя, а у мошенников будут данные банковской карты, которые были введены при оплате комиссии.

Мошенники создают сайты, где предлагают медицинские услуги, информацию о лекарствах, мерах социального обеспечения. В том числе, на таких ресурсах вам могут предложить заменить полис медицинского страхования за плату или оформление услуги по получению социальных выплат. На самом деле эти услуги вы можете оформить бесплатно или дешевле. А тут просто вымогают деньги.

Нередко обманывают покупателей и интернет-магазины. Они завлекают низкими ценами. При заказе вас могут попросить внести предоплату на какой-либо электронный кошелек или банковскую карту. Затем магазин будет придумывать отговорки, почему товар не доставлен либо пришлет некачественный товар.

На какие меры безопасности необходимо обратить внимание:

- уточните адрес, на который вы сможете направить претензию в случае, если останетесь недовольны покупкой;
- читайте отзывы о сайтах, где вы намерены сделать покупки;
- оплачивайте товары только на проверенных сайтах известных компаний;
- если вы оформляете какие-либо документы, делайте это только на официальных сайтах ведомств или на портале «Госуслуг»;
- не вводите свои данные на сайтах, где вам предлагают получить какие-то компенсации или дополнительные социальные выплаты. Решением этих вопросов занимаются только официальные сайты государственных ведомств;
- осторожно относитесь к предложениям заработать большие суммы в интернете. За ними, скорее всего, кроются мошеннические схемы.

Куда сообщить о мошенниках?

Сообщать о фактах мошенничества нужно обязательно. Можно обратиться в отделение полиции по месту жительства или отправить на сайте МВД электронное обращение.

На Авито можно сообщить о мошенниках-продавцах и покупателях. Для этого нужно перейти в раздел «Помощь». Он находится в верхнем меню сайта. Здесь есть раздел «Безопасность» и пункт «Защита от мошенников». Там можно оставить свое сообщение, если вас обманули. Также внизу есть возможность написать в службу поддержки [3.10](#).

Как обезопасить себя от мошенников?

- Перепроверяйте информацию, прежде чем совершить платеж.
- Не вводите свои данные на подозрительных и незнакомых сайтах.
- Используйте безопасные сервисы оплаты.
- Не переходите по ссылкам, полученным от незнакомцев.
- Устанавливайте настройки безопасности и приватности в социальных сетях.

3.10

The screenshot shows the Avito help page with a search bar and navigation links. The main content is organized into three columns:

- Мои объявления** (My ads):
 - Подать бесплатно
 - Опубликовать
 - Редактировать
 - Удалить и восстановить
 - Как выглядит моё объявление
- Проблемы с объявлением** (Problems with ad):
 - Не удаётся разместить
 - Отклонили
 - Заблокировали
 - Объявления нет в поиске
 - В объявлении не мой телефон
 - Объявления сняты с публикации
- Профиль** (Profile):
 - Настроить
 - Профиль заблокирован
 - Добавить или сменить телефон
 - Добавить или сменить почту
 - Удалить профиль

Below these are three more categories:

- Войти на Авито** (Log in):
 - Не получается войти
 - Не подходит логин или пароль
 - Зарегистрироваться
 - Способы входа
- Безопасность** (Security):
 - Защита от мошенников
 - Скрыть номер
 - Защитить профиль
 - Приходит спам
 - Защитить бренд
 - Во время пандемии
- Доставка** (Delivery):
 - Продавец
 - Покупатель

В социальных сетях также всегда можно пожаловаться в техподдержку на действия пользователей. Так, в ВКонтакте нажмите на значок профиля и выберите раздел «Помощь» 3.11.

3.11

The screenshot shows a VK profile page for Ivan Romanov. The profile information includes:

- Иван Романов** (Ivan Romanov)
- установить статус
- День рождения: 3 февраля 1946 г.
- Город: Волгоград
- Образование: ВГАФК
- Показать подробную информацию

Below the profile information, there is a section for photos with 1 photo. On the right side, a dropdown menu is open, showing the following options:

- Иван Романов
- Перейти в VK Connect
- Настройки
- Помощь** (Help)
- Выйти

Затем перейдите в раздел «Безопасность и доступ к аккаунту» либо выберите пункт «Задать вопрос» и опишите вашу ситуацию.

Если у мошенников есть сайт, то можно сообщить о нем Яндексу и Гуглу. В Яндексе для этого нужно перейти в раздел «Службы поддержки» и по данной ссылке разместить информацию о сайте злоумышленников: <https://yandex.ru/support/search/troubleshooting/delspam.html>

Можно ли вернуть украденные деньги? По закону «О национальной платежной системе» банк должен вернуть деньги, если клиент сообщил

об интернет-мошенниках в течение суток. После обращения банк заблокирует счет и начнет проводить проверку. По закону на расследование у него есть 30 дней.

Однако нужно принять во внимание, что если проблема на стороне банка, то есть был взлом системы, то деньги вернут. А вот если вы сами сообщили мошенникам данные или сами перевели им деньги, будет гораздо сложнее их вернуть.

Риски публичных Wi-Fi сетей

К работе в публичных Wi-Fi сетях также стоит относиться осторожно. Дело в том, что именно в таких сетях злоумышленники могут увидеть ваши пароли, данные вашей платежной карты и т.п. И тем более не стоит пользоваться незапароленными сетями. Хакеры в этом случае часто создают поддельную точку доступа. И, соответственно, могут видеть все данные тех, кто к ней подключился. Но и закрытые сети могут быть поддельными, ведь мошенникам несложно узнать пароль от Wi-Fi в кафе или отеле и также создать фальшивую одноименную сеть с таким же паролем 3.12.



3.12

Не проводите платежи, не заходите на личные страницы в социальных сетях в зоне Wi-Fi с публичным доступом.. Старайтесь выключать Wi-Fi, если не пользуетесь им. Отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.

Дело в том, что у сетей Wi-Fi есть возможность следить за вами. Когда вы заходите в торговый центр, телефон автоматически начинает искать точку Wi-Fi. При этом он транслирует свой собственный уникальный адрес. Эти данные заносятся в журнал приемника, и по ним маркетолог может следить, как клиент перемещается по отделам, и показывать вам соответствующую вашим интересам рекламу.

Альтернативой может стать подключение по виртуальной сети VPN. Можно поискать подобные приложения и даже найти бесплатные варианты у ProVPN, Cyber Ghost, Your Freedom или HotSpot Shield. Они, возможно, будут работать чуть медленнее, зато безопаснее.

Внешние носители

30% вредоносных программ распространяется через съемные накопители: карты памяти и USB-флешки. В 2012 году были обнаружены компьютерные вирусы на двух американских электростанциях, которые были отключены от сети интернет. Причиной стали флешки, которые принес из дома один из рабочих и подключил к рабочим компьютерам.

Съемные накопители отлично переносят из компьютера в компьютер нежелательные программы. Когда флешка вставляется в зараженный компьютер, активный вирус может просто записать себя на нее [3.13](#).

3.13



Более того, известны случаи, когда инфицированные флешки намеренно оставляли в тех или иных организациях в людных местах с какой-нибудь привлекающей внимание подписью: «Зарплата сотрудников», «Планы по ротации персонала» и т.д. И всегда находились те, кто не мог сдержать любопытство и подключал флешку к рабочему компьютеру, провоцируя таким образом хакерскую атаку на всю корпоративную систему.

Поэтому старайтесь перед тем, как начать работать, проверять USB-накопители антивирусной программой. Разделяйте флешки на те, что хранят ваши архивы, и те, которые можно использовать для переноса информации из других источников.

Также имейте в виду, что зарядка телефонов через USB в общественных местах может быть чревата последствиями. USB-разъем также может передавать информацию о вашем телефоне и приложениях на нем. Поэтому, если есть необходимость зарядить мобильное устройство в общественном месте через USB-разъем, не работайте на нем, пока идет зарядка.



Какую информацию нельзя доверять интернету

Поскольку из сети невозможно полностью удалить все следы своего присутствия, нужно внимательно относиться к тому, что вы делаете в интернете.

Не стоит размещать в публичном доступе свои личные данные, в том числе сканы паспортов или других документов.

Сообщая данные своего паспорта, обращайте внимание, что за ресурс их запрашивает. Если это действительно необходимо, то не присылайте скан паспорта, а просто перепишите данные в текстовом виде.

Если все же нужно выслать скан паспорта, прикройте при сканировании вашу подпись. Так будет сложнее воспользоваться вашими паспортными данными.

Не делитесь публично своими финансовыми планами, информацией о ваших платежных картах. Никому не высылайте фотографии банковской карты. Они не нужны для проведения финансовых операций. Достаточно сообщить номер карты или номер телефона, к которому карта привязана.

Не размещайте на страничках в социальных сетях номер своего мобильного телефона и адрес электронной почты.

Проверяйте сайты, на которых вы проводите оплату. Если что-то вас насторожило, лучше откажитесь от оплаты и найдите другой способ покупки товара или услуги.

Контрольные вопросы

1. Как работают вредоносные программы?
2. Откуда может появиться вредоносная программа на устройстве?
3. Что такое социальная инженерия?
4. Какие варианты и схемы мошенничества вам известны?
5. Какие действия нужно предпринять, если вам звонит сотрудник банка и просит сообщить данные банковской карты?
6. Каким сообщениям не стоит доверять в социальных сетях?
7. Почему стоит осторожно относиться к съемным USB-носителям?



Настройка безопасности компьютера

4 ГЛАВА

Зачем нужен Firewall (Файервол)/ Брандмауэр

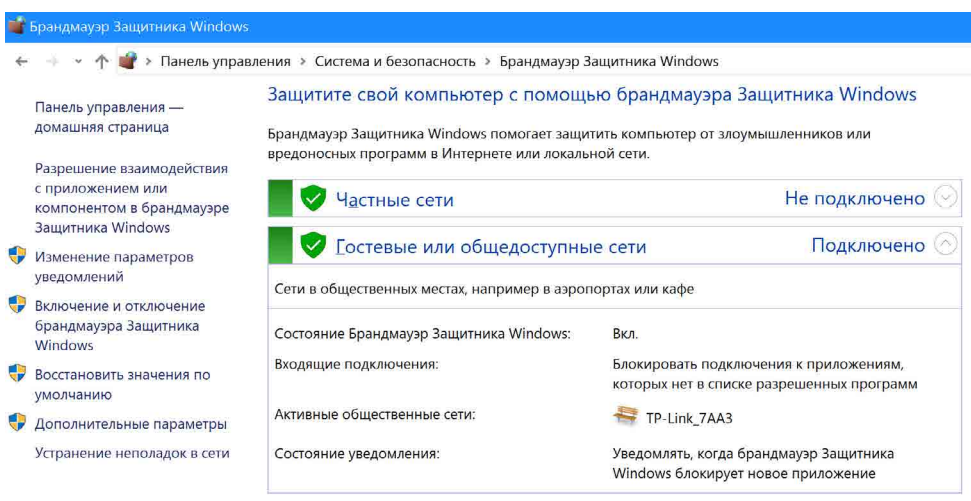
Кроме антивирусных программ, которые пользователь сам устанавливает на устройство, есть программы, защищающие всю систему в целом. Это брандмауэр или файервол. По сути, это некий экран или стена, которая фильтрует всю поступающую на компьютер и исходящую информацию на предмет угроз и вредоносных программ.



Брандмауэр отличается от антивируса тем, что он оповещает пользователя о большинстве вредоносных программ извне (из интернета). Если вирус все же уже попал в компьютер, брандмауэр его не увидит, а антивирус увидит его.

В операционной системе Windows встроенный брандмауэр. Его настройки можно увидеть, перейдя в «Панель управления» (в Windows 10 раздел «Параметры»). Открыв «Пуск» на компьютере, в строке поиска введите запрос «Брандмауэр Защитника Windows». Откроется окно, где можно увидеть настройки брандмауэра 4.1.

4.1



Переключаясь по пунктам меню слева, можно корректировать работу программы. Но, как видите, ряд настроек можно регулировать только с правами администратора.

Это серьезные настройки безопасности компьютера, и экспериментировать с ними не стоит. По умолчанию брандмауэр должен быть у вас обязательно включен.

Если на компьютере установлен антивирус, то часто он имеет встроенный брандмауэр и управляет настройками компьютера в этой части.

Безопасная настройка браузера

Главная программа, через которую проходит весь ваш интернет-трафик (вся информация о действиях в сети), – это браузер. Именно он знает о вашем местоположении, в нем сохраняются файлы-куки, кэш и история посещенных вами страниц, введенные вами пароли, логины и все данные при заполнении форм.

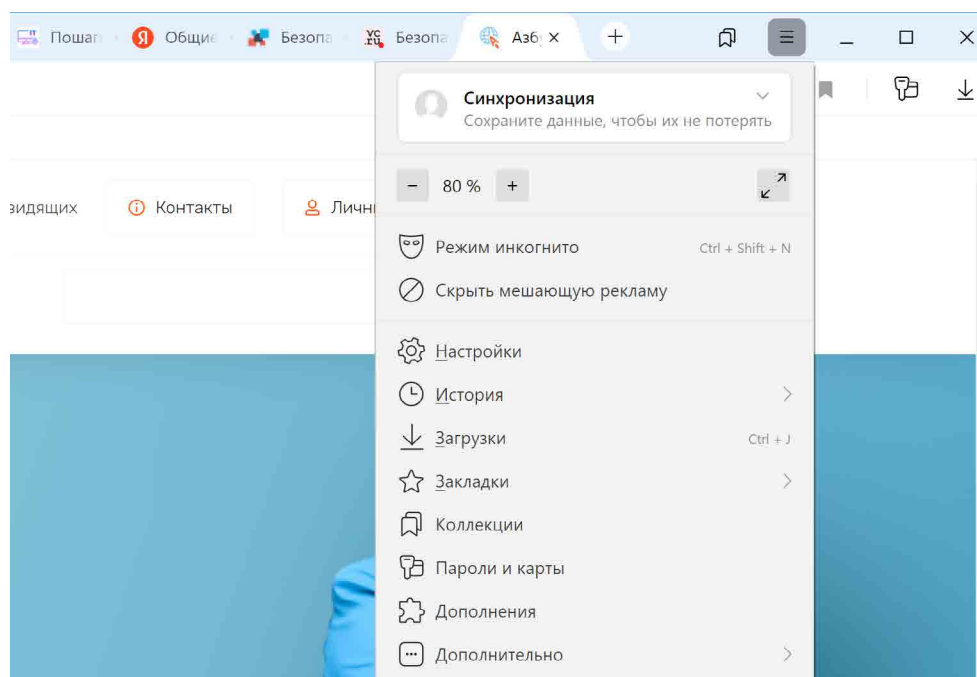
Поэтому настройки браузера важны для сохранения конфиденциальности и безопасного поиска.

Они немного отличаются у разных программ, предоставляющих возможность входа в интернет. Но функционал, как правило, одинаковый.

Рассмотрим настройку Яндекс.Браузера.

Чтобы перейти к функционалу безопасности, вверху справа зайдите в меню настроек. Это три горизонтальные черты. Здесь есть целый ряд полезных для безопасности разделов [4.2](#).

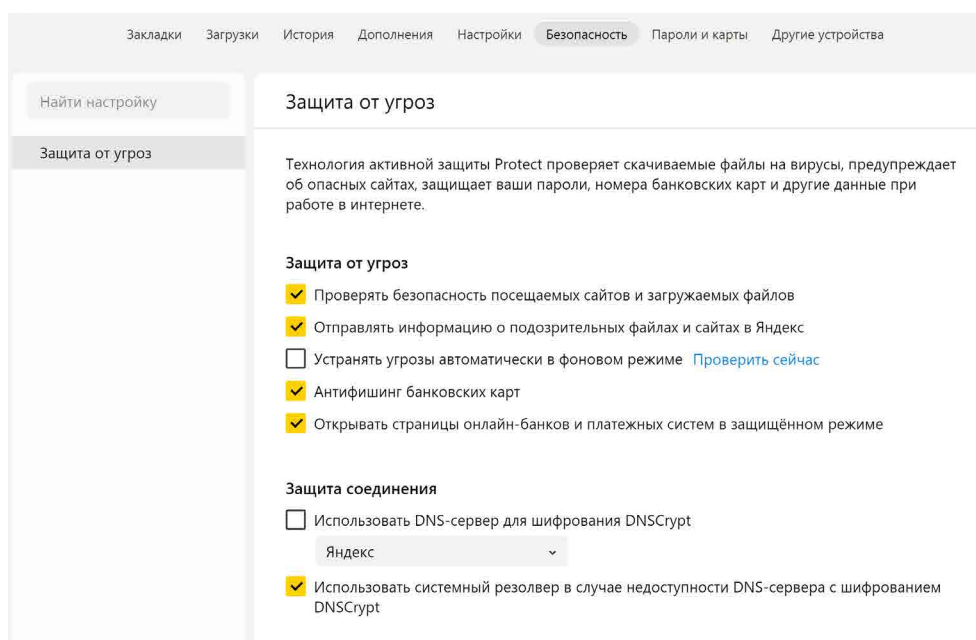
4.2



Можно перейти в режим «Инкогнито». Это режим анонимности. В этом случае браузер не запоминает историю ваших поисков, не хранит историю ваших загрузок и не собирает файлы-куки, но так или иначе у браузера есть информация о вашем местоположении, но это не защитит вас от вредоносных программ. Рекомендуется в режиме инкогнито работать на чужих компьютерах.

Здесь же есть раздел «История», где вы можете посмотреть список ранее посещенных интернет-ресурсов.

Чтобы посмотреть, какие функции защиты в браузере включены, нужно перейти в раздел «Настройки» и выбрать сверху «Безопасность». В браузер встроена система защиты Protect. Здесь необходимо активировать настройки, которые будут проверять безопасность сайтов и файлов, защищать от перехода на поддельные сайты и открывать страницы оплаты в защищенном режиме. Браузер может проверить компьютер на наличие угроз. Для этого нужно нажать «Проверить сейчас» 4.3.



4.3

Чтобы запретить сайтам присылать вам запросы на отправку уведомлений:

1. Перейдите в меню браузера, нажав три полоски сверху справа.
2. Выберите пункт «Настройки».
3. Далее сверху также нажмите на вкладку «Настройки».
4. Слева выберите «Сайты».
5. Активируйте пункт «Не показывать запросы на отправку».

Далее сверху выберите раздел «Настройки». Переходя по разделам слева, можно настроить вид, панель инструментов, а также включить некоторые настройки безопасности.

Настройки=Инструменты

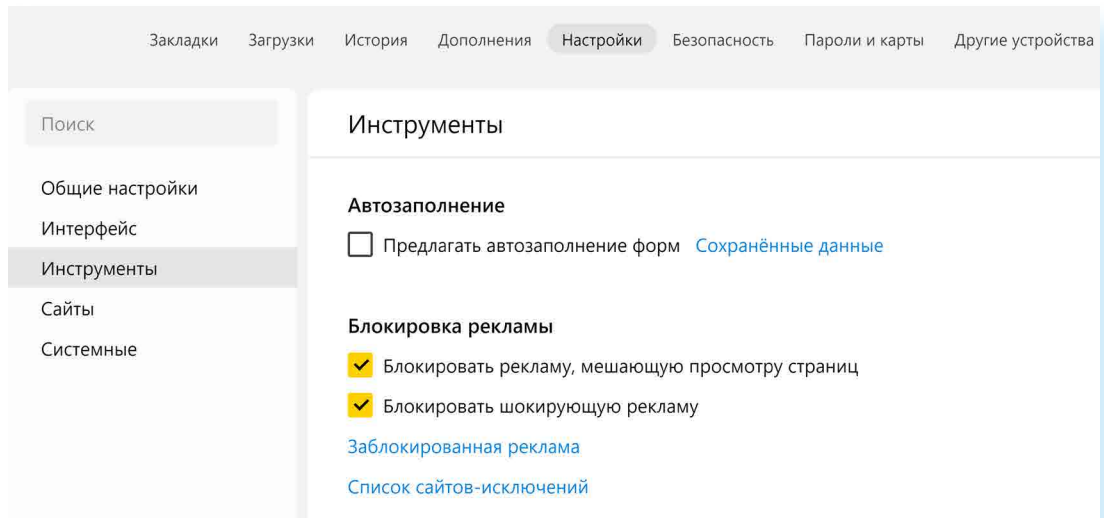
Чтобы перейти в раздел «Инструменты», нужно:

- открыть меню браузера;
- перейти в раздел «Настройки»;
- выбрать сверху вкладку «Настройки»;
- слева кликнуть на строчку «Инструменты».

Здесь поставьте галочки напротив опций, позволяющих блокировать неприятную рекламу и рекламу, мешающую просмотру страниц.

Также обратите внимание на пункт «Автозаполнение». Лучше отключить данную опцию, чтобы ваши личные данные случайно не отображались в формах на ненадежных, подозрительных сайтах 4.4.

4.4



Настройки=Сайты

Чтобы перейти в раздел «Сайты», нужно:

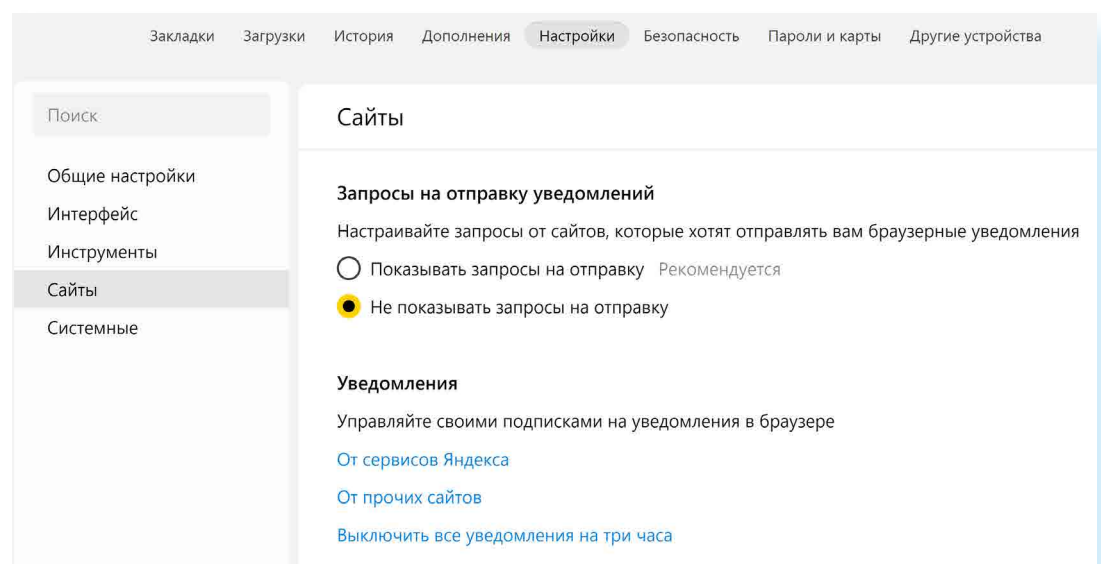
- открыть меню браузера;
- перейти в раздел «Настройки»;
- выбрать сверху вкладку «Настройки»;
- слева кликнуть на строчку «Сайты».

Здесь много полезных настроек. Например, можно установить размер шрифта на сайтах. И здесь же настроить показ уведомлений от сайтов.

В разделе «Запросы на отправку уведомлений» установите отметку напротив пункта «Не показывать запросы на отправку».

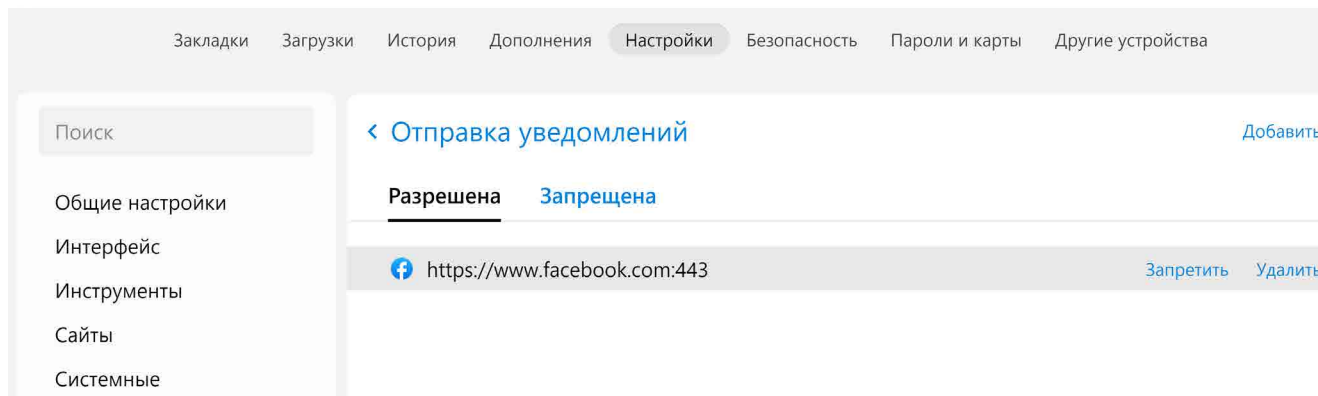
Если вы случайно подписались на какие-то уведомления от сайтов, тут их можно отключить. В блоке «Уведомления» нажмите строчку «От прочих сайтов» 4.5.

4.5



Во вкладке «Разрешена» можно посмотреть список сайтов, которым разрешена отправка уведомлений. Выделив ссылку на сайт, можно включить запрет 4.6.

4.6



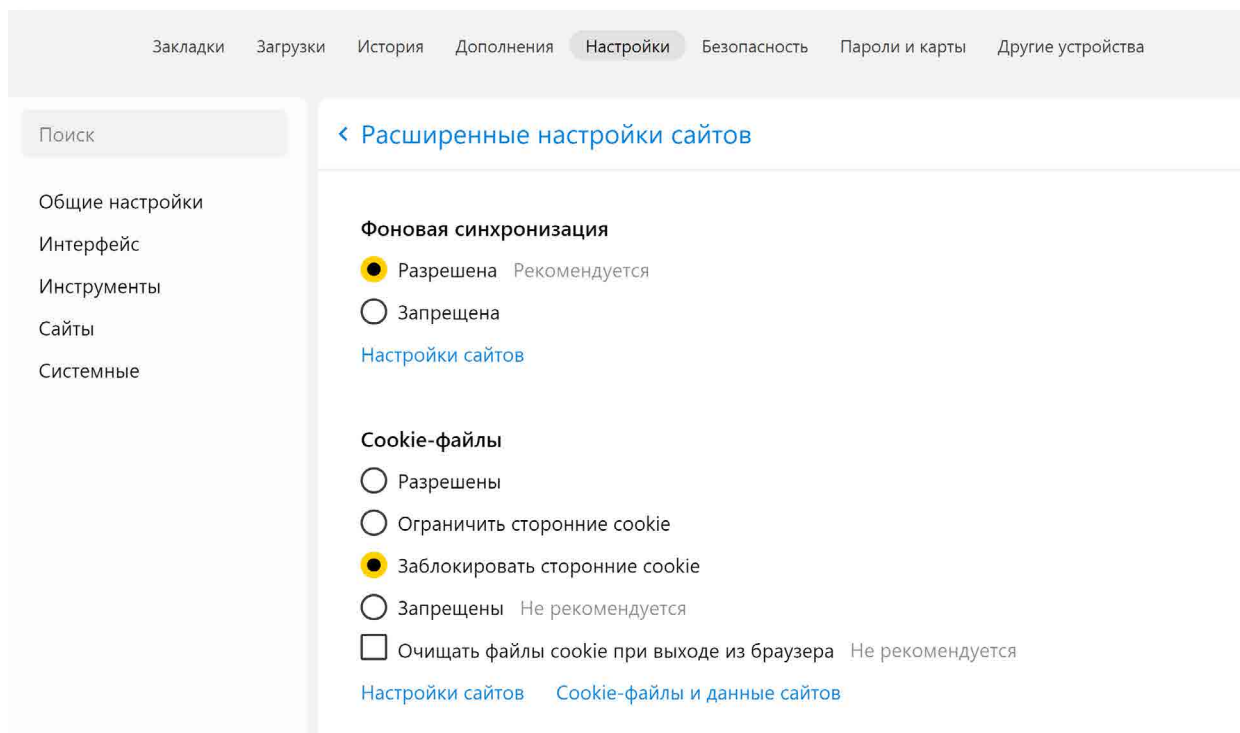
В разделе «Сайты» есть возможности для расширенной настройки сайтов. Такая строчка-ссылка есть внизу блока. Можно поставить запрет на всплывающие окна, обязательство запрашивать разрешение на доступ к камере, микрофону, запретить автоматическую загрузку файлов.

Чтобы заблокировать сторонние куки-файлы, нужно:

1. Перейти в меню браузера.
2. Выбрать пункт «Настройки».
3. Затем вверху выбрать вкладку «Настройки».
4. Слева нажать раздел «Сайт».
5. Выбрать блок «Cookie-файлы».
6. Активировать команду «Заблокировать сторонние cookie».

Здесь же есть настройки по управлению куки-файлами. Можно установить запрет на сохранение куки-файлов либо дать команду очищать куки при выходе из браузера. Но надо помнить, что при этом будут стираться все данные в заполненных формах, введенные вами логины и пароли. Это значит, что для того, чтобы зайти в электронную почту или личный кабинет на каком-то сайте, нужно будет снова вводить ваши данные. Поэтому решать вам. Однозначно стоит активировать блокировку сторонних куки-файлов, потому что это запись ваших действий, которая отправляется сторонним ресурсам для анализа ваших интересов в сети 4.7.

4.7



Настройки=Системные

Чтобы перейти в раздел «Системные», нужно:

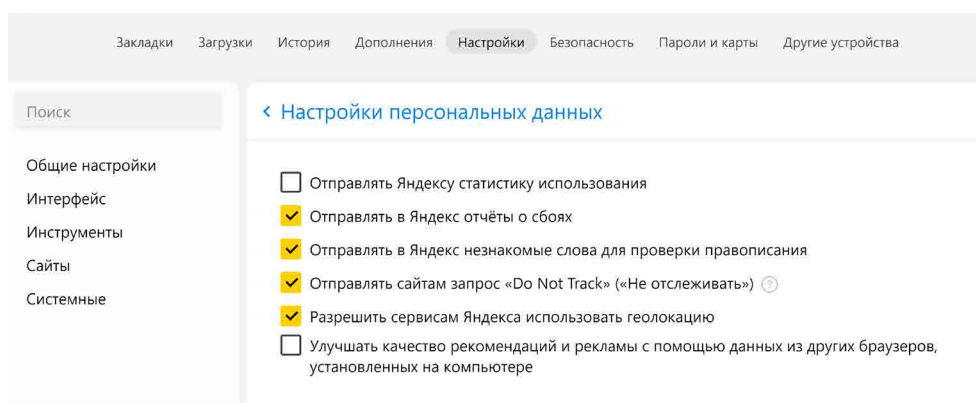
- открыть меню браузера;
- перейти в раздел «Настройки»;
- выбрать вверху вкладку «Настройки»;
- слева кликнуть на строчку «Системные».

В центре страницы расположен ряд важных настроек.

В разделе «Сеть» поставьте галочку напротив команды «Автоматически открывать сайт по протоколу HTTPS». Это защищенное соединение с сайтами.

Внизу нужно нажать на строчку «Настройка персональных данных». Здесь можно отключить отправку статистики о вашем пребывании в интернете, активировать отправку сайтам запроса «Не отслеживать» 4.8.

4.8



Нужно учитывать, что запрос «Не отслеживать» понимают не все сайты. Многие из них все равно будут собирать и использовать данные о вашей работе в интернете. Также мы оставили галочку напротив пункта Геолокации. Определение местоположения пользователя позволяет быстрее находить в интернете нужные адреса, товары и услуги. Но вы можете ее также отключить.

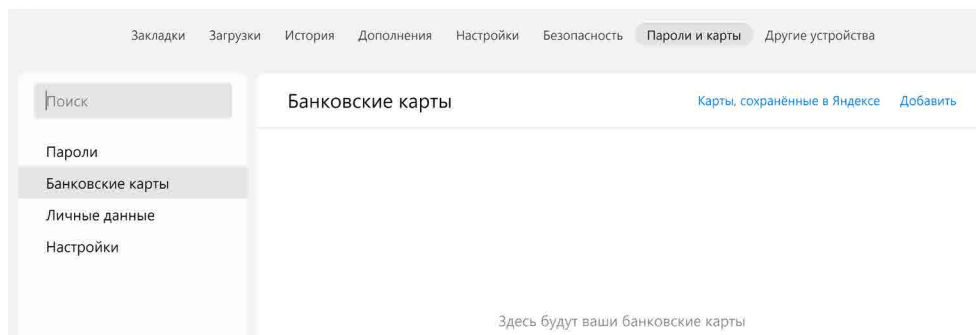
Пароли и карты

Чтобы перейти в раздел «Пароли и карты», нужно:

- открыть меню браузера;
- перейти в раздел «Настройки»;
- выбрать вкладку «Пароли и карты».

Настройками можно управлять с помощью меню слева. Здесь вы найдете личную информацию, которая сохранена в вашем браузере по итогам посещения сайтов. Если слева выбрать «Пароли», откроется список сайтов и логинов, которые сохранены у вас в браузере. Пароли вы не увидите. Она зашифрованы. Браузер будет их просто подставлять при вводе логина в форму авторизации.

В разделе «Банковские карты» вы увидите данные карт, которые вы сохранили в браузере. Для неопытных пользователей рекомендуется все данные карт удалить и никогда не сохранять их после ввода на сайтах 4.9.

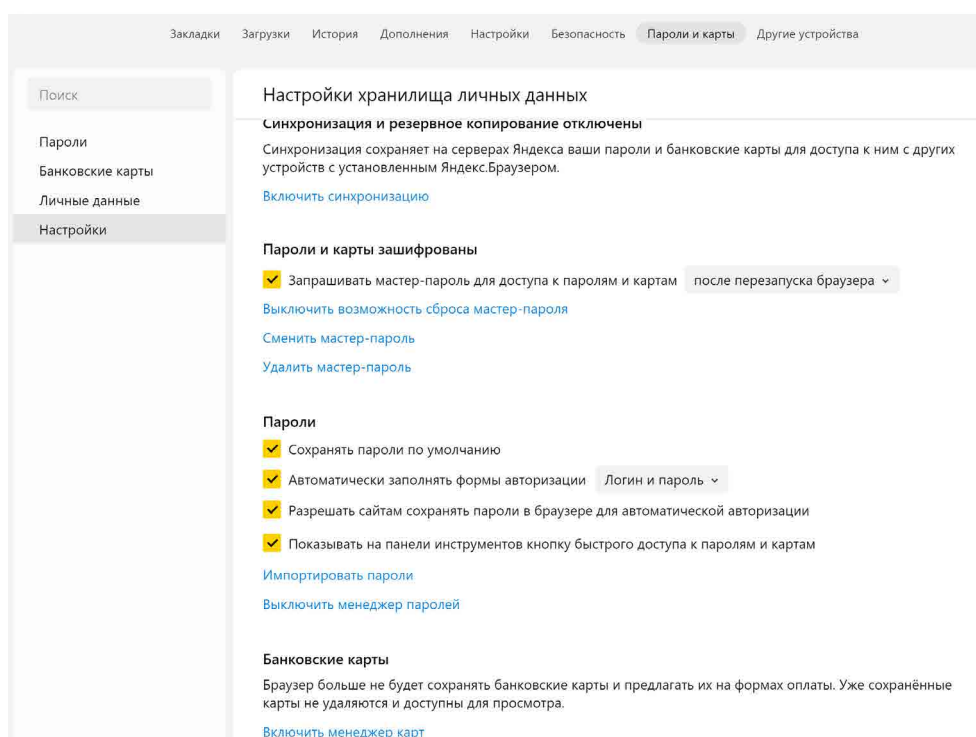


4.9

В разделе «Личные данные» можно увидеть ваши имя и фамилию, адрес электронной почты, которые вы обычно вводите на формах для регистрации на сайтах. Их также можно удалить.

В разделе «Настройки» можно отредактировать варианты хранения личных данных в браузере. Рекомендуется выключить синхронизацию, чтобы ограничить доступ к вашим данным на разных устройствах, а также выключить менеджер банковских карт и менеджер паролей.

Надо признать, что сохранение паролей – удобный функционал, если вы часто заходите в электронную почту, в социальные сети. Выключив менеджер сбора паролей, вы будете каждый раз при входе в личные кабинеты на сайтах вводить логин и пароль заново. Поэтому, если вы не отключили менеджер паролей, рекомендуется зашифровать доступ к ним. Для этого вам предложат придумать мастер-пароль. И при каждом входе в систему авторизации на сайтах вам нужно будет всегда вводить данный мастер-пароль, чтобы браузер мог подставить в форму ваши сохраненные данные 4.10.



4.10

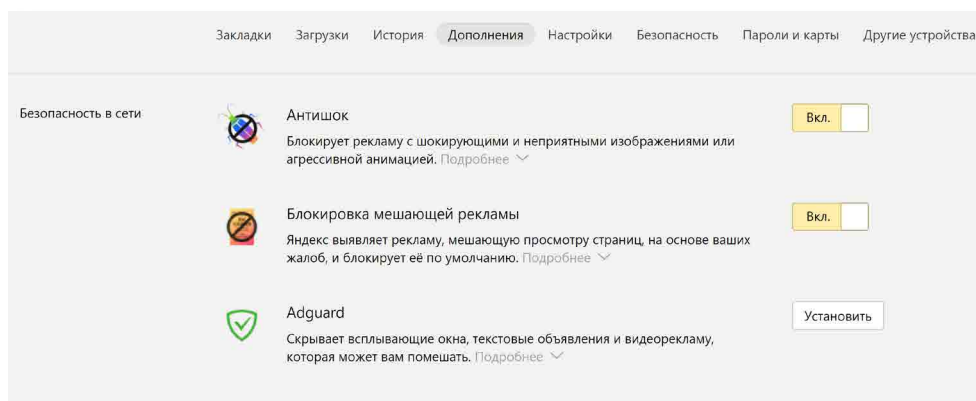
Дополнения

Важными для безопасности будут настройки в разделе «Дополнения». Перейти к ним можно из основного меню Яндекс. В списке разделов будет пункт «Дополнения».

Это небольшие приложения, которые включают в браузер дополнительные функции. Их еще называют «Расширения». Некоторые из них уже предустановлены в браузере. Другие можно скачать. Все расширения разделены по тематике. Один из блоков касается вопросов безопасности в сети.

В нашем примере установлены дополнительно два расширения, блокирующие некоторые рекламные объявления в интернете. Также можно установить еще одно, которое помогает скрыть всплывающие окна, видеорекламу и т.д. 4.11.

4.11



Можно добавить больше расширений. Для того, чтобы выбрать подходящие, нужно будет прокрутить страницу вниз и нажать ссылку «Каталог расширений Яндекс.Браузер». В настройках вы в любой момент можете отключить или включить нужные дополнения к основному функционалу браузера.

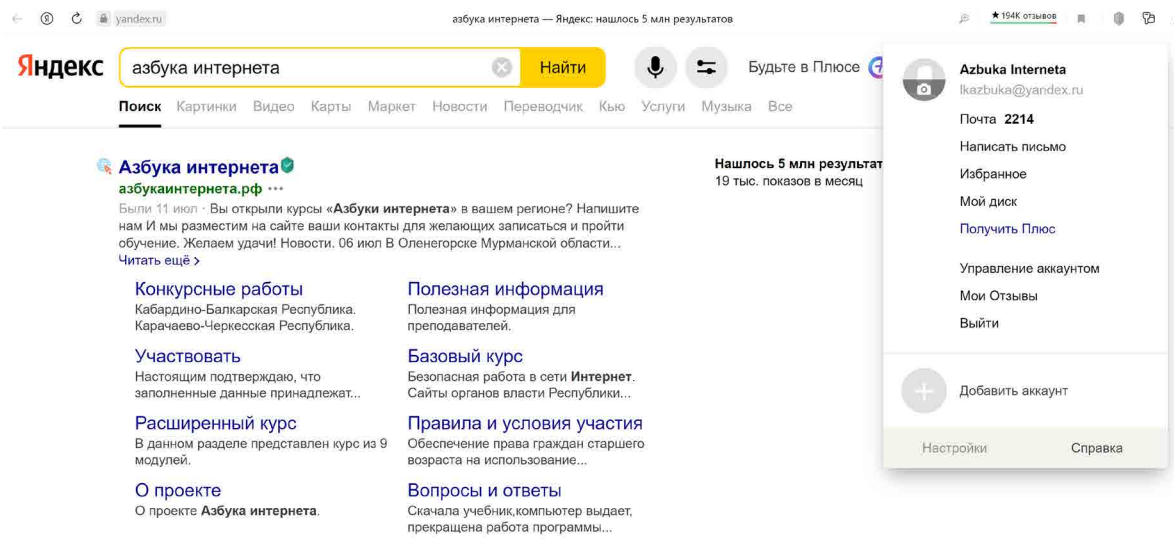
Настройки личного аккаунта в браузере

Практически каждый браузер имеет дополнительные сервисы: страницу поиска, карты, переводчик, электронную почту и т.д. Чтобы получить доступ ко всем этим возможностям, пользователю предлагают зарегистрироваться.

Например, у многих есть почта на Яндексе. Автоматически логин и пароль от электронной почты будет и логином и паролем от вашего аккаунта на Яндекс.Браузере. Безопасность аккаунтов можно и нужно настраивать.

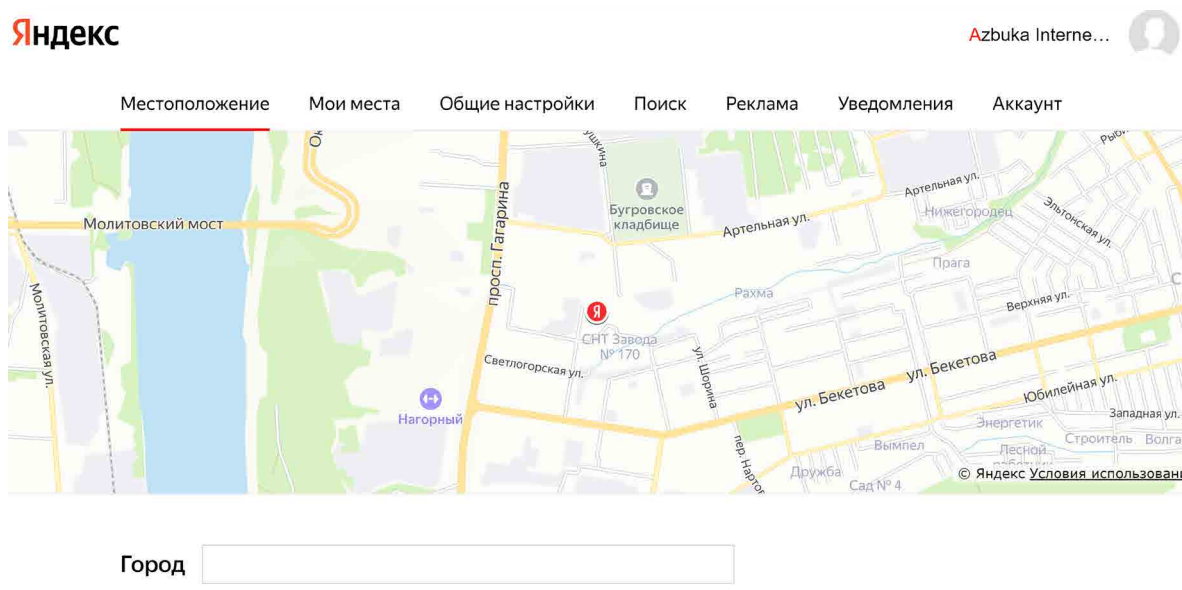
Чтобы перейти в аккаунт Яндекс, на странице браузера вверху справа зайдите в свой профиль. Достаточно ввести логин и пароль от своей электронной почты в Яндекс.

Значок вашего аккаунта отобразится вверху справа. Нажмите на него. В открывшемся меню выберите «Настройки» 4.12.



4.12

На следующей странице вы увидите возможные индивидуальные настройки браузера для вашего аккаунта. Для перехода между разделами воспользуйтесь верхними вкладками 4.13.



4.13

В разделе «Местоположение» можно убрать галочку около строчки «Определять город автоматически». В этом случае Яндекс не будет показывать вам актуальную погоду и новости именно для вашего региона. И в большинстве сервисов ваше местоположение также нужно будет указывать вручную.

В разделе «Мои места» вы сможете строить на карте маршруты, но сохранять их у себя в аккаунте не рекомендуется.

Достаточно интересный раздел «Поиск». Внизу можно выбрать фильтрацию поиска. Если указать «Семейный поиск», в результатах не будет нежелательного контента.

В разделе «Реклама» можно убрать галочки с разделов, разрешающих ее показ 4.14.

4.14

Яндекс

Azбука Interne... 

Местоположение Мои места Общие настройки Поиск **Реклама** Уведомления Аккаунт

Настройка рекламы

Главная страница и новая вкладка Яндекс. Браузера

Показывать рекламу

Мы стараемся размещать рекламу, которая может быть вам полезна. Если по какой-то причине вы не хотите видеть рекламу на главной странице Яндекса и в новой вкладке Яндекс. Браузера, её показ можно отключить.

Яндекс.Директ

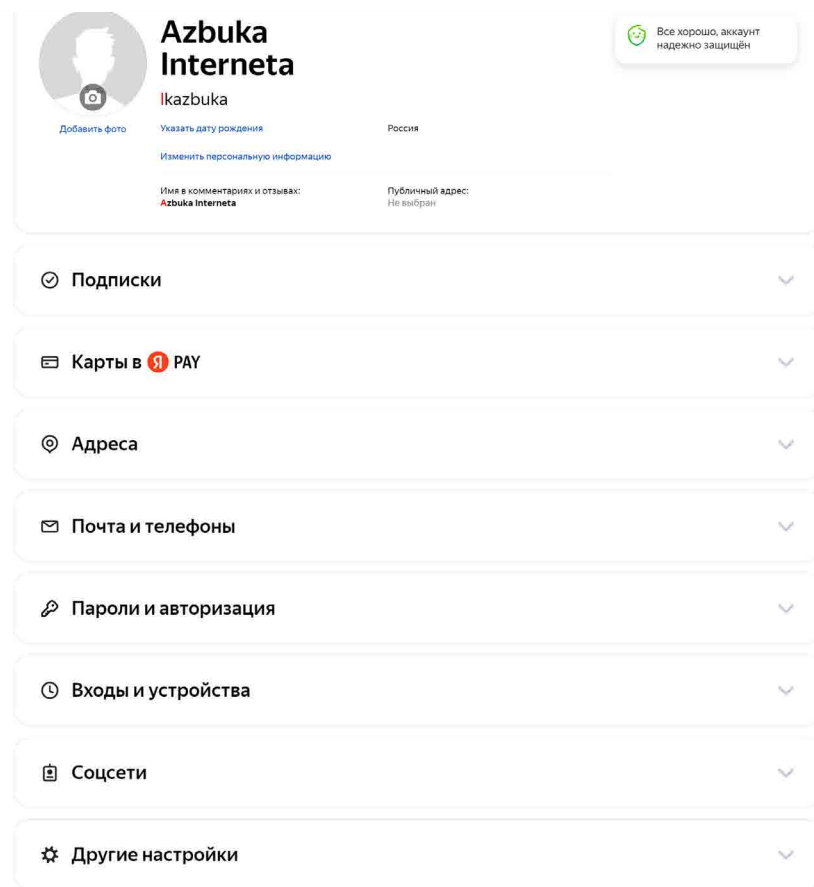
Учитывать мои интересы

При показе рекламы Яндекс учитывает индивидуальные интересы пользователей, которые определяются по их поведению на Яндексе и на ресурсах-участниках Рекламной сети Яндекса. Это позволяет избавить вас от просмотра ненужных и неинтересных рекламных предложений. При этом на сайтах общей направленности не показывается реклама деликатных тематик; Яндекс никогда не применяет учёт интересов пользователей для рекламы, если она затрагивает заведомо личную (не публичную) информацию пользователя, его личные трудности и переживания, самовосприятие пользователя как члена социальной группы.

Также стоит снять галочки с тем уведомлений (вкладка «Уведомления»), разрешенных вами для показа.

В разделе «Аккаунт» есть полезные сервисы. Их можно найти внизу страницы. Чтобы открыть тот или иной раздел, напротив его названия нужно кликнуть на изображение стрелки 4.15

4.15



Azбука Interneta
kazбука
Россия

Добавить фото Указать дату рождения Изменить персональную информацию

Имя в комментариях и отзывах: **Azбука Interneta** Публичный адрес: Не выбран

Все хорошо, аккаунт надежно защищён

- Подписки
- Карты в PAY
- Адреса
- Почта и телефоны
- Пароли и авторизация
- Входы и устройства
- Соцсети
- Другие настройки

Например, в разделе «Пароли и авторизация» стоит настроить двухфакторную аутентификацию. Что это значит? Это значит, что каждый вход с незнакомого устройства на вашу почту будет возможен только после ввода кода, который придет вам в смс на номер мобильного телефона. Для этого нужно будет указать в данных почты свой номер.


В блоке «Входы и устройства» можно посмотреть историю входов в вашу почту. Всегда можно проверить, заходил ли в вашу почту кто-то с незнакомого компьютера или телефона.

Внизу страницы в разделе «Другие настройки» можно запретить рекламные рассылки от Яндекса. Для этого нужно перейти по ссылке «Управление промо-рассылками». А можно скачать и удалить всю информацию о вас, собранную Яндексом.

Нажмите «Управление данными», подтвердите свои действия, введя в указанное поле код, пришедший в смс.

На этой странице вы можете посмотреть, какие данные о вас хранит Яндекс, а также удалить данные, которые собрали приложения Яндекса. Для этого ниже выберите приложение. Чтобы удалить информацию, нужно нажать значок «корзины» около информации о данных 4.16.

Ваши данные на Яндексе



Яндекс обращается с вашими данными очень бережно и тщательно их защищает.

На этой странице вы можете посмотреть, какие данные сейчас хранит Яндекс, и распорядиться ими по своему усмотрению.

↓ Скачать данные

- 📁 Какие данные будут в архиве
- 📄 Как скачать данные Почты, Диска и Календаря

Удаление данных

Здесь вы можете посмотреть, какие данные хранятся на разных сервисах Яндекса, и удалить любые из них.

⚠ После удаления данные сразу станут недоступны. Некоторые виды данных Яндекс будет хранить ещё какое-то время, потому что этого требует закон.

[Узнать подробности](#)

- Алиса**
История общения
- Я
Бизнес
Данные клиентской базы малого и среднего бизнесов
- Запись о вашем профиле, информация о бронировании столов и заказов**

4.16

Как перейти к настройкам аккаунта в Яндекс.Браузере:

1. Зайти в аккаунт.
2. Вверху справа нажать на значок аккаунта.
3. Выбрать в открывшемся списке «Настройки».

Нужно ли очищать кэш и куки

Эксперты по безопасности рекомендуют периодически очищать кэш и куки. Кэш – это фактически копии посещенных вами страниц в интернете. Они хранятся, чтобы в следующий раз вы смогли быстро попасть на ранее посещенный вами сайт. Кэш во многом засоряет оперативную память компьютера. Стоит удалять и файлы куки, и периодически очищать историю просмотров. Это очень помогает в том случае, когда компьютер начинает «тормозить».

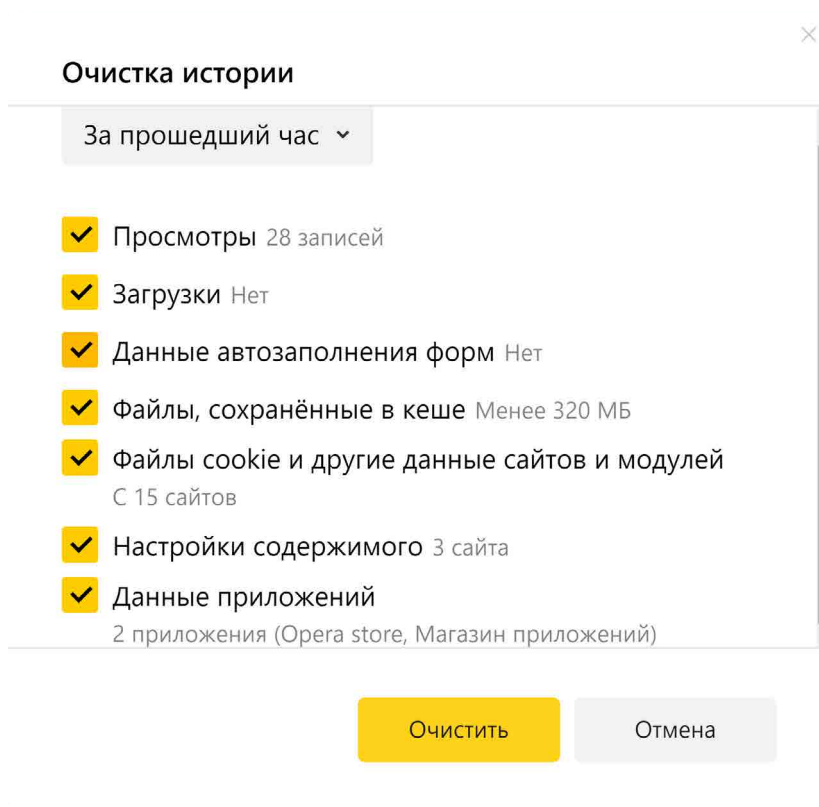
Чтобы очистить компьютер от собранных данных во время вашей навигации в интернете:

1. Зайдите в настройки браузера. В Яндексe три горизонтальные черты вверху справа.
2. Наведите курсор на строчку «История». В открывшемся окне кликните по надписи «История».
3. Далее найдите внизу строчку «Очистить историю».
4. В открывшемся окне поставьте галочки напротив всех строчек. (Имейте в виду, что в этом случае также будут удалены все данные паролей и логинов для входа на сайты. Определитесь, ставить или не ставить галочки напротив соответствующих строчек).
5. Вверху выберите, за какой срок удалить данные. Вы можете выбрать: «За прошедший час», или «За последний месяц», или «За все время» 4.17.

4.17

Как очистить историю просмотров в браузере:

1. Зайдите в настройки браузера.
2. Выберите пункт «История».
3. Далее нажмите «Очистить историю».
4. Укажите период.
5. Выберите, что конкретно вы хотите удалить.
6. Нажмите «Очистить».



6. Нажмите «Очистить».

Блокировщики рекламы

Рекомендуется также использовать блокировщик рекламы. Как правило, такие программы устанавливаются как дополнение к браузеру (расширение), бывают встроены в антивирусные программы. Встроенный в браузер блокировщик вряд ли защитит от отслеживания, зато не позволит показывать навязчивую рекламу, которую могут использовать и мошенники.

В Kaspersky Internet Security уже есть функция «Антибанер».

Расширение-блокировщик также уже встроено в Яндекс.Браузер. Мы его настраивали в разделе «Настройки/Инструменты».

Найти его можно:

1. В настройках Яндекса.
2. В разделе «Дополнения».

В блоке «Безопасность» должно быть данное расширение. Если его нужно активировать, нажмите «Установить». Если его нет, листайте вниз страницы и нажмите кнопку «Каталог расширений для Яндекс.Браузера».

На следующей странице в строке поиска введите запрос «блокировщик рекламы». Появятся предложения расширений. Чтобы выбрать подходящий, смотрите описание, рейтинг, отзывы, условия установки [4.18](#).

4.18

Совместимо с Яндекс.Браузером

блокировщик рекламы

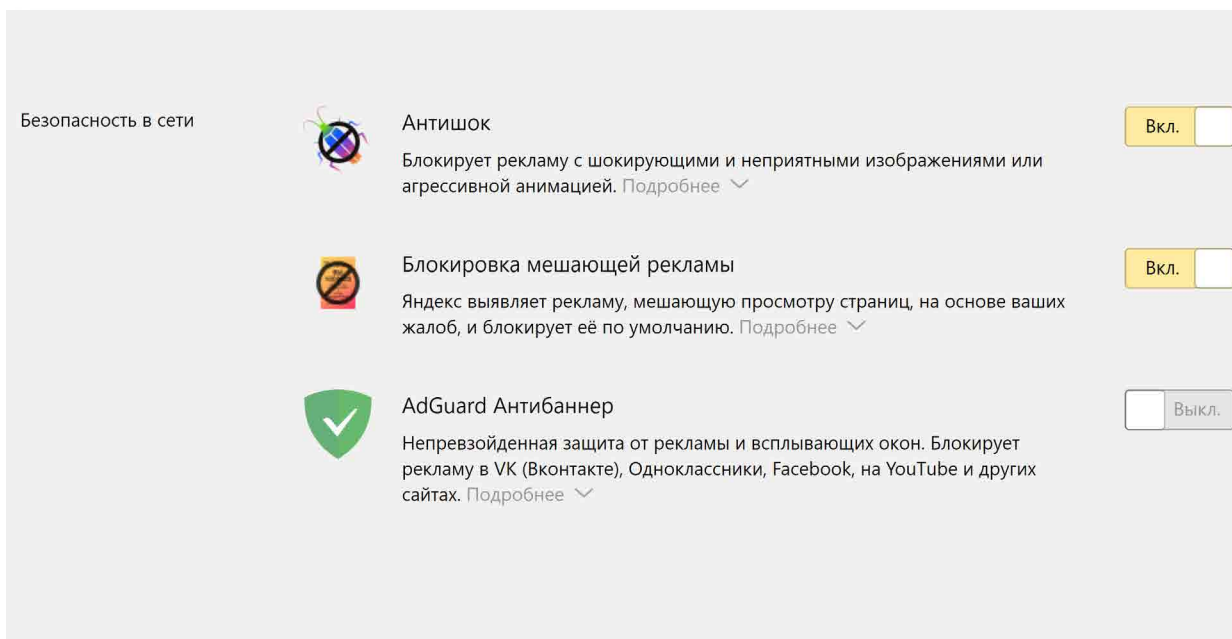
Расширения Число результатов поиска для 'блокировщик рекламы': 25

	Вконтакте без ... Убрать рекламу... ★★★★★ (5)		EX.UA/FS.UA б... Позволяет отклю... ★★★★★ (7)		AdBlocker Ulti... Бесплатный и ул... ★★★★★ (225)		Stop Reclame Удаление навязч... ★★★★★ (144)
	Calculator Sma... Универсальный... ★★★★★ (12)		«You Clever» ... В YouTube еще у... ★★★★★ (35)		Ghostery Ghostery - это мо... ★★★★★ (1043)		Adguard Непревзойденна... ★★★★★ (3032)
	Pre-Roll Block Автоматически п... ★★★★★ (2)		AllBlock AllBlock - беспла... ★★★★★ (13)		AdNauseam Противодействи... ★★★★★ (85)		Kenzo VK Улучшение инте... ★★★★★ (91)

После того, как вы выбрали расширение, нажмите «Добавить в Яндекс.Браузер». Можно настроить отображение скачанного расширения в верхней панели.

Вы всегда сможете остановить работу расширения. Для этого нужно перейти в «Настройки», далее в раздел «Дополнения» и поставить рычажок напротив соответствующего расширения в положение «Выключено» 4.19.

4.19



Безопасный поиск в интернете

Все настройки безопасного поиска в интернете есть в браузере. Во многом они защищают пользователя от шокирующего или нежелательного контента 4.20.

4.20

Но есть сайты-поисковики, которые предоставляют возможность анонимного поиска.

Такие поисковики не сохраняют ваш IP-адрес, не используют и не сохраняют файлы куки для отслеживания.

Например, Mozilla (Мозила) заботится о приватности, поэтому Firefox (Фаерфокс) не только не подсматривает за вами, но и блокирует чужие инструменты слежки.

Поисковики DuckDuckGo (Дак дак гоу) и StarPage (СтарПейдж) не запоминают, что вы искали. Но и результаты поиска на ваши запросы в этих поисковых системах не столь полные, как в привычных поисковиках.

Вам выбирать, какие инструменты и настройки использовать. Здесь главное соблюсти баланс. Быть осторожным, но не впадать в панику.

Контрольные вопросы

1. Как работает брандмауэр?
2. Какие настройки нужно прежде всего найти в браузере?
3. Достаточно ли для безопасности только настроить браузер?
4. Как настроить блокировщик рекламы?
5. Нужно ли удалять куки и кэш? Зачем?
6. Можно ли убрать из браузера информацию о введенных вами данных платежных карт?
7. Стоит ли смотреть настройки аккаунта в браузере?



Система надежных паролей

5

ГЛАВА

Как работает цифровой пароль

Вся личная персональная информация в сети защищается паролями. Пара «Логин-Пароль», которую вы придумываете, регистрируясь на сайтах, – это главный ключ к вашей информации. И если логином может быть стандартная информация: номер сотового телефона, адрес электронной почты, ваше имя, то вот паролем должна быть сложная комбинация цифр, букв и символов.

Когда вы проходите регистрацию на сайте, введенные логин и пароль сохраняет браузер и сайт, где вы регистрируетесь.

Пароли дают вам доступ к вашему счету в банке, к услугам государственных ведомств, электронной почте, к аккаунтам в социальных сетях, к интернет-магазинам. Уже в 2017 году у одного пользователя было в среднем порядка 191 регистраций в сети по логину и паролю. Это 191 пароль.

Сложно помнить и управлять таким количеством паролей, поэтому люди в конечном итоге используют один и тот же пароль или самые простые комбинации, что повышает шансы стать жертвами мошенников.

Как работает сервис восстановления паролей

В целом, это полезная функция. Можно восстановить пароль, если забыли его. Для этого при регистрации на сайтах вас могут попросить указать данные электронной почты, или номер мобильного телефона, или контрольный вопрос [5.1](#).

5.1

Куда ВХОД

РЕГИСТРАЦИЯ

Email *

Логин * ?

Пароль * ?

Подтверждение пароля *

Имя *

Фамилия *

Телефон

Даю своё **согласие** ОАО «РЖД» на обработку представленных мной персональных данных. [Политика обработки персональных данных в ОАО «РЖД» *](#)

Соответственно, при восстановлении пароля вам могут предложить выбрать, как восстановить пароль: через почту, номер мобильного телефона или через ответ на контрольный вопрос.

Поэтому рекомендуется указывать действующие номер телефона или адрес электронной почты.

Вместе с тем, узнав ваш пароль от электронной почты, мошенники могут восстановить и другие данные.

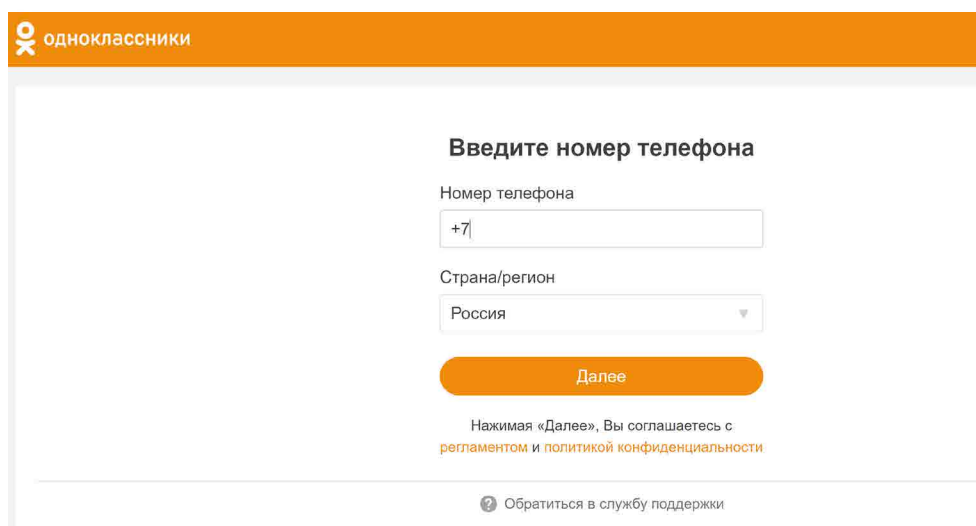
Обратите внимание, если при восстановлении пароля вам на почту высылается введенный некогда вами логин и пароль, значит, сайт хранит ваши данные в открытом виде. Рекомендуется такие сайты не посещать, не проводить на них каких-либо платежных операций и по возможности удалить свои данные с них.

Чаще всего пароли хранятся в хеше, то есть это некий набор символов, который невозможно расшифровать, поэтому вам всегда предлагается придумать на смену старому паролю новый.

Также сегодня используются новые технологии для восстановления пароля: переходы по QR-коду, биометрия, двухфакторная аутентификация. Такие форматы считаются достаточно надежными вариантами восстановления пароля.

Некоторые сайты перешли на регистрацию только по номеру мобильного телефона. По нему же можно и восстановить пароль [5.2](#).

5.2



The screenshot shows the registration page for 'одноклассники' (ok.ru). The header is orange with the logo and name. The main content area is white and contains the following elements:

- Title: **Введите номер телефона**
- Label: **Номер телефона**
- Input field: Contains '+7|' with a cursor.
- Label: **Страна/регион**
- Dropdown menu: Shows 'Россия' with a downward arrow.
- Button: Orange button with the text 'Далее'.
- Text: Нажимая «Далее», Вы соглашаетесь с [регламентом](#) и [политикой конфиденциальности](#).
- Link: Обратиться в службу поддержки with a question mark icon.

С одной стороны, это более безопасный способ в отличие от восстановления по адресу электронной почты, с другой, телефон тоже может попасть в руки мошенников или быть утерян. А значит, безопасность аккаунта может быть под угрозой. К тому же есть риск полной утраты доступа на такой сайт. Поэтому обычно при регистрации по номеру телефона дополнительно просят ввести и адрес электронной почты.

Старайтесь избегать вариантов восстановления пароля по кодовому слову или ответу на секретный вопрос. А если все же используете подобный вариант, то для разных сервисов используйте разные секретные вопросы. К слову, записать их можно в программе менеджер паролей. Как работает данное приложение, рассмотрим в этой главе.

Эксперты по кибербезопасности рекомендуют: зарегистрируйте несколько ящиков электронной почты. Один будет для переписок, уведомлений с портала Госуслуг, интернет-банкинга, второй используйте для регистрации в интернет-магазинах, форумах, социальных сетях.



Как мошенники получают доступ к паролям

Есть несколько вариантов.

1. **Простая кража данных.** Пароли на сайтах часто хранятся в открытом или зашифрованном виде. Если аферу захочет проверить администратор сети, и у него есть ключ к зашифрованным данным пользователей, значит, он всегда их может расшифровать, продать или сам воспользоваться информацией для того, чтобы получить доступ к интернет-банкингу и вашему счету. Если пользователь к тому же вводил данные карты и совершал покупку на этом сайте, то нечистый на руку сотрудник по номеру карты может вычислить банк. Если у вас везде один пароль, получить доступ к интернет-банкингу проще простого.

2. Другой вариант – **социальная инженерия**. Мошенники с помощью различных уловок заставляют пользователя сообщить нужные данные. Многие ведутся на предложения получить дополнительные выплаты – и в результате на подставных сайтах вводят свои пароли от личного кабинета портала Госуслуг или сайта банка, где у них открыты счета. Верят, что им звонят из банка, и якобы для спасения своих денег на счету сообщают пароли и ПИН-коды от платежных карт или интернет-банкинга.

Внимательно смотрите на адрес сайта, на который вы перешли после призыва получить дополнительную (лишнюю) социальную выплату. Лучше сами зайдите на портал Госуслуг и проверьте информацию. Если вам предлагают получить выплату, такое сообщение будет у вас на Госуслугах в уведомлениях в личном кабинете. Лучше просто перезвонить в ведомство. Не предпринимайте никаких действий, если звонят якобы из вашего банка. Положите трубку и перезвоните в банк, уточните ситуацию.

Как мошенники получают доступ к паролям:

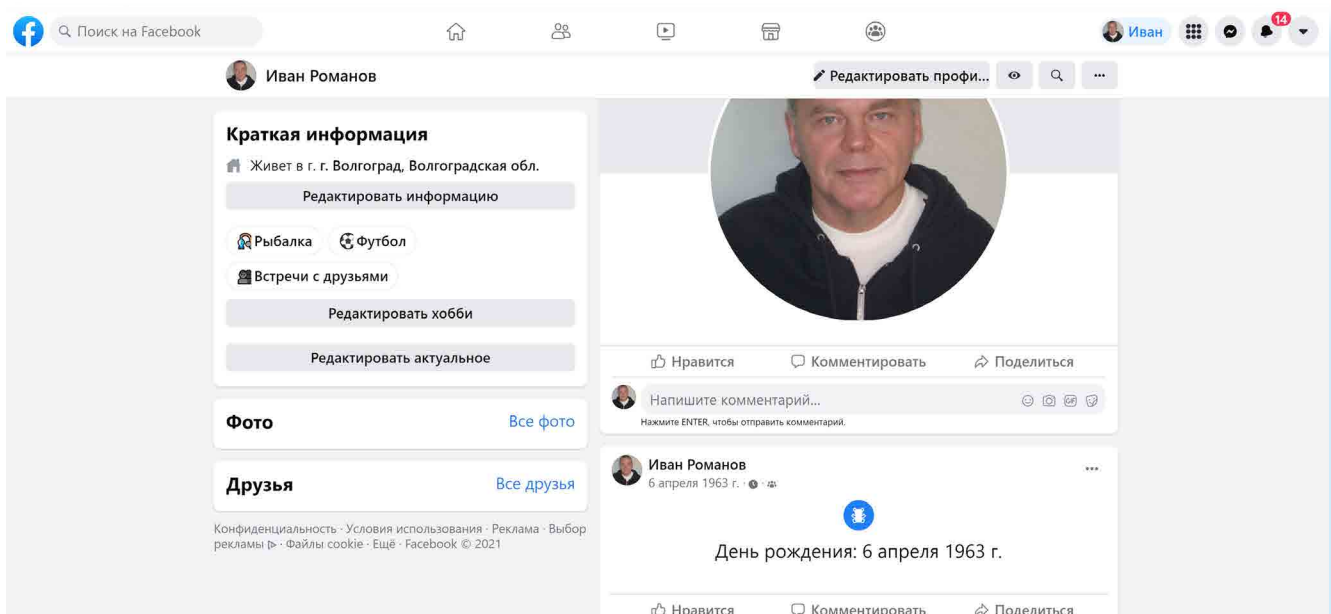
1. Кража с сайтов открытых данных.
2. Технологии социальной инженерии.
3. Взлом паролей – подбор по словарю и брутфорс.

Примеры этих схем в главе 3 «Как действуют мошенники в интернете, способы защиты» модуля 10 «Кибербезопасность» расширенного курса «Азбука интернета».

3. **Взлом пароля.** Существует два варианта подбора пароля: по словарю – когда программа последовательно перебирает весь свой словарь и подставляет подходящие слова, а второй – подбор перестановок букв в слове (брутфорс). **Брутфорс** – насильственный метод угадывания пароля. Если пароль короткий, типа 12345 или qwerty11, программа практически сразу его раскроет.

Точно так же быстро можно справиться и с паролем, содержащим ваше имя, или дату рождения, или кличку любимого домашнего животного. В 90% случаях эти данные есть в социальных сетях или на других сайтах, где вы указывали информацию о себе 5.3.

5.3



Двухфакторная аутентификация, биометрия, QR-коды

Двухфакторная аутентификация

Система двухфакторной аутентификации была изобретена для дополнительной защиты пользовательских аккаунтов. Она позволяет проверить, действительно ли человек, зашедший в аккаунт, тот, за кого себя выдает. К тому же, у пользователей появляется больше возможностей не потерять доступ к аккаунту. Работает она так: вы вводите логин и пароль. Если они правильные, на ваш телефонный номер приходит смс с кодом, который нужно будет ввести в следующем поле. В некоторых случаях это может быть звонок на ваш мобильный телефон. Нужно будет ввести в поле четыре последние цифры номера, с которого поступил звонок.

Фактически это двойной пароль. Бывает многофакторная аутентификация, то есть проверка по трем-четырем данным. Это может быть пароль, код из смс и отпечаток пальца. Тут три уровня защиты аккаунта.

Доступ в банковские приложения часто осуществляется через систему двухфакторной аутентификации. Чтобы зайти в аккаунт, нужно ввести пароль и код, пришедший в смс.

Такой способ защиты сегодня можно подключить и к своему электронному почтовому ящику, и даже для входа в аккаунты в социальных сетях.

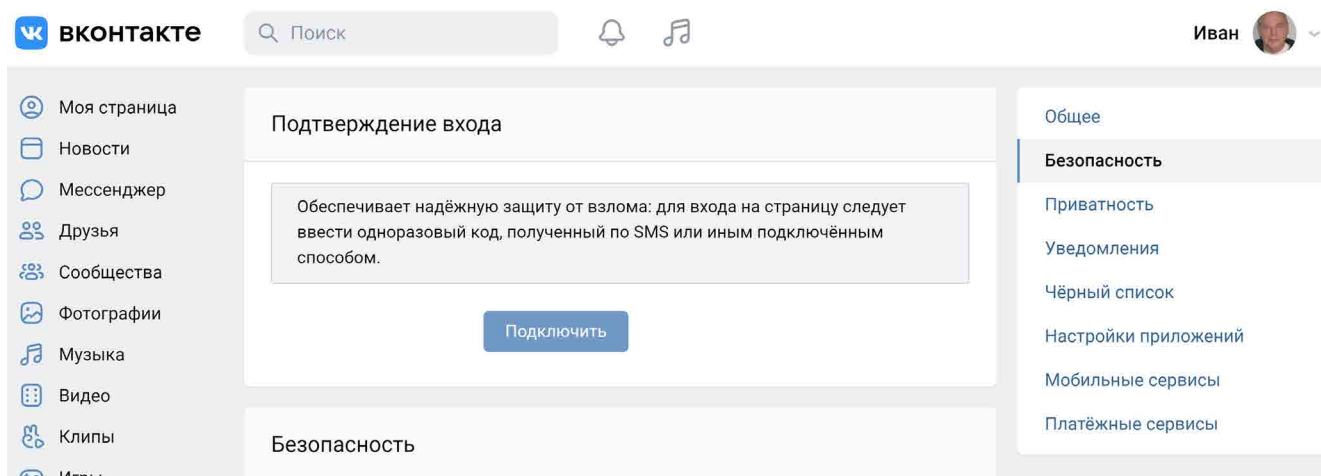
Чтобы настроить двухфакторную аутентификацию в социальной сети ВКонтакте, нужно:

- нажать на значок профиля вверху справа;
- выбрать раздел «Настройки» 5.4;

5.4

The screenshot shows the VK profile page for Ivan Romanov. The top navigation bar includes the VK logo, the text 'вконтакте', a search bar with 'Поиск', and notification and music icons. The left sidebar contains a menu with options: 'Моя страница', 'Новости', 'Мессенджер', 'Друзья', 'Сообщества', 'Фотографии', 'Музыка', 'Видео', 'Клипы', 'Игры', 'Мини-приложения', 'VK Pay', and 'Работа'. The main content area shows the profile picture of Ivan Romanov, a 'Редактировать' button, and a 'Воспоминания' section. To the right, the profile information is displayed: 'Иван Романов', 'установить статус', 'День рождения: 3 февраля 1946 г.', 'Город: Волгоград', and 'Образование: ВГАФК'. Below this is a 'Показать подробную информацию' link. A '1 фотография' section is visible. On the far right, a dropdown menu is open, showing options: 'Иван Романов', 'Перейти в VK Connect', 'Настройки', 'Помощь', and 'Выйти'.

- далее справа выбрать пункт «Безопасность»;
- 5.5
- затем под пунктом «Подтверждение входа» кликнуть «Подключить» 5.5;



- и далее приступить к настройке.

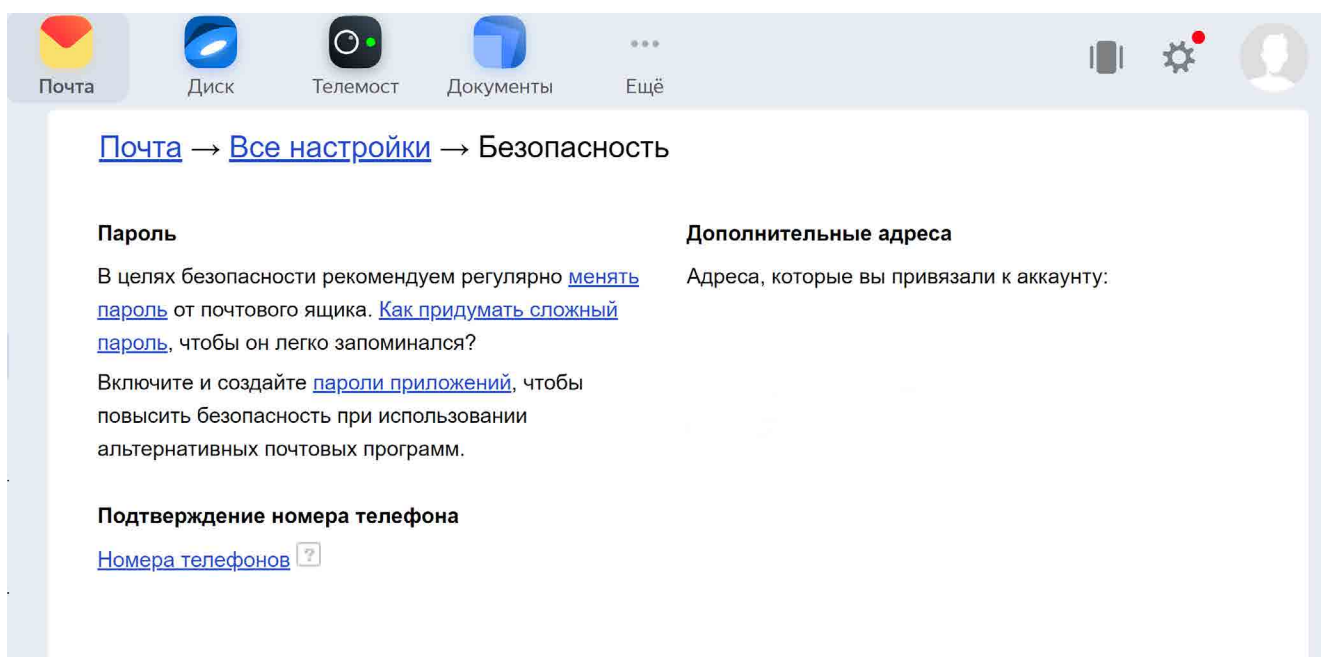
! Обратите внимание, что, подключая двухфакторную аутентификацию в аккаунте в социальной сети в ВКонтате, нужно указать и номер телефона, и вашу электронную почту. В случае утери пароля вам будет проще восстановить доступ на страницу.



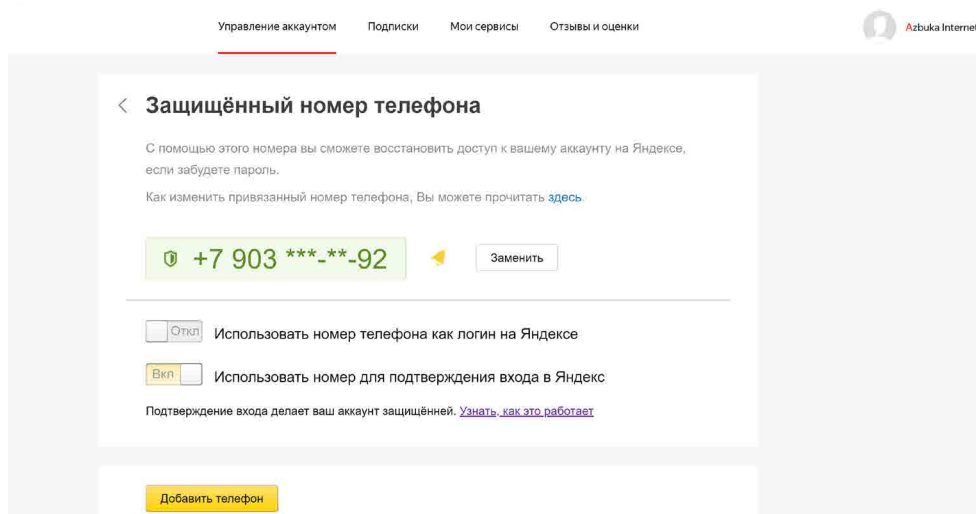
Также можно подключить проверку по смс-коду и к Яндекс.Почте:

- зайдите в свою Яндекс.Почту;
- вверху справа выберите «Настройки» (значок шестеренки);
- далее кликните по разделу «Безопасность»;
- затем в блоке «Подтверждение номера телефона» кликните на строчку «Номера телефонов» 5.6.

5.6



На следующей странице напротив строчки «Использовать номер для подтверждения входа в Яндекс» ползунок нужно передвинуть вправо, то есть включить. Теперь, если в почте авторизуются на другом устройстве, на телефон придет смс с кодом, который нужно будет ввести, чтобы получить доступ в почту 5.7.



5.7

Чтобы настроить двухфакторную аутентификацию в почте или социальных сетях, нужно:

1. Перейти в настройки вашего профиля.
2. Выбрать блок «Безопасность».
3. Выбрать настройки подтверждения входа по смс (либо настройки двухфакторной аутентификации).

Биометрия и QR-коды

В 2019 году социальная сеть Фейсбук признала, что пароли от миллиона аккаунтов в Инстаграм хранятся в недостаточно защищенной базе данных. А летом этого же года логины и пароли покупателей маркетплейса OZON оказались в сети в свободном доступе. В октябре 2019 года в интернет попали сведения о владельцах кредитных карт Сбербанка. В результате уже многие компании намерены отказаться от паролей и начать использовать **биометрические данные**: отпечатки пальцев, сканирование радужной оболочки глаз, движения лица.

Так, в 2019 году National Westminster Bank начал испытывать дебетовые карты со встроенным в них «сканером» отпечатков пальцев.

Впрочем, биометрическая информация также может быть украдена, хотя сделать это намного сложнее, чем подобрать пароль. К примеру, существует технология, которая позволяет «извлечь» отпечаток пальца человека из фотографии, сделанной на расстоянии 1,5 м.

И все-таки, на сегодня это достаточно надежный вариант сохранить свои личные данные. Например, биометрию уже давно используют в мобильных телефонах. В настройках можно установить вход по **TouchID** (ТачАйди) – по отпечатку пальца 5.8.



5.8

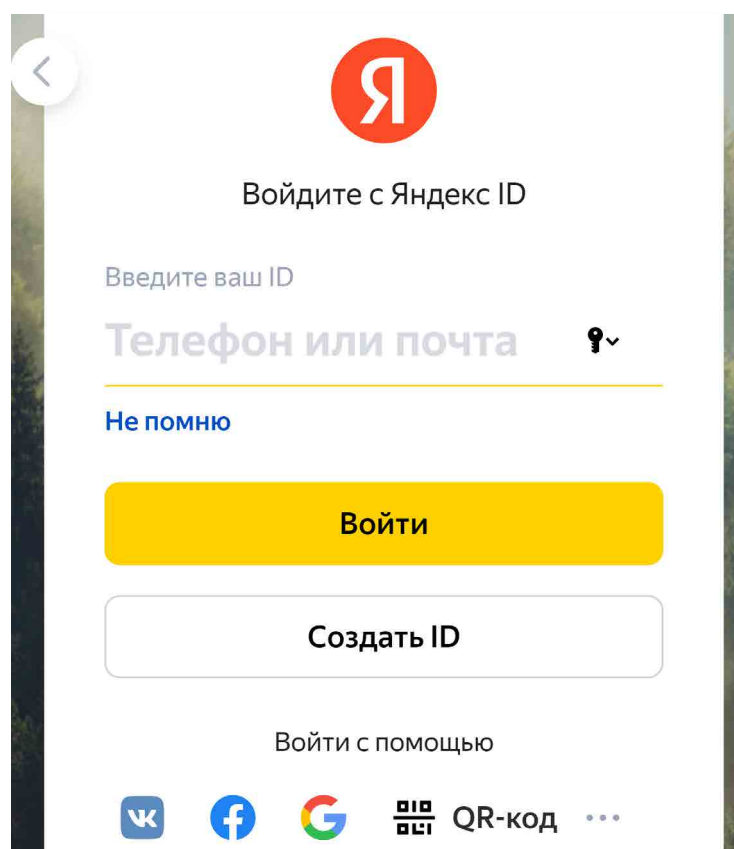
В Айфонах применяется технология **FaceID** (ФейсАйди) – распознавание лица. Если у вас установлена такая функция, то вход в приложение онлайн-банка или в приложение Госуслуги будет по биометрическим данным. Пароль вводить не потребуется.

Если в вашем устройстве включен вход по биометрическим данным, войти чужому человеку будет сложно. Ему нужно будет, как минимум, отключить данную функцию. А это практически невозможно в отсутствие владельца.

Еще один вариант авторизации в аккаунте – **QR-код**. Это удобно, если у вас электронная почта открыта на мобильном устройстве, и вы теперь хотите войти в нее на компьютере.

Так в Яндекс.Почте, если вы откроете форму авторизации, внизу увидите функционал «Войти с помощью QR-кода» 5.9.

5.9



Если кликнуть по этой надписи, откроется QR-код. Вам нужно открыть в мобильном телефоне «Камеру» и навести ее на QR-код. Компьютер загрузит данные, и вы сможете войти в свою почту. Данный вариант подтверждения личности также достаточно безопасен.



Если вы решили зайти в почту на чужом компьютере, делайте это в режиме «Инкогнито». Для этого нужно перейти в настройки браузера и выбрать «Режим Инкогнито». В этом случае история ваших посещений не сохранится на чужом компьютере.

Пароли для финансовых приложений

Безопасность онлайн-банков – одна из главных задач и для клиентов, и для самих финансовых организаций. Если банк не будет усиливать и обновлять систему безопасности, то просто потеряет клиентов.

Банковские сайты сегодня ограничивают количество попыток входа в онлайн-банк. Финансовые организации следят, чтобы веб-сайты имели дополнительные уровни шифрования.

Конечно, для входа в онлайн-банк нужно придумать сложный и надежный пароль. Ваш пароль должен быть уникальным и ни в коем случае не тот же самый, что и для других сайтов.

Если финансовое приложение стоит на смартфоне, для входа на устройство поставьте биометрический пароль (например, TouchID).

Обратите внимание еще на несколько правил:

- работайте в онлайн-банке только на компьютерах с антивирусной программой;
- не заходите в приложения финансовых организаций, на электронную почту и в свои аккаунты в социальных сетях в общественных Wi-Fi сетях;
- прежде чем войти на сайт банка, закройте все остальные вкладки и приложения (при работе на компьютере);
- никогда не переходите в онлайн-банк по ссылкам, присланным в письмах от банков. Почти 100% вероятность, что это письма от мошенников. А сайты, на которые предлагается перейти и ввести данные якобы для тестовых платежей или других транзакций, – поддельные;
- когда проводите платежи, переходите сами в онлайн-банк, набирая адрес в браузере (при работе на компьютере).

Как придумать надежный пароль

Самый главный вопрос – как придумать надежный пароль. С течением времени программы-взломщики совершенствуются. И те алгоритмы составления пароля, которые применялись 5 лет назад, сегодня с легкостью разгадываются мошенниками.

Насколько надежен ваш пароль?

1. Он длинный? Сколько в нем символов? Эксперты рекомендуют минимум 10–12 символов, а лучше еще длиннее. Программе будет сложнее подобрать комбинации для взлома пароля.
2. Какие символы у вас в пароле? Только буквы? Пять букв и пять цифр? А есть строчные и заглавные буквы? В правильном пароле обязательно должны быть разнообразные символы: цифры, буквы строчные и заглавные, символы пунктуации. Для бутфорса особенно сложно распознать символы, отличные от буквенно-цифровых.

Как создать надежный пароль:

1. Длина пароля должна быть не менее 10 символов.
2. Использовать разные символы.
3. Не использовать повторяющиеся цифры и буквы.
4. Использовать нелогичные сочетание символов.
5. Никогда не создавать пароль из личных данных: ФИО, кличка собаки, номер телефона или дата рождения.

Желательно, чтобы цифры, буквы и символы не повторялись. Например, вы придумали пароль: OnStage179. Если добавить сюда нижнее подчеркивание OnSt_age179, разгадать пароль будет уже сложнее.

Не думайте, что сможете провести взломщиков, если наберете русское название на клавиатуре в латинской раскладке. Такие уловки брутфорс быстро распознает. Лучше, если в вашем пароле используются необычные или нелогичные сочетания.

Конечно, самым надежным будет пароль из случайных символов, типа qo9n76R2Xlk89g%. Но если вы все-таки в основу пароля закладываете какое-то слово, как например, «onstage» (перевод с английского: «на сцене»), можно добавить к нему нелогичное сочетание букв, скажем: OnSt_age179_sjf.

Иногда для создания надежного пароля используют первые буквы какой-то нелогичной фразы. Например, Ze_Sl&Ho?PoKг. Здесь в сочетании с пунктуационными символами зашифрована фраза: «Зеленые слоны ходят по кругу». Взяты по две первые буквы из каждого слова.

Для создания пароля можно воспользоваться онлайн-генератором паролей. Вот один из сайтов, который готов помочь в создании паролей – onlinepasswordgenerator.ru. Здесь нужно выбрать, какие символы будут в пароле, каково их количество. И нажать «Создать». Вот несколько надежных паролей, который создал генератор [5.10](#).

5.10

Генератор паролей

Хотите сгенерировать пароль? Просто заполните форму ниже и нажмите кнопку "Создать пароль".

Настройки генератора:

- Цифры
- Прописные буквы
- Строчные буквы
- Спец. символы %, *,), ?, @, #, \$, ~

Длина пароля: 10 - символов

Создать пароль

Ваши сгенерированные пароли:

- SY5L2lqdS~
- HCz7P|nLPb
- J5*nlygJeZ
- QJJAzELNnd
- mNm0~OD74*
- leyFQdexx0
- nGBg}NQx}q
- ubrj8DxLf3
- ICHt~%LVxm
- laV0EajjdP

Иногда и не нужно обращаться к генератору паролей. Зачастую сайт, на котором вы регистрируетесь, сам предлагает создать надежный пароль. Можно этим воспользоваться. Но не забудьте пароль записать.

Не используйте одинаковые пароли для разных сайтов. Они должны быть разные. Особенно для соцсетей, банковских приложений, личных кабинетов финансовых организаций и любых порталов, где может храниться ценная для вас информация. Меняйте пароли примерно раз в полгода.



Эксперты рекомендуют составлять пароль так, чтобы он был понятен вам, но труден для машинного подбора.

Как и где хранить пароли, менеджер паролей

Можно записать пароли в блокноте. Но он может потеряться или попасть в руки к нечестным людям.

Можно записать в текстовом файле на компьютере. Но его без труда может найти и прочитать взломщик или вирусная программа.

Можно предпринять несколько вариантов защиты. Например, в списке паролей в каждом из них добавить лишние цифры, о которых будете знать только вы. Тут главное не забыть об этом.

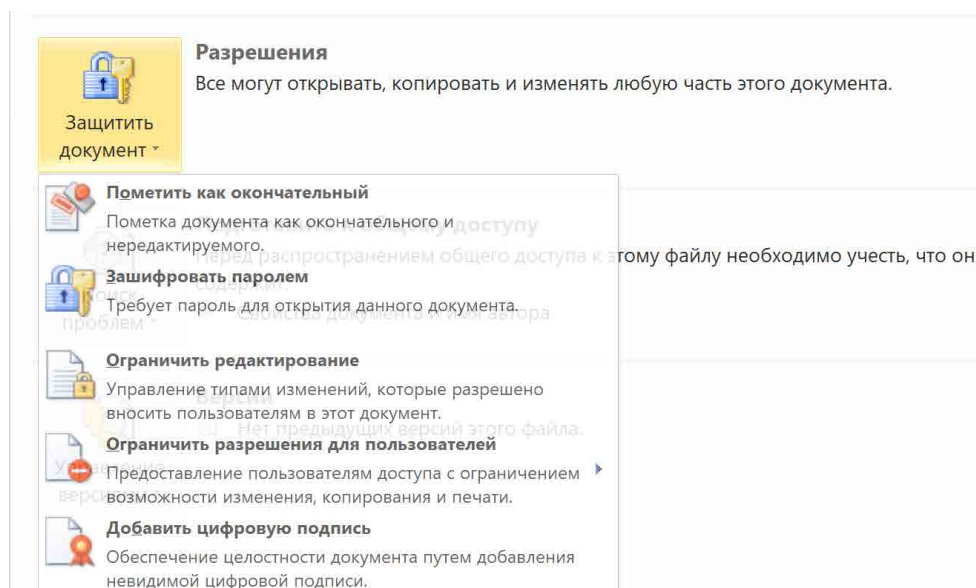
Шифрование файла с паролями

Можно также файл зашифровать.

В программе Microsoft Word, чтобы зашифровать документ, нужно:

- нажать в верхнем меню «Файл»;
- в разделе «Сведения» перейти к блоку «Разрешения»;
- нажать на надпись «Защита документа»;
- в выпавшем меню выбрать «Зашифровать с использованием пароля» 5.11;

5.11

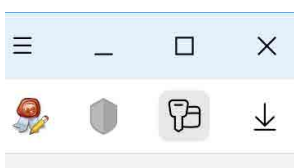


- затем ввести пароль и нажать «ОК».

То есть вам нужно будет запомнить лишь один пароль, чтобы найти все остальные. Очень важно его не забыть, поскольку восстановить такой пароль от зашифрованного документа не получится.

Менеджер паролей в браузере

Можно использовать менеджер паролей в браузере. Браузер и так сохраняет ваши логины и пароли, если, конечно, вы не настроили запрет на такие действия или автоматическое стирание всей истории при выходе из браузера. Но теперь можно защитить паролем сохраненные в браузере данные.

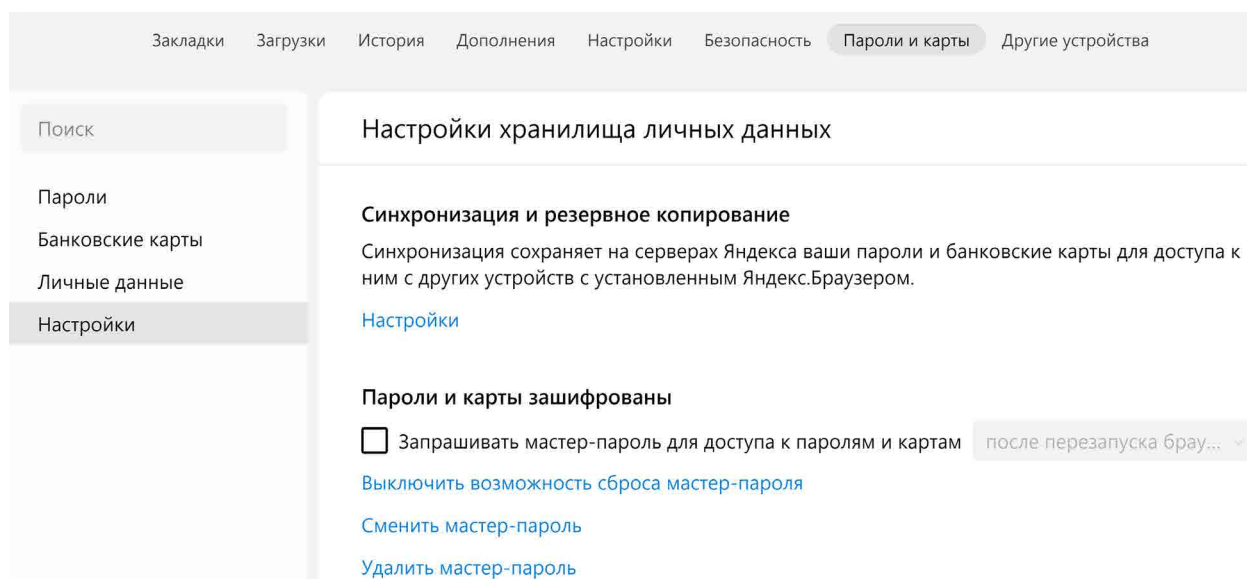


В Яндекс.Браузере вкладка «Пароли и карты» по умолчанию выведена в панель управления вверху справа. (Если такого значка у вас нет, к вкладке «Пароли и карты» можно перейти через «Настройки» браузера).

Чтобы поставить мастер-пароль к хранилищу логинов и паролей в браузере Яндекс, нужно:

1. В разделе «Пароли и карты» слева выбрать пункт «Настройки».
2. Кликнуть в квадратике около строчки «Запрашивать мастер-пароль для доступа к паролем и картам» [5.12](#).

5.12



3. Придумать и ввести надежный мастер-пароль.
4. Нажать «Сохранить».

Теперь для доступа к вашим логинам и паролям нужно будет набрать мастер-пароль. Запомните или запишите его и положите в надежное место.

Обратите внимание: по умолчанию включается функция возможности сброса мастер-пароля, если вдруг вы его забудете. Конечно, для большей надежности лучше выключить данную возможность.

В целом, это достаточно безопасный вариант хранения паролей.

Менеджер паролей как дополнительная программа

Можно установить и отдельную программу, где будут храниться в зашифрованном виде ваши пароли. Таких программ много. Есть менеджер паролей от Лаборатории Касперского, он встроен в антивирусную программу. Есть бесплатная программа KeePass Password Safe. У нее есть Portable (портабл) версия, которую не нужно устанавливать, а можно просто носить на флеш-накопителе. Есть платные и бесплатные менеджеры паролей. Здесь важно выбрать то, что будет удобнее для вас.

В целом, как вы уже заметили, все менеджеры паролей работают по одному принципу. Создается база паролей, и доступ к ней шифруется мастер-паролем.

Он также должен быть надежным, и важно его не потерять. Менеджер паролей – удобная программа, учитывая, что сейчас пользователи регистрируются на десятках сайтов, и запомнить все логины и пароли просто невозможно.

Обязательно выберите для себя удобный и безопасный способ хранения паролей.

Контрольные вопросы

1. Где применяются пароли?
2. Почему нужно придумывать надежные пароли?
3. Можно ли хранить в браузере введенные на сайтах логины и пароли?
4. Каким должен быть надежный пароль?
5. Что такое двухфакторная аутентификация?
6. Для чего используется менеджер паролей?
7. Почему биометрия является одним из надежных вариантов пароля?



Сохранность личной информации

6 ГЛАВА

Несем устройство в ремонт

Если ваш компьютер или телефон сломался, единственный выход – нести его в мастерскую. Но перед этим нужно обратить внимание на два момента.

1. Насколько профессиональны мастера, которым вы отдаете устройство для ремонта.
2. Необходимо установить защиту данных, которые находятся на компьютере или смартфоне.

Не идите в первый попавшийся или самый разрекламированный сервисный центр. Поинтересуйтесь рекомендациями ваших знакомых. Возможно, кто-то уже пользовался услугами по ремонту.

Если вы ищете ремонтную мастерскую через интернет, почитайте отзывы о данной компании, и только потом принимайте решение.

Когда будете сдавать устройство в ремонт, вам должны выдать квитанцию приема-выдачи оборудования.

В квитанции должны быть:

- дата;
- ФИО и подпись ваша и приемщика;
- подробное описание неисправности;
- описание технического и визуального состояния устройства;
- указание модели, серийного номера, IMEI.

Некоторые специалисты рекомендуют сделать фотографии вашего устройства на момент сдачи в ремонт.



После диагностики обычно озвучивают точную сумму ремонта. Если же после диагностики вам снова называют приблизительную стоимость и приблизительный срок ремонта, примерный срок гарантии, то, возможно, это сигнал поискать другую ремонтную мастерскую.

На что обратить внимание, если необходимо отнести устройство в ремонт:

1. Выбор ремонтной мастерской.
2. Защита конфиденциальной информации, которая есть на устройстве.

Варианты, как защитить свои данные при сдаче компьютера в ремонт:

1. Воспользоваться командой «Сделать резервную копию», а затем удалить все данные с компьютера.
2. Зашифровать жесткий диск.
3. Вручную скопировать приватные папки и файлы, затем удалить их с устройства.
4. Попросить в ремонтной мастерской при вас вытащить накопительный диск и забрать его.

Обязательно уточняйте: какие работы будут проведены, за какую сумму, в какие сроки и каков период гарантии.

Когда будете принимать устройство, обязательно проверьте его работу и осмотрите визуально. И только после этого принимайте и подписывайте акт выполненных работ.

Если неисправность устройства не ограничивает вам доступ к личным данным, то стоит провести ревизию. Внимательно посмотрите, что нужно обязательно удалить (при этом не забыть сохранить эту информацию на флеш-накопителе), а что можно оставить.

Есть несколько вариантов:

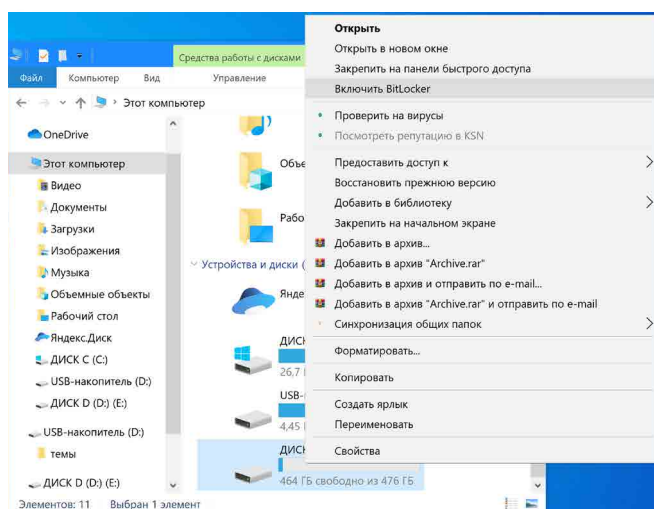
- воспользоваться командой «Сделать резервную копию» и так перенести данные на флешку, а затем удалить все с компьютера (в смартфоне это процесс проще);
- вручную перенести нужные данные на внешний накопитель (флешку) и затем удалить файлы и папки, которые скопировали;
- зашифровать жесткий диск;
- попросить при вас вытащить из компьютера SSD-накопитель (диск внутри компьютера, на котором хранится информация) и забрать его с собой.

Шифрование жесткого диска

Один из вариантов решения для защиты своих данных – шифрование жесткого диска. В Windows есть технология **BitLocker**. Программа уже встроена в операционную систему и проста в использовании:

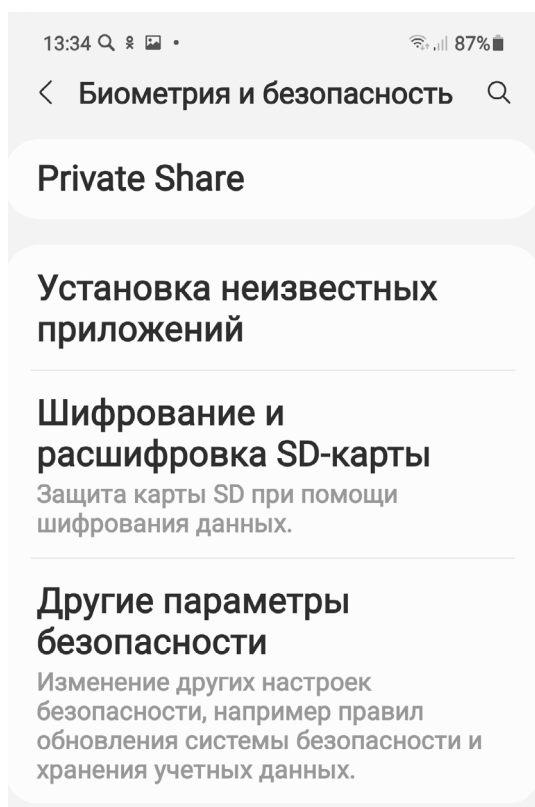
- перейдите в «Пуск»;
- затем зайдите в раздел «Проводник»;
- выберите «Этот компьютер» или «Мой компьютер»;
- выберите диск, который намерены зашифровать, например, диск D;
- наведите на диск курсор и нажмите правую кнопку мыши;
- в выпавшем меню кликните по команде «Включить BitLocker» 6.1.

6.1



Далее понадобится придумать надежный пароль. Обязательно запишите его. Теперь при каждом входе на диск компьютер будет спрашивать пароль.

В смартфоне также есть возможность шифрования данных. На некоторых моделях таким образом можно зашифровать доступ ко всем данным смартфона, а на других – только доступ к SD-карте. Для подключения шифрования в операционной системе Android в «Настройках» нужно перейти в раздел «Биометрия и безопасность» и выбрать пункт «Шифрование и расшифровка SD-карты» (в нашем примере) 6.2.



6.2

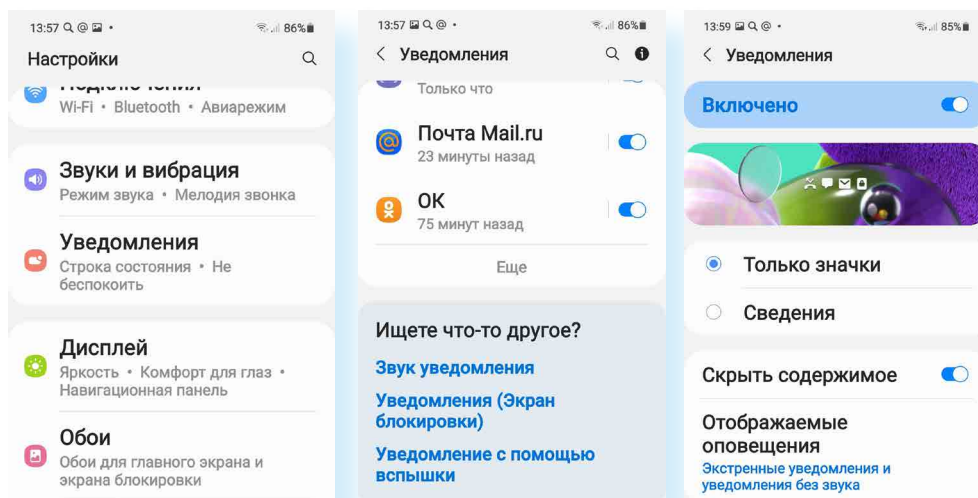
В различных моделях и версиях смартфонов раздел может называться по-разному. Может быть просто «Безопасность», например.

Принцип тот же, что и в компьютере. Нужно будет подтвердить ваше намерение зашифровать данные и придумать надежный пароль. Теперь каждый раз, чтобы получить доступ к информации на SD-карте, нужно будет вводить пароль. Есть и программы, которые позволяют зашифровать данные на смартфоне.

Будет полезным поставить вход по биометрии, по отпечатку пальца (Touch ID). В этом случае при блокировке экрана все данные в смартфоне также находятся в зашифрованном виде. При этом на главном экране могут отображаться уведомления. Их необходимо отключить.

Для этого перейдите в «Настройки», выберите пункт «Уведомления», внизу кликните по строке «Уведомления (Экран блокировки)». Выключите показ уведомлений (передвиньте влево ползунок около надписи «Включено») 6.3.

6.3

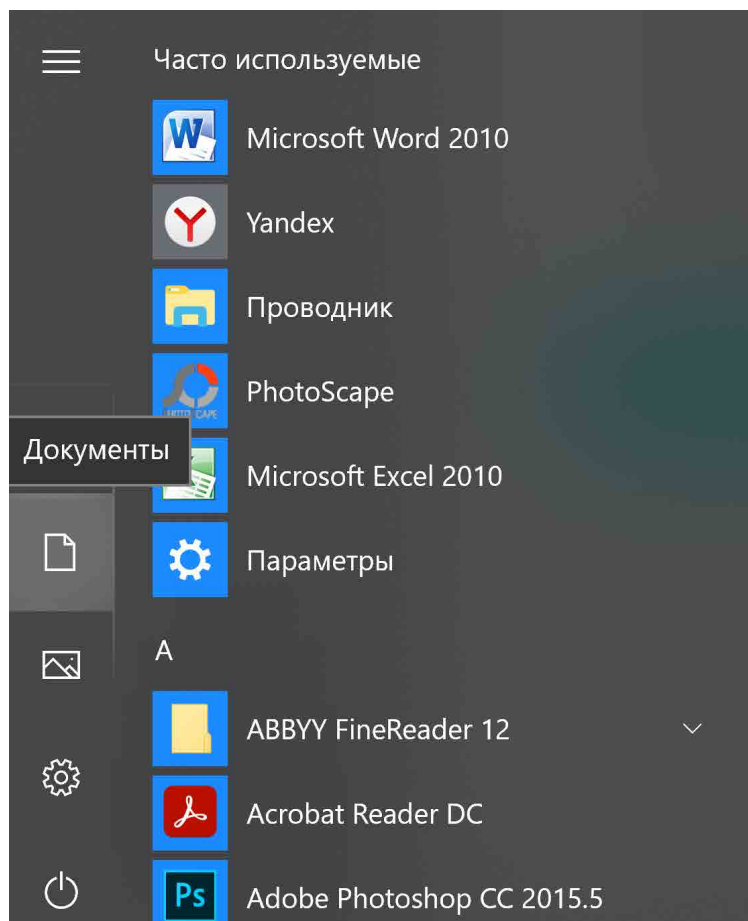


Копирование и удаление важной информации вручную

Один из самых простых способов защиты данных – провести ревизию содержимого вашего компьютера и выбрать файлы, которые нужно скопировать на внешний накопитель (флешку), а с компьютера удалить:

- нажмите «Пуск»;
- затем выберите «Компьютер» (в Windows 7), «Проводник» или «Документы» (в Windows 10) 6.4;

6.4



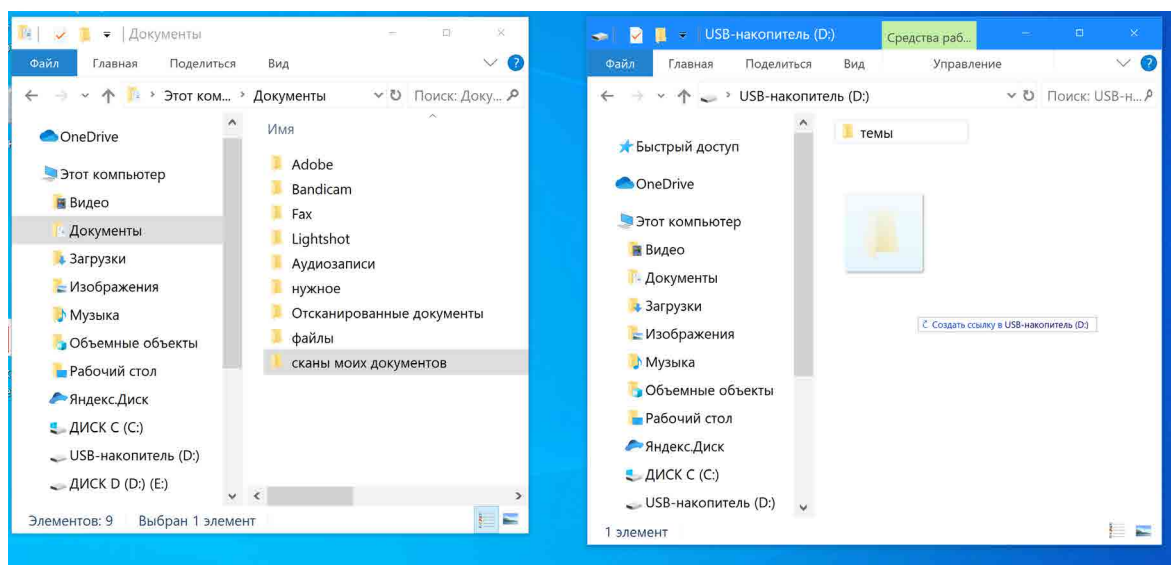
- в меню слева можно перейти в папки, которые есть на компьютере, и выбрать, какие вы будете удалять, а какие оставлять. Это могут быть папки и файлы, хранящиеся на рабочем столе, в пользовательских папках «Документы», «Изображения», «Музыка», на диске D.

Обратите внимание на папки или файлы, где есть записанные пароли от разных интернет-ресурсов (помните, что храниться на компьютере такая информация может только в зашифрованном виде).

Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность»

Проверьте, не хранятся ли на компьютере ваши личные данные (сканы паспортов, других документов, где есть данные вашего СНИЛС, ИНН, адреса электронной почты). Примите во внимание потенциально компрометирующие вас файлы, если таковые есть.

Вставьте внешний накопительный USB-диск (флешку). Откройте его на компьютере и скопируйте сюда файлы и папки, которые не должны попасть в поле зрения посторонних. Можно просто открыть два окна и мышкой перетащить файлы из одного в другое 6.5.



6.5

После того, как вы скопировали нужные данные на флешку, можно удалить папки и файлы с компьютера.

Также в браузере стоит полностью очистить историю вместе с куки-файлами и данными форм сайтов. Для этого в настройках браузера нужно перейти в историю просмотров.

Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность»

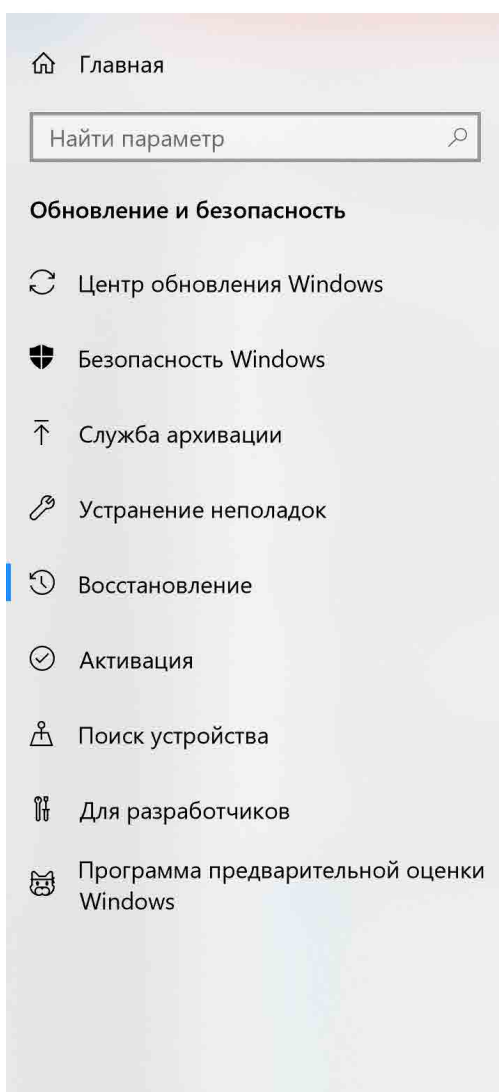
Для списка паролей в браузере лучше включить функцию «мастер-пароль». Выйдите из электронной почты, аккаунтов социальных сетей, личного кабинета портала Госуслуг и других сайтов, где вы проводите оплату. При этом позаботьтесь о сохранении логинов и паролей. Лучший вариант – менеджер паролей.

Можно вообще полностью удалить все ваши данные с компьютера и вернуть его к заводским настройкам. Такой вариант может понадобиться, если вы решили продать устройство.

Чтобы удалить всю информацию на Windows 10:

- нажмите «Пуск»;
- выберите «Параметры»;
- затем блок «Обновление и безопасность»;
- в левом меню выберите «Восстановление»;
- в блоке «Вернуть компьютер в исходное состояние» нажмите «Начать» 6.6;

6.6



Восстановление

Вернуть компьютер в исходное состояние

Если ваш компьютер работает нестабильно, попробуйте восстановить его исходное состояние. Вы сможете при этом сохранить или удалить личные файлы, а затем переустановить Windows.

Начать

Особые варианты загрузки

Запустите систему с устройства или диска (например, USB-накопителя или DVD-диска), измените параметры встроенного ПО компьютера, настройте загрузку Windows или восстановите систему из образа. Ваш компьютер перезагрузится.

Перезагрузить сейчас

Дополнительные параметры восстановления

[Узнайте, как начать заново с чистой установкой Windows](#)

- далее нужно будет выбрать удаление всех файлов и папок и возвращение к исходным заводским настройкам.



При возврате к заводским настройкам будут удалены все программы, которые были установлены пользователем на компьютер, останутся только предустановленные.

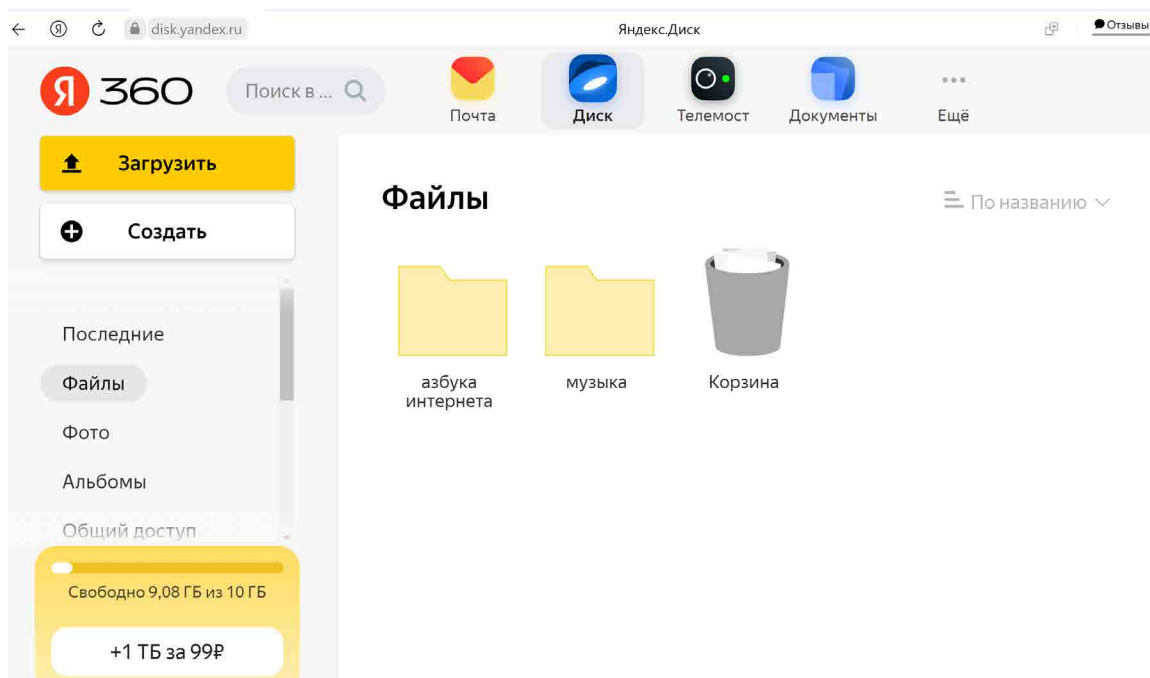
Резервное копирование и облачные сервисы для сохранения ваших данных

Можно также воспользоваться встроенными в операционную систему программами и провести резервное копирование всей информации на устройстве.

При этом скопировать данные можно на внешний накопитель с большим объемом памяти (от 128 ГБ и более), так как на устройстве хранится немало данных. Например, те же фотографии и видео могут занимать большой объем памяти.

Но сейчас все чаще для резервного копирования используют **облачные хранилища**. Это удаленные архивы информации, которые хранятся в сети интернет постоянно. Доступ к тем или иным хранилищам предоставляют различные интернет-ресурсы.

Такие облачные хранилища сегодня есть практически при каждом почтовом сервисе и поисковой системе (Яндекс.Диск у Яндекс.Почты 6.7., Облако Мэйл у Мэйл Почты, Гугл Диск и Гугл Почты и т.д.), у операционных систем Windows – OneDrive (Вандрайв), у iOS (операционной системы устройств Apple) – iCloud (Айклауд), у Самсунг – Samsung Cloud (Самсунг Клауд).



6.7

Это удобно, ведь для регистрации в электронной почте, смартфоне или на компьютере вам предлагается авторизоваться. Практически тут же вы получаете доступ к облачному хранилищу и можете зайти в него с любого устройства в любое время. Вы можете что-то сохранить на компьютере в облаке, а потом посмотреть эти файлы уже с планшета или смартфона.

Например, у Айфона по умолчанию стоит резервное копирование. Оно позволяет, например, не переносить контакты и всю информацию вручную с одного смартфона на другой, если вы решили поменять модель смартфона.

Резервное копирование на компьютере в операционной системе Windows выполнить несколько сложнее, чем на смартфоне или планшете. В Windows это можно сделать через Центр архивации и восстановления, выбрав в настройках параметры «Обновление и безопасность». Здесь понадобятся навыки продвинутого пользователя.

Можно попросить сделать резервную копию и затем полностью очистить компьютер при вас в мастерской. Для этого стоит принести с собой внешний диск. Лучше, если он будет объемом от 128 ГБ до 1 ТБ. Чем больше, тем лучше. Больше шансов, что вся резервная копия на нем уместится. И затем также в мастерской, принимая устройство после ремонта, можно попросить при вас восстановить данные. Возможно, что услуга будет платной.

На смартфоне или планшете сделать резервную копию возможно и пользователю, имеющему только базовые навыки работы на устройстве.

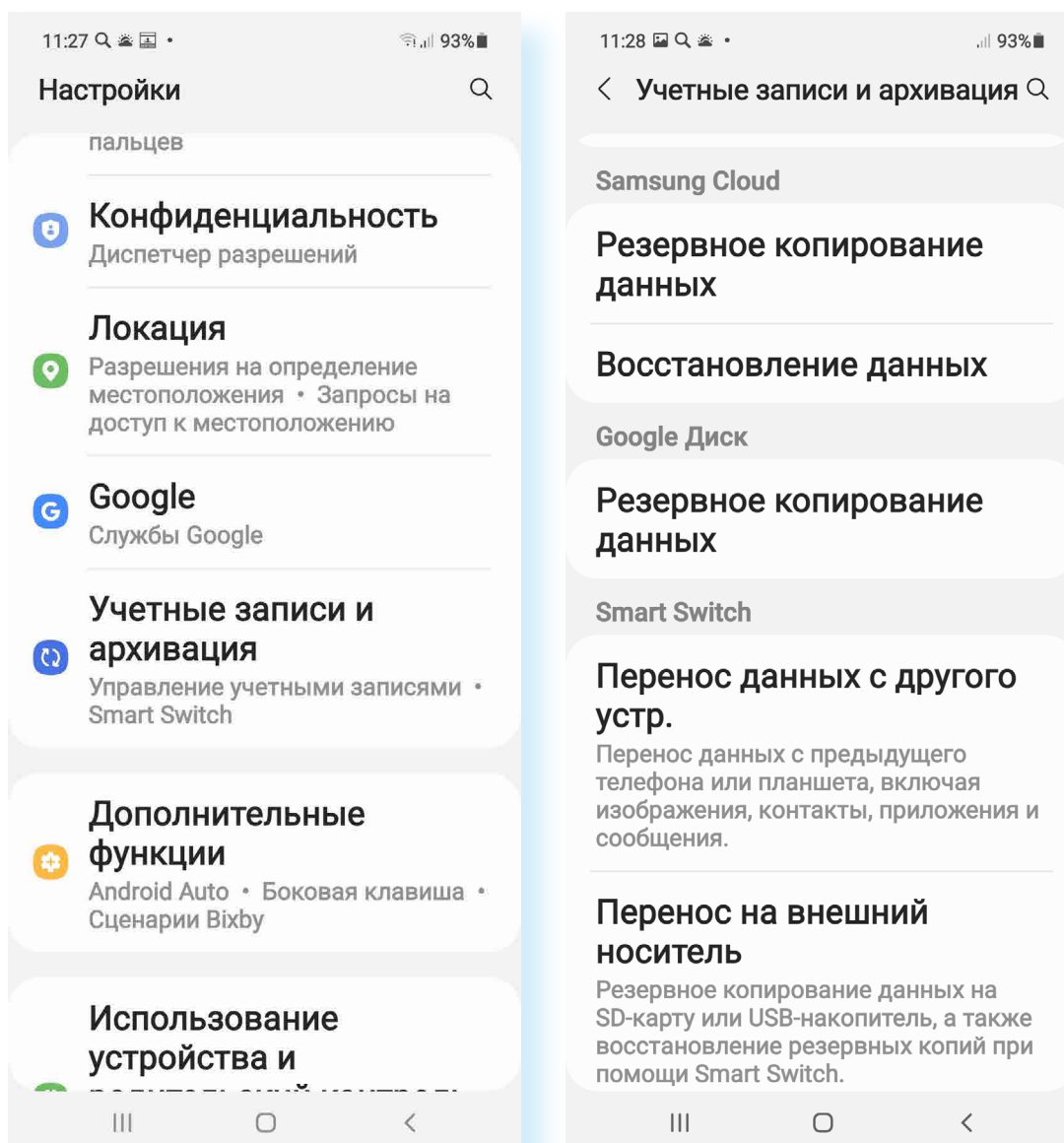
Принцип такой же: создаете резервную копию, а затем удаляете всю информацию с устройства. Именно на мобильных устройствах это нужно сделать обязательно. На смартфоне, как правило, установлены разные приложения – личные кабинеты в банках, социальных сетях, госуслугах и прочее. Бывают случаи, что, отдавая смартфон в ремонт, обратно пользователь получает телефон с основательно подчищенными банковскими счетами и, возможно, даже с новыми кредитами, оформленными онлайн от вашего имени. А если еще в смартфоне активирован и бесконтактный модуль оплаты и система финансовых расчетов (Pay Pal (Пэй Пэл), Samsung Pay (Самсунг Пэй), Apple Pay (Эппл Пэй), Google Pay (Гугл Пэй)), риски попасть в неприятную ситуацию увеличиваются.


Подробнее о системе финансовых расчетов в главе 5 «Финансовые расчеты через приложения» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета»

Чтобы сделать резервную копию на смартфоне:

- откройте приложение «Настройки»;
- перейдите в раздел «Учетные записи и архивация» (на различных моделях смартфонов раздел может иметь другие названия);
- далее нужно выбрать, куда поместить резервную копию. В нашем варианте предлагаются облачные хранилища Samsung Cloud и Google Диск или перенос информации на внешний носитель [6.8](#).

6.8

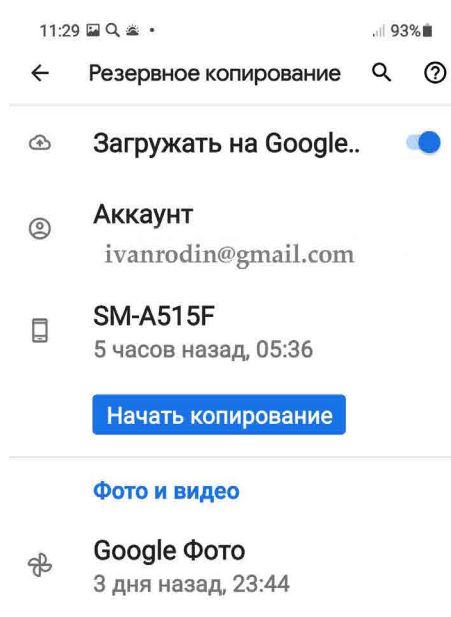


В том случае, если вы приняли решение сделать резервную копию на внешнем накопителе (флешке), ее нужно будет подключить к устройству. 

Обычно смартфоны с операционной системой Андроид привязаны к Google Диску, поэтому резервное копирование можно сделать в это облачное хранилище. Нажмите в блоке Google Диск пункт «Резервное копирование данных». Здесь обозначен ваш аккаунт на Google (адрес электронной почты), логин и пароль от которого также будут являться данными для входа в облачное хранилище Google Диск.

Для того, чтобы создать резервную копию, нужно нажать «Начать копирование» [6.9](#).

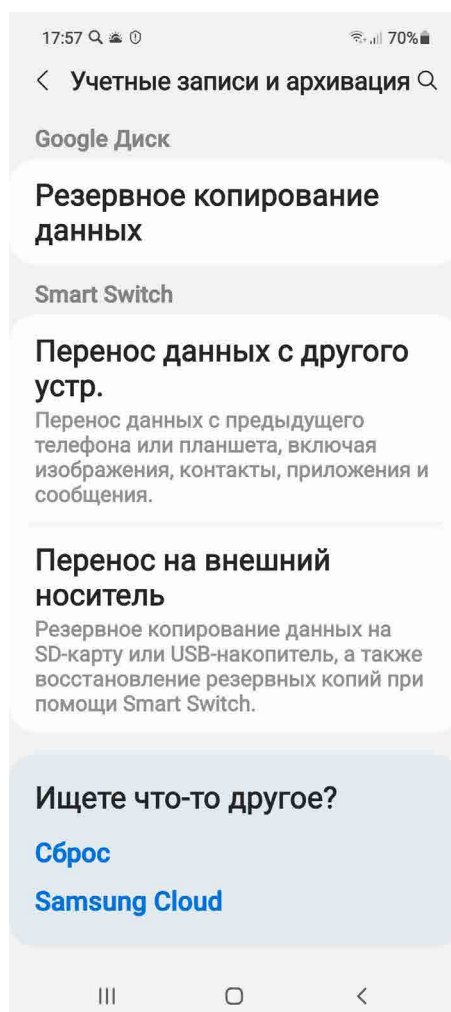
6.9



Это займет какое-то время. Дождитесь завершения процесса.

После этого можно провести сброс всех параметров. Перейдите в «Настройки», в раздел «Учетные записи и архивация». Внизу найдите пункт «Сброс» 6.10.

6.10



Далее нужно выбрать «Сброс всех параметров» или «Сброс данных».

На следующей странице можно посмотреть, какие данные будут стерты, и нажать команду на сброс всех настроек.

Чтобы затем восстановить данные на устройстве, при авторизации нужно ввести логин и пароль вашей учетной записи, в которой вы проводили резервное копирование данных.

В целом функция резервного копирования данных будет полезна не только при ремонте, а еще, например, в случае потери устройства. Зайдя в аккаунт Google, можно удаленно стереть данные с потерянного устройства и восстановить все данные на новом смартфоне.

Что делать, если взломали ваш аккаунт

Сегодня почти у каждого человека есть аккаунты в социальных сетях, зарегистрированы электронные почтовые ящики, есть личные кабинеты в интернет-магазинах. И, как следствие, есть вероятность, что вашу почту или аккаунт в социальных сетях взломают. Как понять, что это случилось? Например, вы не можете войти в свою учетную запись, потому что изменился пароль.

Главное в этой ситуации оценить, какие данные могут попасть в руки мошенников и постараться минимизировать потери. Безусловно, нужно предупредить друзей и знакомых, что у вас взломали почту или страничку в соцсети, и что не нужно отвечать на письма и сообщения, которые могут в этот момент приходить якобы от вас.

Обязательно нужно постараться восстановить контроль над учетной записью.

Первым делом попробуйте воспользоваться сервисом восстановления пароля. Есть шанс, что мошенники не успели отвязать от аккаунта вашу почту или номер мобильного телефона.

Если не получается это сделать, обратитесь в службу поддержки, разъясните ситуацию.

Если мошенники смогли добраться до аккаунта в какой-то платежной системе или интернет-банкинге, звоните в банк и просите заблокировать вашу карту или аккаунт.

Если взломали электронный почтовый адрес, постарайтесь вспомнить, где еще вы его вводили для регистрации, ведь ссылки для восстановления пароля на таких сервисах будут приходить именно на эту почту. Зайдите во все сервисы и постарайтесь изменить электронную почту или отвязать от учетной записи взломанный адрес.

Поменяйте пароли в тех сервисах, где вы использовали тот же пароль, что и от взломанного аккаунта. А еще лучше сразу настройте двухфакторную аутентификацию – подтверждение входа в учетную запись двумя разными способами (например, ввод логина и пароля и кода проверки, который приходит на мобильный телефон или электронную почту).

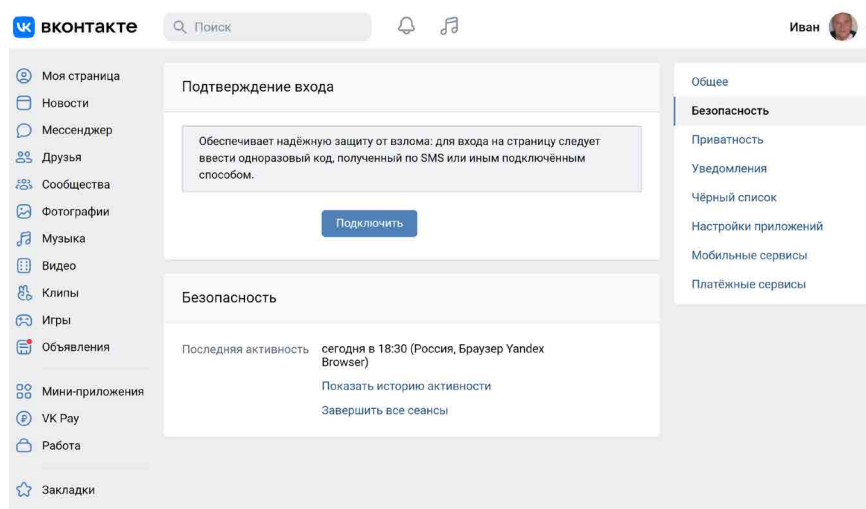
Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность» расширенного курса «Азбука интернета»

Если вам удалось восстановить доступ к взломанному аккаунту, сразу поменяйте пароль, ответьте на контрольные вопросы и настройте двухфакторную аутентификацию. Например, вот так выглядит страница настройки дополнительной защиты аккаунта в ВКонтакте 6.11.

6.11

Для того, чтобы настроить доступ к взломанному аккаунту в соцсети, нужно:

1. Нажать на значок профиля вверху справа.
2. В открывшемся меню зайти в «Настройки».
3. Выбрать справа «Безопасность».
4. Следовать инструкции на экране.



Если настроить ее, то при каждом входе в профиль на ваш мобильный телефон, связанный с учетной записью в ВКонтакте, будет приходить СМС с кодом. Только после ввода данного кода вы сможете войти на свою страницу.

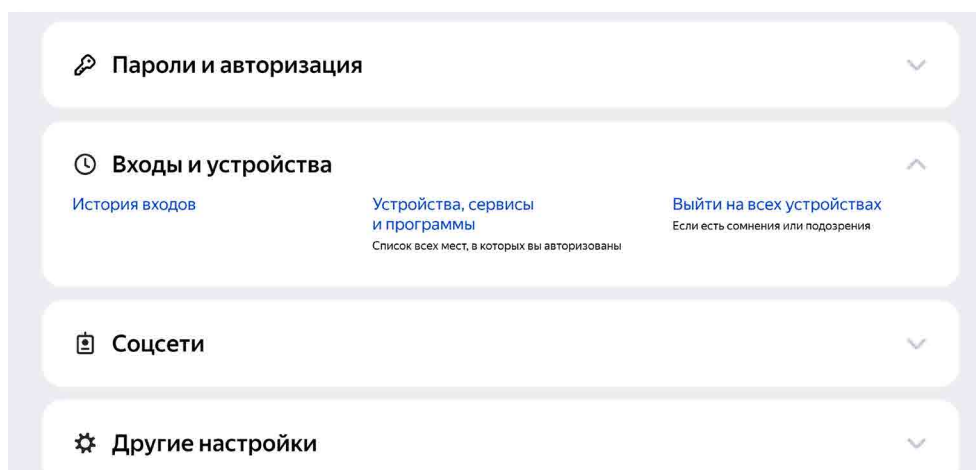
Чтобы настроить данную опцию в соцсети, нужно:

1. Нажать на значок профиля вверху справа.
2. В открывшемся меню зайти в «Настройки».
3. Выбрать справа «Безопасность».
4. Следовать инструкции на экране.

Многие сервисы информируют о подозрительной активности в вашем аккаунте. Если вы увидели такое письмо, никогда не переходите по указанной в нем ссылке. Это может быть и письмо от мошенников. Зайдите в аккаунт, набрав адрес в строке браузера, и, как минимум, поменяйте пароль и настройте сервисы безопасности. Также можете проверить историю входов. Такую функцию предоставляют сегодня многие порталы. Если увидите, что в ваш аккаунт зашли с незнакомого устройства, нажмите команду «Выйти из всех устройств».

Например, в Яндексе, чтобы увидеть историю входов, нужно зайти в «Настройки», затем выбрать «Управление аккаунтом» и далее нужно выбрать пункт «Входы и устройства» 6.12.

6.12



Бывают случаи, когда вам приходит сообщение от мошенников, в котором они сообщают, что заразили ваш компьютер вирусом и полностью отслеживают все ваши перемещения, более того, записали на веб-камеру компромат или скопировали переписку и, угрожая опубликовать данные, требуют выкуп.

Скорее всего, никто ничего не взламывал, а это просто вымогатели рассылают письма всем подряд из какой-нибудь купленной базы адресов. Нужно проверить компьютер на вирусы любой антивирусной программой-сканером. Проверку на вирусы часто предлагают установить бесплатно. На всякий случай поменяйте пароль доступа к электронной почте и включите двухфакторную аутентификацию.

Контрольные вопросы

1. Что нужно учесть при необходимости сдать компьютерное устройство в ремонт?
2. Как работает сервис шифрования жесткого диска?
3. Можно ли зашифровать диск в Windows?
4. Как вручную можно почистить компьютер?
5. Зачем нужна система резервного копирования?
6. Где могут храниться резервные копии информации с устройства?
7. Как на мобильном телефоне сделать резервную копию устройства?
8. Что делать, если ваш аккаунт взломали?



Безопасность мобильного устройства

7 ГЛАВА

Особенность мобильных гаджетов с точки зрения киберугроз

Количество пользователей смартфонов и планшетов растет с каждым годом. Растет и число вредоносных программ, разработанных для мобильных устройств. Разработчики антивирусов Zimperium Labs в начале 2015 года подсчитали, что 95% устройств Android можно взломать с помощью простого текстового сообщения.

Какие зловерные программы создаются для мобильных устройств?

1. Для сбора логинов и паролей, которые используются для входа в банковские системы.
2. Программы-вымогатели, которые блокируют доступ к важным файлам, к фото и видео пользователя.
3. Рекламные программы, которые также занимаются сбором информации о вас и передают ее третьим лицам. Главная цель – показать вам баннер, который бы заставил принять рекламное предложение. Особенно распространено так называемое сталкерское программное обеспечение. Оно легально, но также занимается наблюдением за пользователем и сбором личных сведений.
4. СМС-троянцы, которые отправляют с вашего номера сообщения на платные номера.
5. Вирусы, которые действуют через специальные программы для людей с ограниченными возможностями.

Постоянно появляются новые и новые варианты программ, которые ставят под угрозу безопасность ваших данных на мобильном телефоне или планшете.

К тому же есть риск потерять смартфон или планшет, или устройства могут украсть, а с ними пропадут и все ваши данные.

Конечно, сегодня можно настроить удаленное управление мобильным устройством и так же удаленно стереть с него данные.

Подробнее об управлении мобильным устройством через Google-аккаунт в главе 3 «Основы работы с приложениями. Настройки» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета».

Как действуют вирусные программы на мобильных устройствах:

1. Собирают данные ваших логинов и паролей.
2. Блокируют доступ к личным данным с целью вымогательства.
3. Собирают о вас информацию для маркетологов и рекламистов.
4. Удаленно управляют вашими учетными записями.
5. Отправляют сообщения на номера телефонов с оплатой за счет отправителя.

Основные рекомендации для безопасной работы на мобильном устройстве

Чтобы максимально обезопасить себя, будьте внимательны, когда используете мобильное устройство:

- не скачивайте программы и приложения с подозрительных сайтов в интернете;
- не подключайте в телефоне функцию бесконтактных платежей: это удобно, но менее безопасно;
- не сохраняйте данные банковской карты ни в аккаунте смартфона, ни в браузере;
- правильно настраивайте доступ приложений к другим вашим данным. Они должны быть логичными. Понятно, почему Вайбер запрашивает доступ к контактам, но если такое же разрешение просит приложение Лупа или Фонарик – это, как минимум, странно. Удаляйте такие приложения;
- после работы на мобильном устройстве всегда выключайте его, блокируйте экран доступа, ведь иногда мошеннику достаточно тридцати секунд, чтобы получить доступ к вашим данным;
- не переходите по ссылкам, присланным в сообщениях в мессенджерах или социальных сетях и электронной почте незнакомцами;
- проверьте настройки конфиденциальности и безопасности в приложении-браузере и аккаунте, который привязан к мобильному устройству. Обязательно поставьте запрет на скачивание приложений из неизвестных источников;

Подробнее о настройках безопасности в главе 3 «Основы работы с приложениями. Настройки» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета»

- отключайте Bluetooth и Wi-Fi, если вы ими не пользуетесь;
- не заходите в личные аккаунты и не проводите платежи в общественных сетях Wi-Fi;
- установите антивирус на мобильный телефон. При этом убедитесь, что в него встроена услуга на случай кражи устройства (возможность управлять удаленно);
- настройте блокировку экрана, желательно используя биометрические данные;
- для защиты приложений можно использовать программы-защитники данных. Например, App Lock (можно скачать из магазина приложений), или встроенную в смартфоны Samsung папку Кнох. Принцип работы один. Это приложение, куда вы можете перенести файлы с ценной информацией, а также другие важные приложения, например, банковское. Доступ будет под паролем. Это практически так же, как если бы вы в большой сейф спрятали еще один маленький сейф с важными документами.

Биометрия для телефона

Блокировка экрана – одна из самых важных функций для безопасности вашего смартфона. Суть в том, что, если вы где-то оставили свое устройство, никто из посторонних не сможет получить доступ к вашей информации. Если для того, чтобы перейти к приложениям, достаточно просто провести по экрану пальцем, это значит, что у вас нет защиты. Обязательно установите ее. Это могут быть биометрические данные, графический ключ или пароль.

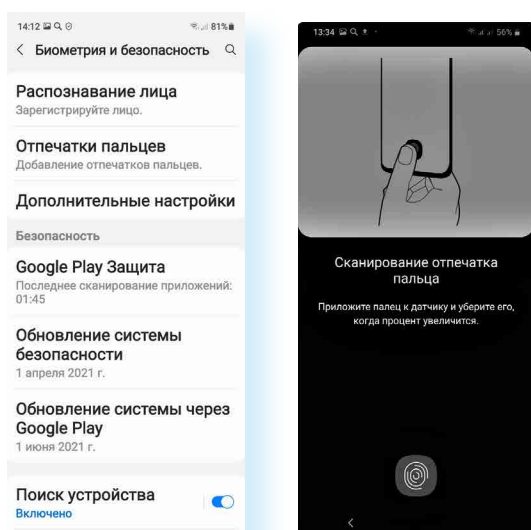
Подробнее об установке пароля на экран блокировки в главе 3 «Начало работы на планшетном компьютере» модуля 6 «Основы работы на планшетном компьютере» расширенного курса «Азбука интернета»

Специалисты считают, что одна из самых надежных технологий – использование биометрических данных. В современных смартфонах есть возможность настроить вход по отпечатку пальца (Touch ID – Тач Ай Ди) или по распознаванию вашего лица (Face ID – Фэйс Ай Ди). Наиболее удобный способ – отпечаток пальца.

Для того, чтобы настроить блокировку экрана по биометрическим данным:

- перейдите в раздел «Настройки»;
- выберите пункт «Биометрия и безопасность» (название опции может отличаться на разных устройствах);
- определите, какой тип биометрии вам подойдет (распознавание лица или отпечаток пальца).

Например, вы выберете «Отпечатки пальцев». Далее вам потребуется ввести графический код разблокировки или пароль. Дело в том, что будут работать два варианта разблокировки экрана. Если по каким-то причинам у вас не получается войти по отпечатку пальца, вы сможете получить доступ к смартфону другим способом – путем ввода пароля или графического ключа. Далее вас попросят приложить палец, которым вы будете делать разблокировку смартфона, к сканеру. На экране будет отмечено это место [71](#).



Для настройки экрана блокировки с использованием биометрии:

1. Перейдите в раздел «Настройки».
2. Выберите пункт «Биометрия и безопасность» (название опции может отличаться на разных устройствах).
3. Определите, какой тип биометрии вам подойдет.
4. Следуйте инструкциям для полной настройки.

71

(Есть модели, где для сканирования отпечатка необходимо приложить палец к фронтальной камере или к кнопке навигации. Внимательно читайте инструкции на экране). После того, как будет создан отпечаток вашего пальца, завершите настройку. Теперь, чтобы разблокировать смартфон, вам нужно будет приложить палец к обозначенному внизу экрана сканеру.

Обратите внимание, что теперь вы сможете использовать вход по отпечатку пальца и в другие приложения, установленные на смартфоне. Например, на портал «Госуслуг», в онлайн-банк, в личный кабинет «Ростелекома». Данную функцию нужно включить в настройках приложения.

Работа в публичных точках доступа Wi-Fi

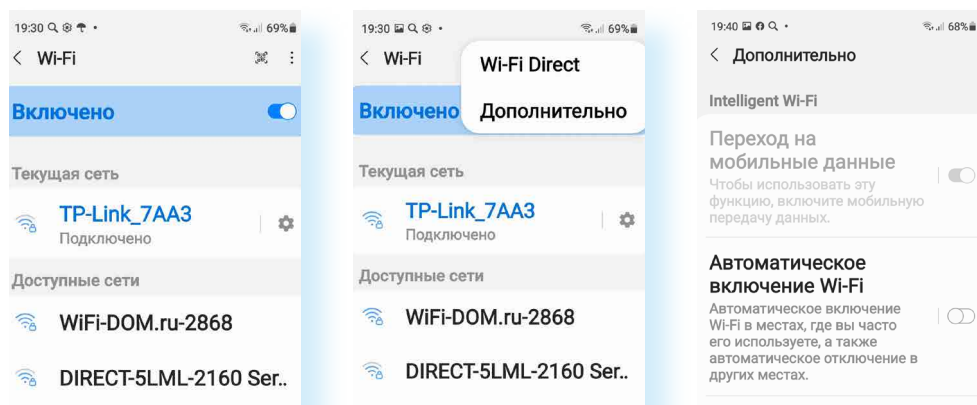
В ходе недавнего опроса 70% владельцев планшетов и 53% владельцев смартфонов и мобильных телефонов заявили, что они используют общедоступные точки доступа Wi-Fi. Такую информацию приводит «Лаборатория Касперского». Можно считать, что более половины владельцев мобильных устройств фактически отдают свои личные данные в руки мошенников.

Мы уже выясняли, что с помощью трекеров (программ, которые собирают данные для маркетологов и рекламщиков) в общедоступной сети Wi-Fi очень просто отследить ваши перемещения. Не удивляйтесь, если в продуктовом магазине, в торговом центре вам вдруг пришло сообщение о низкой цене на какие-то продукты. Скорее всего, ваш смартфон настроен так, что автоматически ищет и подключается ко всем общедоступным Wi-Fi сетям. Лучше отключить эту функцию.

Для этого:

- перейдите в «Настройки»;
- зайдите в раздел «Подключения»;
- нажмите на строку Wi-Fi;
- затем сверху зайдите в настройки Wi-Fi (это три точки, расположенные вертикально);
- в блоке «Автоматическое включение Wi-Fi» передвиньте ползунок влево (положение «Выключено») 7.2;

7.2



- в блоке «Hotspot 2.0» (подключение к другим устройствам, раздающим интернет) также поставьте ползунок в положение «Выключено».

Названные выше разделы «Настроек» могут отличаться в зависимости от модели и версии операционной системы.



Если вам срочно понадобилось выйти в интернет, то используйте интернет мобильного оператора, либо выходите в интернет через VPN. Это безопаснее, чем подключаться к общественным Wi-Fi сетям.

Работа в Bluetooth

Многие гаджеты сегодня работают по **Bluetooth**(Блютуз)-соединению. Это формат беспроводного соединения между компьютерными устройствами и различными электронными гаджетами. Как правило, оно работает на расстоянии от 10 до 100 метров.

Подробнее о Bluetooth-подключении в главе 3 «Начало работы на планшетном компьютере» модуля 6 «Основы работы на планшетном компьютере» расширенного курса «Азбука интернета»

По Блютуз подключаются беспроводные наушники, выносные акустические колонки, «умные вещи», смарт-часы, поэтому очень часто соединение Блютуз остается в мобильном устройстве активированным. Включенный Блютуз может стать для хакеров лазейкой к вашим данным. Это беспроводное соединение имеет слабый уровень защищенности. Взлом Блютуз позволит получить доступ к вашим контактам, личной почте, аккаунтам в социальных сетях и даже платежным данным. Данную технологию также используют для слежки за покупателем, изучения его предпочтений. Собранные данные передаются рекламщикам.

Поэтому отнеситесь внимательно к использованию такого соединения. Эксперты рекомендуют отключать Блютуз, когда вы его не используете.

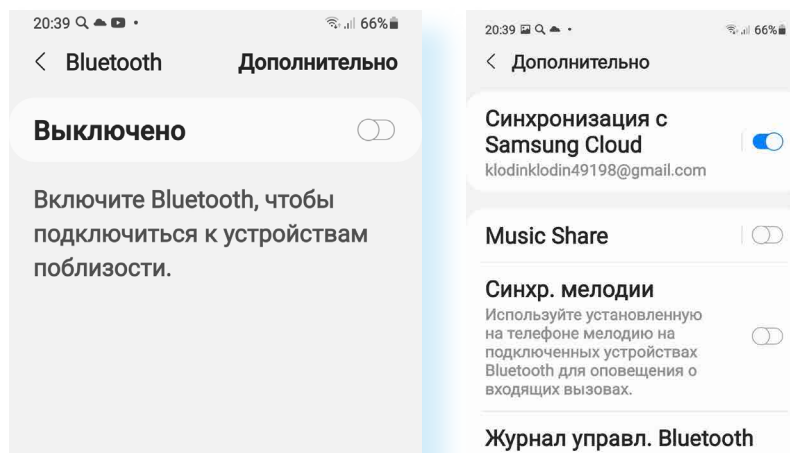
На мобильном устройстве практически нет настроек Блютуз, помогающих защитить соединение.

В телефонах Samsung появилась технология Music Share, которая позволяет делиться с друзьями музыкой объемом до 2 ГБ.

Желательно также отключить ее, если не используете:

- перейдите в «Настройки»;
- выберите «Подключения»;
- затем нажмите «Bluetooth»;
- вверху кликните «Дополнительно»;
- далее передвиньте ползунок в неактивное положение напротив надписи «Music Share» [7.3](#).

7.3



Феномен и риски селфи

Слово селфи («selfie») в 2012 году по версии журнала «Тайм» вошло в топ-10 самых модных словечек года. По сути **селфи** – это автопортрет, который делается с расстояния вытянутой руки.

Селфи – это удобно, потому что не нужно просить кого-то фотографировать себя в путешествии, и, с одной стороны, в этом нет ничего плохого. Это такой новый способ общения с внешним миром. Но психологи считают постоянное желание делать селфи новой формой психологической зависимости. При этом человек ждет позитивных отзывов, лайков, и, если этого не происходит, у автора паблика может даже возникнуть расстройство психики.

В погоне за яркими селфи и большим количеством лайков и комментариев пользователи (в основном молодые люди) делают такие автопортреты, рискуя жизнью.

Министерство внутренних дел России разработало специальную методичку «Безопасное селфи» 7.4.

7.4



Также ваше селфи – это говорящее фото. Можно увидеть, где и с кем вы находитесь, обстановку в вашем доме. Эта информация может быть полезна мошенникам, которые вполне могут уже иметь ваши личные данные, а по вашей ленте в соцсетях можно определить ваши маршруты и узнать о поездках.

Поэтому чрезмерно не увлекайтесь автопортретами на мобильный телефон, не рискуйте в погоне за суперселфи, и лучше всего выкладывайте свои фото несколько позже, чем была ситуация, запечатленная на селфи.

Чьи в семье сим-карты?

Симки для телефонов доступны всем, и очень часто их может быть у человека несколько. А еще бывает так, что номер телефона оформлен на одного человека, а пользуется им другой: родственник, супруг, ребенок или просто знакомый. Скажем, брали симку в салоне и забыли паспорт. Не возвращаться же. Попросили оформить своего друга, у которого паспорт при себе. Теперь номер ваш, но оформлен на другого. А это уже может привести к проблемам.

В России в 2018 году вступил в силу закон, по которому номером телефона должен пользоваться именно тот человек, на кого оформлен договор. Узнать, на вас ли оформлена сим-карта, можно в салоне связи, но нужно иметь в виду – если оператор узнает, что номером пользуется другой человек, будет 15 дней, чтобы предоставить свои данные, иначе номер будет заблокирован.

Что может сделать владелец сим-карты? Он может обратиться к сотовому оператору и расторгнуть договор. И вы рискуете оказаться без связи, возможно, не в самый подходящий момент.

А еще владелец номера может перевыпустить симку, и тогда звонки будут приходиться ему, а не вам. А это и информация о платежных операциях, уведомления с сайтов и приложений, где есть ваш личный кабинет. Вы не сможете восстановить пароли от ряда сервисов, где подтверждение о смене пароля проверяется кодом из смс. А между тем реальный владелец симки сможет узнать, какими сервисами вы пользуетесь, где совершаете покупки и на какие суммы.

Более того, он может забрать себе некоторые учетные записи, которые привязаны к номеру телефона. Например, ваши сообщения в мессенджерах. А вот получить доступ к вашему банковскому счету для владельца номера телефона будет сложнее. Ведь банки запрашивают дополнительные данные с клиента: номер карты или секретный вопрос.

Так что обязательно постарайтесь разобраться, чьими симками вы пользуетесь [7.5](#).



Затем нужно будет переоформить их на себя. Сделать это нужно вместе с владельцем номера. Понадобится заполнить заявление. Переоформить номер можно и в том случае, если человек, на которого оформлен номер, находится в другом городе. И даже если вы не знаете о его местонахождении, можно попробовать обратиться с заявлением к оператору сотовой связи. Есть шансы, что вашу просьбу удовлетворят.

Если люди находятся в разных городах, оператор может предложить обратиться в салон связи по месту жительства и составить заявление. Первым в любом случае должен обратиться текущий владелец номера, то есть тот, на кого оформлен договор.

Сим-карты часто продают с рук безо всякой регистрации. Это незаконная деятельность. За использование такой симки по закону взимается штраф до 2 тысяч рублей для физического лица. Такая симка может перестать работать в любой момент. Вы не сможете восстановить ее в салоне. Могут возникнуть проблемы с привязкой симки к банковскому счету. Бывает, что анонимные сим-карты продают мошенники. Они ждут, когда на номер будет положена определенная сумма денег и блокируют номер, перевыпустив симку. Но даже если это не мошенники, в любом случае у таких сим-карт уже есть владелец. Часто это юридическое лицо, фирма, которая якобы закупила симки для своих сотрудников.

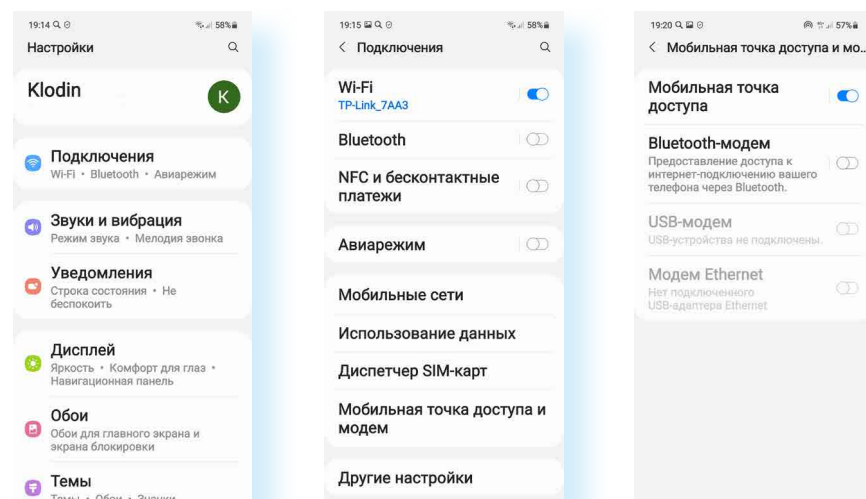
Безопасная работа смартфона в режиме «Точки доступа»

Каждый смартфон может работать как мобильный модем, ведь он выходит в интернет через сотовую связь и может делиться интернет-соединением с другими устройствами по Wi-Fi. Например, смартфон может быть точкой доступа в интернет для ноутбука или планшета.

Это полезная функция. Чтобы подключить ее, нужно:

1. Зайти в смартфоне в «Настройки».
2. Выбрать «Подключения».
3. Перейти в раздел «Мобильная точка доступа».
4. Передвинуть ползунок напротив надписи «Мобильная точка доступа» 7.6.

7.6



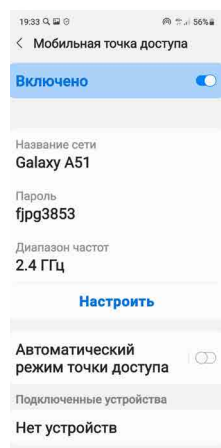
Вы включили передачу данных. Теперь другое устройство по Wi-Fi может подключиться к вашему смартфону и получить ваш доступ в интернет.

Конечно, это небезопасно. На что обратить внимание? Обязательно настраивайте раздачу по паролю. То есть, чтобы подключиться к вашему интернету на другом устройстве, нужно будет ввести пароль.

Если нет необходимости в раздаче интернет-соединения, отключайте данную опцию в смартфоне. Периодически проверяйте настройки вашей точки доступа на телефоне. Там вы сможете увидеть, сколько устройств используют ваше интернет-соединение.

Чтобы настроить точку доступа в смартфоне, нужно:

1. Зайти в «Настройки».
2. Перейти в раздел «Подключения».
3. Далее выбрать «Мобильная точка доступа и модем».
4. Нажать на надпись «Мобильная точка доступа».
5. Здесь вы увидите название сети, пароль к вашей точке доступа, а также подключившиеся к вам устройства **7.7**.



Чтобы подключить точку доступа, нужно:

1. Зайти в смартфоне в «Настройки».
2. Выбрать «Подключения».
3. Перейти в раздел «Мобильная точка доступа».
4. Передвинуть ползунок напротив надписи «Мобильная точка доступа».

7.7

Нажав «Настроить», вы сможете изменить пароль, название своего устройства. Также можно установить дополнительную защиту от чужих подключений, включив опцию «Защищенные кадры управления».

Контрольные вопросы

1. Каковы особенности мобильных телефонов с точки зрения кибербезопасности?
2. На какие правила безопасности стоит обращать внимание при работе на мобильных устройствах?
3. Почему опасно работать в личных кабинетах приложений и проводить платежи со смартфона, подключившись к общественным сетям Wi-Fi?
4. Почему Bluetooth после использования нужно отключать?
5. Почему важно настроить экран блокировки на мобильном устройстве?
6. Чем могут быть опасны селфи?
7. Почему важно оформлять свои сим-карты на себя?



Как защитить детей в интернете

8 ГЛАВА

Смартфон для ребенка. Настройки

Конечно, в покупке смартфона детям есть и плюсы, и минусы. С одной стороны, ребенок всегда на связи, с другой – злоупотребление гаджетами может влиять и на психическое, и на физическое развитие. Ребенка необходимо научить им пользоваться без вреда для него.

Каким должен быть смартфон?

Самое простое решение – отдать старый мамин, папин или бабушкин. Это хороший вариант, если это не модель, где операционная система устарела и уже не может обновляться. Это значит, что есть проблемы с системой безопасности.

Желательно, чтобы экран был большой, и ребенок не портил глаза. Обязательно купите ударопрочный чехол и приклейте на экран противоударные пленку или стекло. Смартфон точно десятки раз будет падать.

Кроме того, аккумулятор должен быть надежный и большого объема, иначе ребенок будет постоянно без связи, потому что смартфон опять разрядился. Желательно взять устройство со слотом для карты памяти. Это в какой-то степени компенсирует небольшой объем оперативной памяти в смартфоне.

Стоит проверить и модуль GPS, который отвечает за определение местоположения. Это очень нужная функция, которая вам точно понадобится. Посмотрите отзывы о модели именно по этому параметру.

Перед тем, как отдать телефон ребенку, его нужно настроить. Понадобится учетная запись. Самостоятельный аккаунт можно заводить только с 13 лет. Для младших детей, чтобы зарегистрироваться, нужно подтверждение с аккаунта родителя.

Сообщать пароль от учетной записи ребенку не обязательно. Сразу включите двухфакторную аутентификацию, привязав ее к своему номеру телефона или к электронной почте.

Что должно быть в смартфоне ребенка?

1. Актуальная операционная система с современными настройками безопасности.
2. Надежный и большой объем аккумуляторной батареи.
3. Средний или большой экран.
4. Противоударный чехол и защитные стекло или пленка на экране.

Безусловно, не нужно указывать никакой платежной информации. Также стоит сразу отключить приложение Gmail. Для этого нужно перейти в «Настройки», далее в «Приложения», далее «Gmail». Выбрать «Выключить».

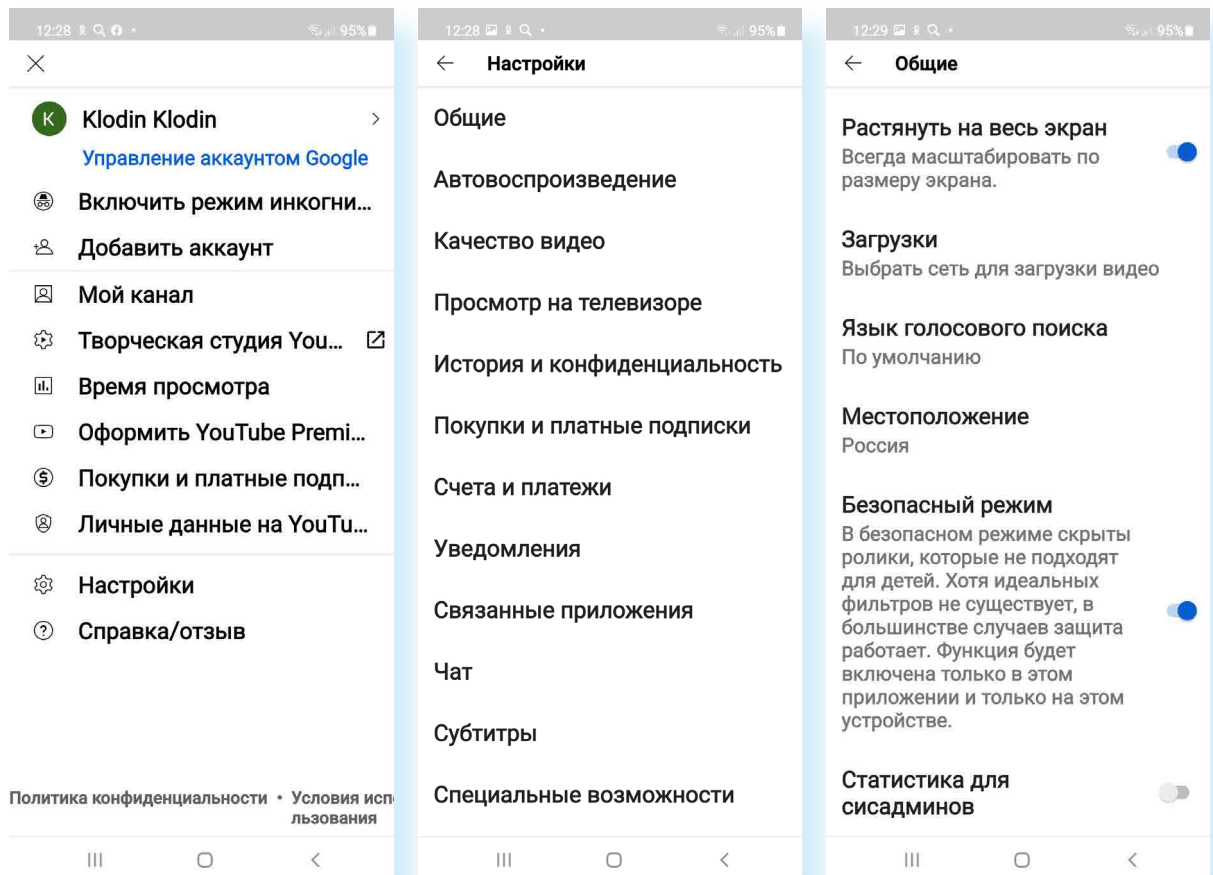
Отдельно посмотрите настройки приложения Youtube, браузера (оставьте одно приложение-браузер на телефоне).

Например, в приложении Youtube нужно перейти в профиль (он привязан к профилю в Google):

- выбрать «Настройки»;
- далее «Общие».

Здесь можно ограничить время просмотра сервиса и поставить напоминание о том, что уже пора ложиться спать. Также нужно активировать «Безопасный режим», передвинув ползунок вправо 8.1.

8.1



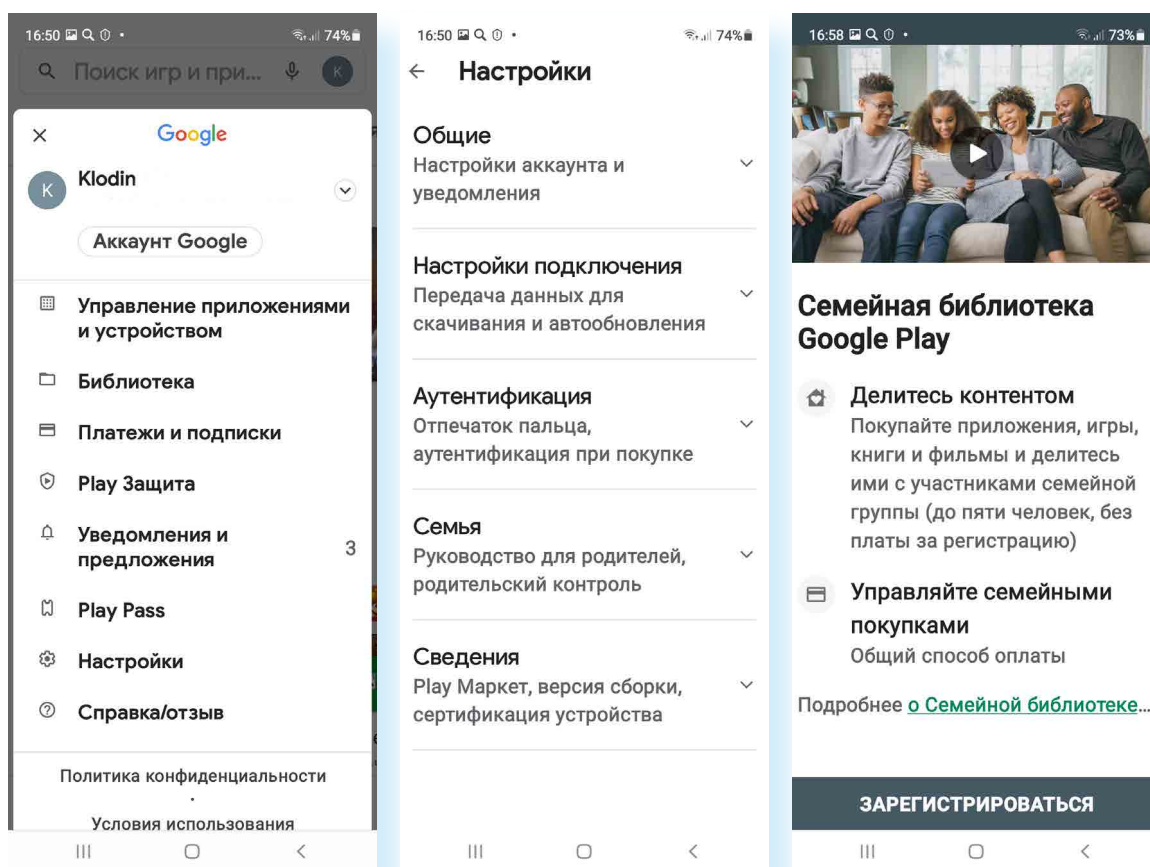
Установите антивирус на смартфон. Есть специальные программы, которые позволяют отслеживать онлайн-активность, публикации в социальных сетях, видеть местоположение ребенка и даже видеть уровень заряда аккумулятора у смартфона.

Также можно сразу установить детские приложения, чтобы ребенок не занимался их поисками самостоятельно. Это может быть Детский Youtube, детский плеер с музыкой, развивающие приложения для детей. В магазине приложений **Play Market** (Плей маркет) в строке поиска наберите запрос: «приложения для детей» и выберите подходящие.

Отдельный вопрос – покупки в интернете. Можно активировать семейную учетную запись Google. Это возможно, если взрослые в семье также используют операционную систему Андроид. Семейный аккаунт позволяет делать покупки на всех включенных в семейную группу устройствах с родительской карты, а также вместе пользоваться онлайн-покупками контента, приложений и т.д.

Чтобы настроить семейный доступ:

- зайдите в Google Play (Гугл Плей);
- вверху перейдите в аккаунт;
- выберите «Настройки»;
- далее нажмите пункт «Семья»;
- затем выберите «Создать Семейную библиотеку»;
- нажмите «Зарегистрироваться» 8.2;



8.2

- выберите «Продолжить»;
- снова «Продолжить»;
- на следующей странице «Настроить»;
- понадобится ввести данные платежной карты и подтвердить их;
- затем выберите, кого вы хотите добавить в семейную группу;
- разошлите им приглашение.

Пользователь, получивший приглашение (сообщение придет на электронную почту), должен перейти по ссылке, принять его и добавиться в группу. Одна из популярных опций для детского компьютера или гаджета – **родительский контроль**.

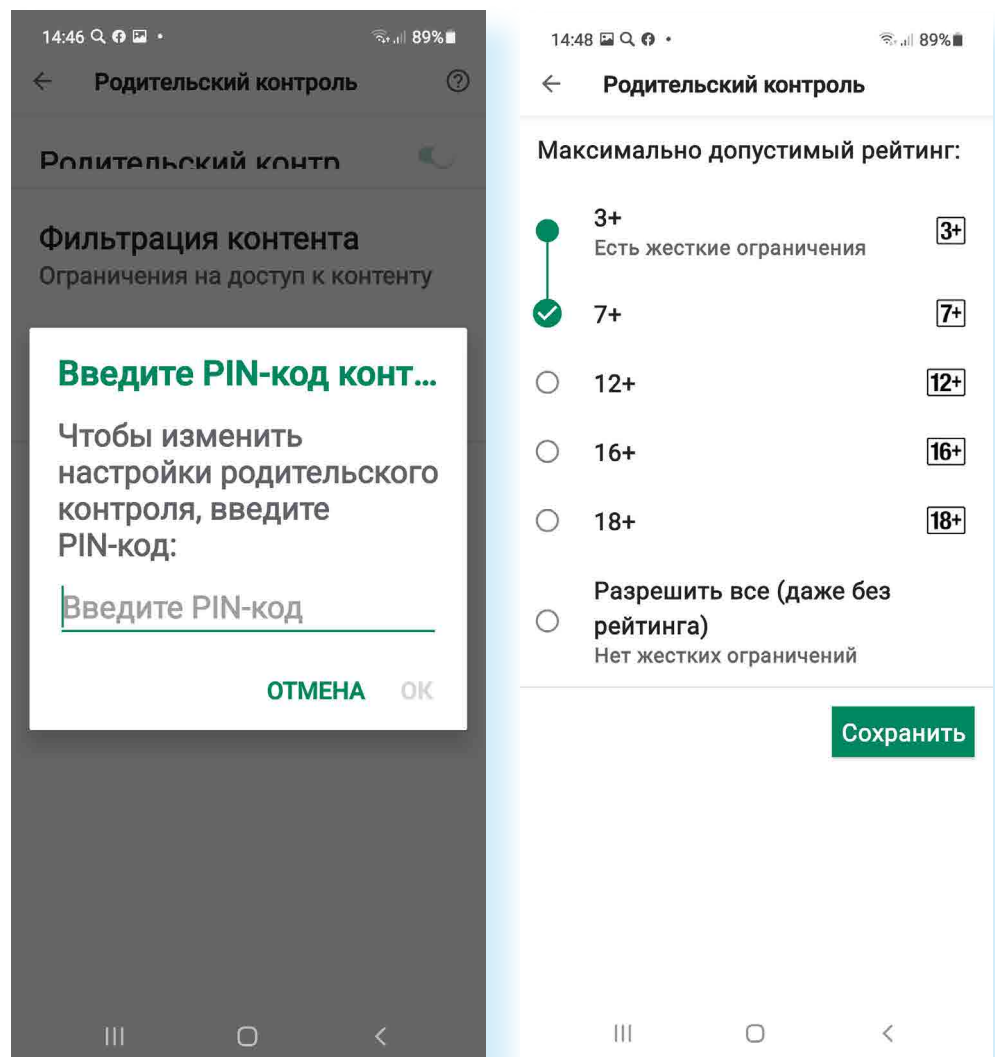
Настройте в магазине приложений ограничения для скачивания. Для этого:

- зайдите в Google Play (Гугл Плей);
- вверху перейдите в аккаунт;
- выберите «Настройки»;
- далее нажмите пункт «Семья»;
- перейдите в раздел «Родительский контроль»;
- включите его. Для этого нужно будет придумать и ввести пин-код;
- далее выберите ограничения по возрасту для скачивания игр, приложений и фильмов 8.3.

8.3

Как подготовить компьютер или мобильное устройство для ребенка:

1. Самим зарегистрировать учетную запись.
2. Активировать настройки безопасного поиска и просмотра в браузере и Youtube.
3. Включить функцию «Родительский контроль».
4. Установить антивирус.
5. Установить интересные и безопасные для детей приложения и программы.



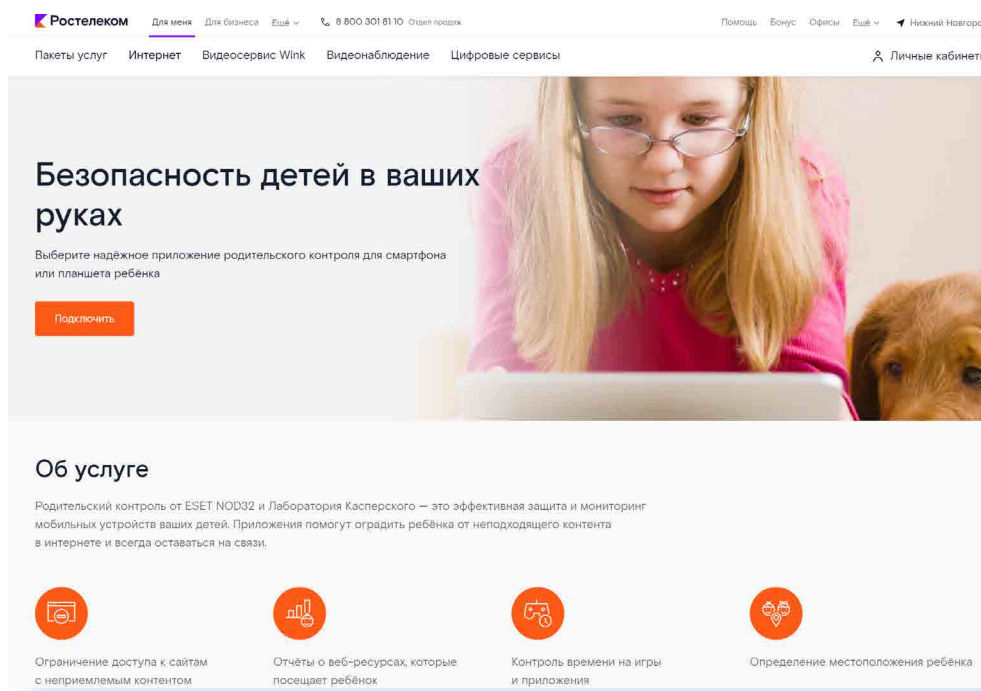
Опция «Родительский контроль»

Полезная услуга, которая помогает родителям защитить малышей от неприятностей в интернете. Ее предлагают многие разработчики. Есть варианты для компьютера, мобильного устройства и цифрового ТВ.

Родительский контроль от «Ростелекома»

Такую услугу, например, предоставляет «Ростелеком» 8.4.

8.4



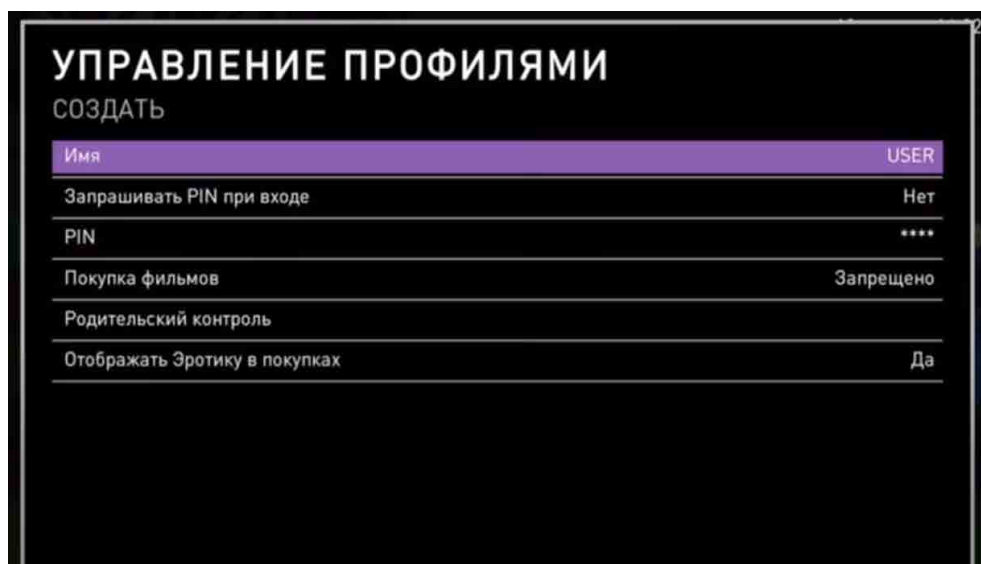
Он предлагает подписку на антивирусные программы для родителей Kaspersky Safe Kids или ESET NOD32 Parental Control. Услуга может быть подключена к нескольким устройствам.

Основные функции: ограничение доступа к нежелательным сайтам, отчеты о посещаемых ребенком интернет-ресурсах, контроль времени на игры, определение местоположения ребенка.

Родительский контроль для телевидения от «Ростелекома» также помогает ограничить доступ к нежелательным каналам. Для настройки нужно перейти в профиль «Настройки» в цифровой приставке:

- выбрать пункт «Родительский контроль»;
- кликнуть по строке «Управление профилями»;
- создать новый профиль пользователя или выбрать уже существующий из списка 8.5;

8.5



- выбрать строку «запрашивать PIN», и в открывшемся окне выбрать «Отмена пин-кода», чтобы при включении приставки система не запрашивала пароль;
- для блокировки ненужных телевизионных каналов впишите пароль в соответствующее поле. Таким образом, доступ на нежелательные каналы будет под паролем;
- установить галочку в поле напротив слова «Нет» в разделе «Отображать эротику в покупках». Это исключит возможность входа на каналы для взрослых;
- нажать «Сохранить». Для этого на пульте необходимо нажать кнопку «Назад» и ввести пароль. После того, как пароль будет введен и подтвержден, настройки начнут действовать.

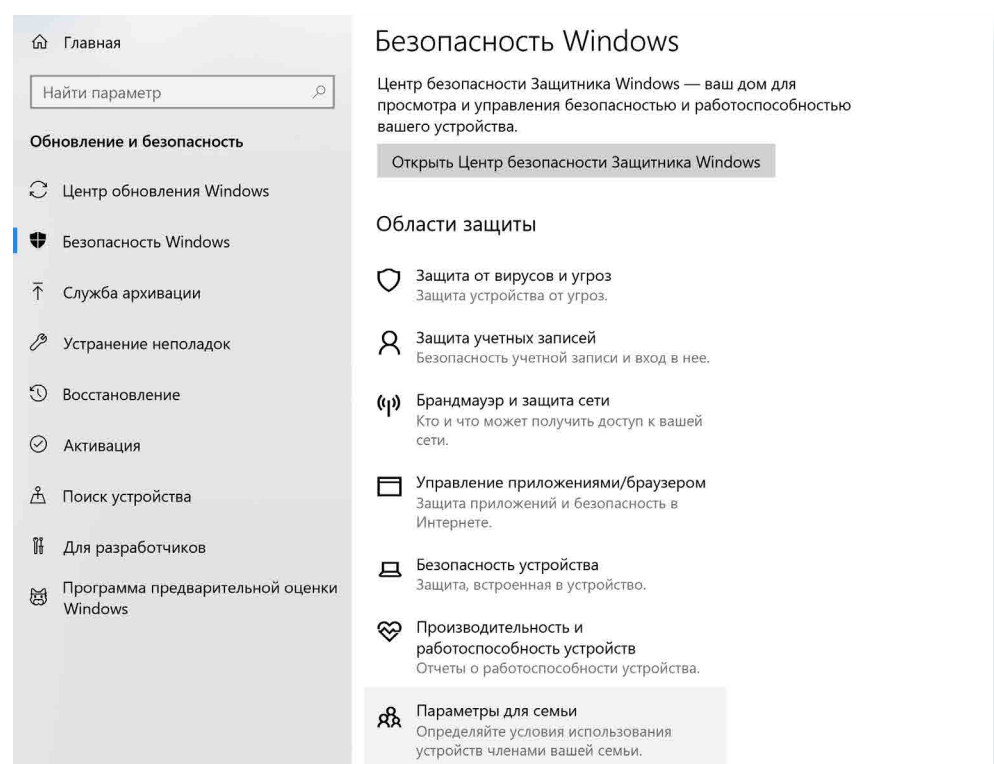
Родительский контроль в Windows

Опцию «Родительский контроль» предлагают и разработчики Windows. Здесь также используется принцип создания семейной группы. При этом у каждого члена семьи должна быть зарегистрирована учетная запись в Windows. Функционал родительского контроля осуществляется через приложение **Microsoft Family Safety** (Майкрософт Фэмили Сэфэти), который нужно будет скачать в магазине приложений.

Чтобы включить родительский контроль в Windows 10, нужно:

- нажать «Пуск»;
- перейти в «Параметры»;
- далее выбрать блок «Обновление и безопасность Windows»;
- в меню слева кликнуть строчку «Безопасность Windows»;
- перейти в пункт «Параметры для семьи» 8.6.

8.6



Опция «Родительский контроль» в Windows кроме стандартных параметров контроля также позволяет проверить устройства всех членов семьи.

Родительский контроль в Андроид

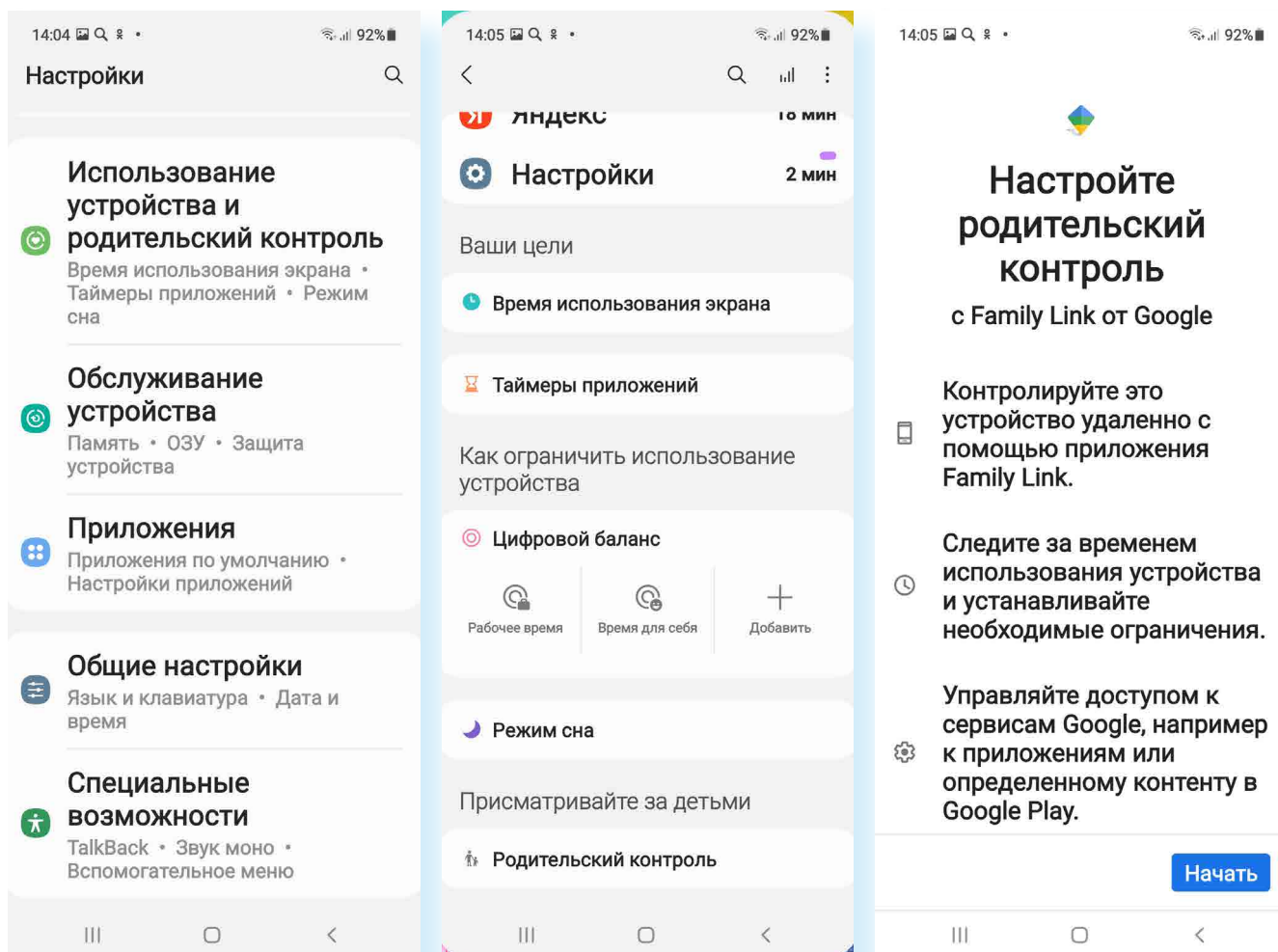
Чтобы активировать функцию на планшетах и смартфонах с операционной системой Андроид, нужно:

- перейти в «Настройки»;
- выбрать «Использование устройства и родительский контроль».

Здесь есть ряд функций и полезной информации. Например, всегда можно посмотреть, сколько часов в день используется телефон и в каких приложениях.

Нажмите на пункт «Родительский контроль». В Андроид функция работает через приложение **Family Link** (Фэмили Линк). Оно должно быть установлено и у ребенка, и у взрослого на телефоне. Чтобы начать процесс активации родительского контроля, нужно нажать «Начать» и далее следовать инструкциям на экране 8.7.

8.7



Одна из разновидностей родительского контроля – программы-трекеры, которые позволяют отслеживать перемещение ребенка и определять его местоположение.

Такие приложения есть, например, у многих сотовых операторов: «МТС Поиск», «Билайн.Локатор», «Локатор» от «Мегафона», «Геопоиск» от «Теле 2».

Пытаясь оградить ребенка от нежелательного контента или зависимости от гаджетов – не перестарайтесь. Ограничения программы «Родительский контроль» должны быть разумными. Больше общайтесь с детьми, проводите больше времени вместе, приобщайте ребенка к «живым играм», найдите совместное хобби. Это больше укрепит психическое здоровья ребенка, чем жесткие технические ограничения на гаджетах.

Телефон в школе

Задача взрослых объяснить, как использовать смартфон или планшет в школе. Здесь есть и плюсы, и минусы.

Смартфон, безусловно, удобен. Он позволяет быть на связи, быстро реагировать на какие-то внештатные ситуации с точки зрения обеспечения безопасности ребенка, школьникам помогает быстрее найти нужную информацию.

При этом нельзя использовать смартфон на уроках, желательно, чтобы у ребенка была не супермодная модель, которая может спровоцировать разного рода конфликты в классе. При этом смартфон иногда становится еще и инструментом для кибербуллинга (травли в интернете).

Конечно, все это нужно принимать во внимание. В детском телефоне для школы не рекомендуется устанавливать приложения для соцсетей, лучше, если будет использоваться один мессенджер. Не храните в смартфоне семейные фото, адреса, пароли. И предупредите ребенка, что в интернете не нужно размещать о себе лишнюю информацию.

Безусловно, поставить запрет можно на все. Но это будет не лучший выход. Задача взрослого – научить ребенка разбираться в качестве информации, соблюдать общие для всех правила использования гаджетов в школе.

Как противостоять кибербуллингу и онлайн-грумингу

Каждый человек может стать объектом травли и мошенничества в сети. Особенно дети.

Кибербуллинг – это шантаж или угрозы в интернете. Этим могут заниматься несколько человек. Часто поводом для травли становится какая-то личная информация, компрометирующие фото или видео. Как уберечь ребенка? Самое главное, чтобы вовремя пришла родительская поддержка. Общайтесь с детьми. Внимательно относитесь ко всем его рассказам, связанным с общением, новыми знакомствами, особенно в интернете, следите за изменением настроения ребенка. Решайте проблему вместе с ним. Будьте 100% на его стороне.

Что нужно и что не нужно делать:

- не нужно отвечать на агрессивные сообщения. Обидчики теряют интерес, если нет ответной реакции;
- занесите этих пользователей в черный список;
- обязательно свяжитесь с технической поддержкой социальной сети. Вам помогут заблокировать пользователя или же написать на него жалобу;
- делайте скриншоты переписки на случай, если вам придется отстаивать свои права в суде;
- если необходимо, обратитесь в правоохранительные органы.

Онлайн-груминг – это мошенничество, когда преступники обманном путем втираются в доверие к пользователям и пытаются выманить у них деньги за несуществующие товары, услуги или личные данные.

Часто для груминга используются взломанные аккаунты пользователей для рассылки сообщений по списку контактов. Поэтому, если ваш ребенок уже зарегистрировал аккаунт в социальных сетях, вместе с ним обсудите некоторые правила безопасности, чтобы он не попался на уловки мошенников.

Объясните ребенку, что стоит сделать:

- закрыть аккаунт от посторонних, а посты публиковать в режиме «для друзей»;
- ограничить контакты с незнакомыми людьми. Если кто-то из незнакомцев настаивает на встрече, нужно сообщить об этом взрослым. На такие встречи нельзя ходить в одиночестве.

Нельзя делать:

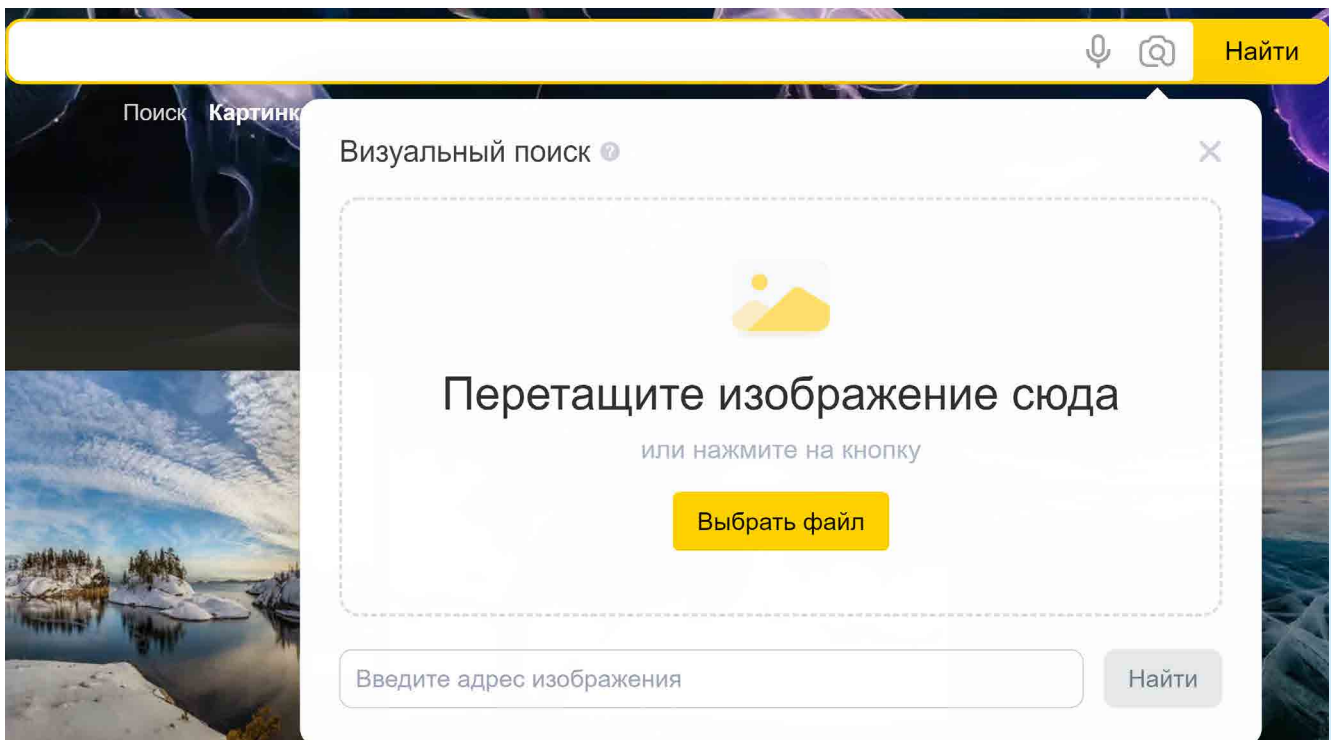
- публиковать в открытом доступе личные данные: адрес, имена и фамилии, номера телефонов, номера документов, банковских карт, билетов и так далее;
- переходить по подозрительным ссылкам, даже если он получил их по почте или в сообщении от знакомого пользователя;
- скачивать файлы на подозрительных или ненадежных сайтах;
- отправлять свои фото и видео незнакомцам.

Посоветуйте ребенку завести два адреса электронной почты: один для регистрации на различных сервисах, а второй для личной переписки.

Как оградить ребенка от деструктивных подростковых сообществ

До определенного возраста стоит контролировать виртуальную переписку своих детей и внуков. Обязательно смотрите, кто у ребенка в виртуальных друзьях, какие сообщества он посещает. Если что-то насторожило вас или непонятна символика группы, можно поискать ее в интернете с помощью сервисов поисковых сайтов Яндекс или Гугл «Поиска по картинкам» 8.8.

8.8



- возможно, стоит обратить внимание на сервисы, позволяющие искать скрытых или скрывающихся друзей;
- наблюдайте за поведением и настроением ребенка. Если что-то не так, вы сразу заметите. Это веский повод пообщаться «по душам»;
- используйте технические возможности контроля. Настраивайте «Родительский контроль». Есть подобные инструменты и для игровых приставок. Можно проверить временные файлы интернета, поинтересоваться, что смотрел ваш ребенок (например, папки `c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files` в операционной системе);
- проверьте настройки веб-камеры и убедитесь, что она отключена или закрыта, если в данный момент не используется;
- не создавайте для ребенка учетную запись с правами администратора. Настройте сами параметры конфиденциальности и безопасности в социальных сетях;
- объясните ребенку, что далеко не вся информация в интернете достойна доверия. А все, что попало в интернет, остается там навсегда. Об этом нельзя забывать, когда делаешь публикации.

Пароли и дети

Отдельный вопрос касается использования детских паролей.

С одной стороны, родители должны научить ребенка использовать надежные пароли, объяснить, что пароли нельзя передавать друзьям, знакомым, что к разным сервисам должны быть разные пароли, что хранить их можно в менеджере паролей и т.д.

С другой стороны, пароль для ребенка может быть способом закрыть информацию от родителей. Это уже скорее вопрос не технических правил, а психологии взаимоотношений. Между взрослыми и детьми должны складываться доверительные отношения. Постарайтесь понять и помочь вашему ребенку (или внуку) разобраться в сложном информационном мире.

Контрольные вопросы

1. На что обратить внимание при выборе смартфона для ребенка?
2. Какие настройки стоит сделать на смартфоне, прежде чем отдать его ребенку?
3. Что такое семейная библиотека?
4. Как воспользоваться сервисом «Родительский контроль»?
5. Как обезопасить ребенка от кибербуллинга и онлайн-груминга?
6. Как оградить ребенка от деструктивных подростковых сообществ?



azbukainterneta.ru
азбукаинтернета.рф