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.

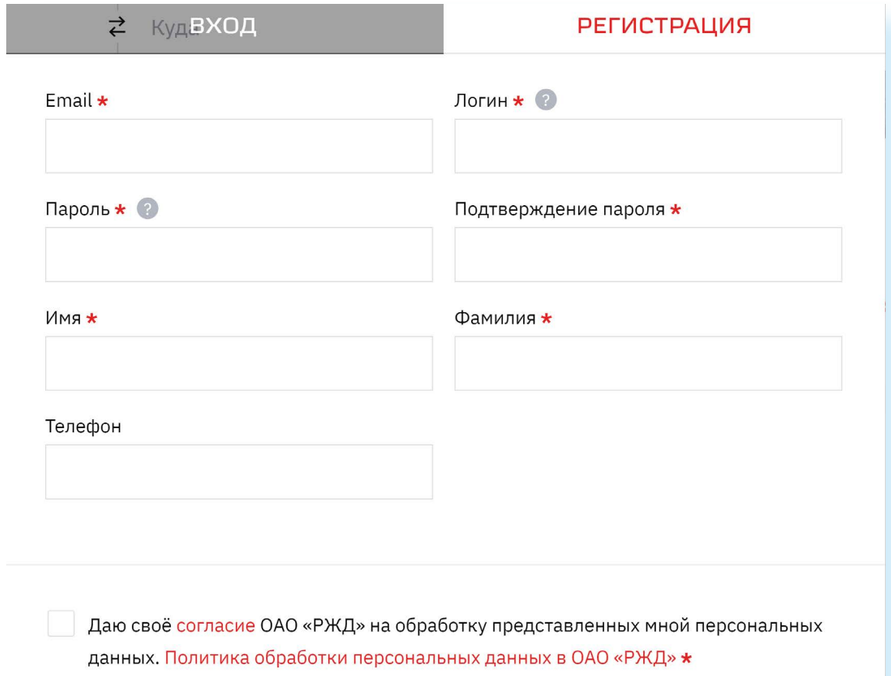
Пароли дают вам доступ к вашему счету в банке, к услугам государственных ведомств, электронной почте, к аккаунтам в социальных сетях, к интернет-магазинам. Уже в 2017 году у одного пользователя было в среднем порядка 191 регистраций в сети по логину и паролю. Это 191 пароль.

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



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.

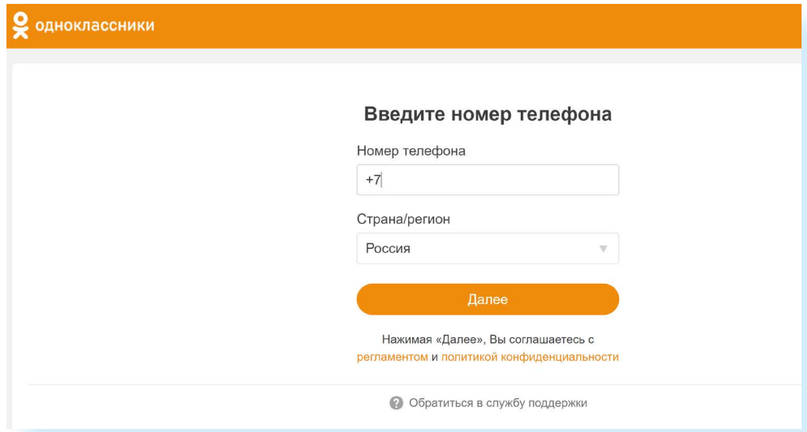
Обратите внимание, если при восстановлении пароля вам на почту высылается введенный некогда вами логин и пароль, значит, сайт хранит ваши данные в открытом виде. Рекомендуется такие сайты не посещать, не проводить на них каких-либо платежных операций и по возможности удалить свои данные с них.

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



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 киберебезопасности 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 провернуть 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.

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

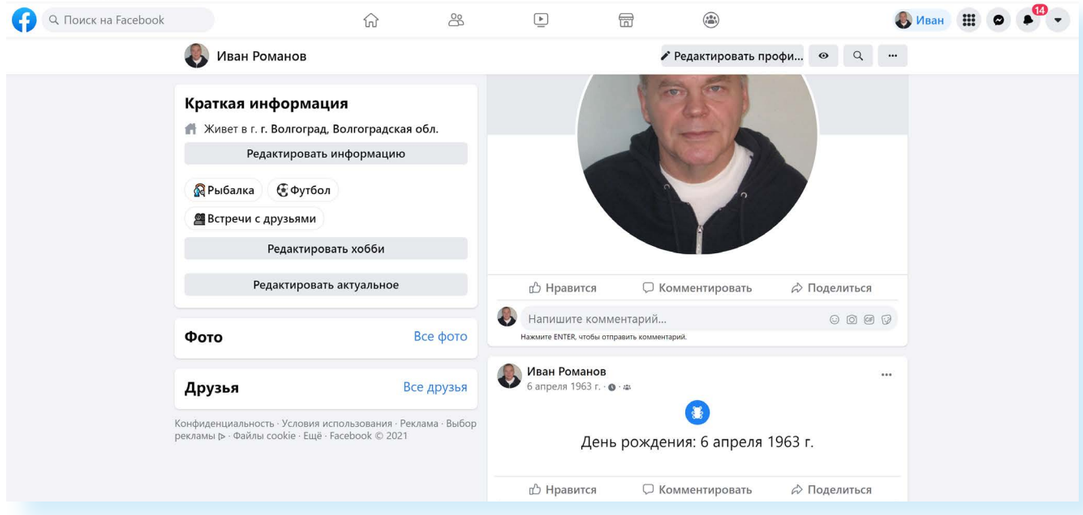
Как мошенники получают доступ к паролям:

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

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.

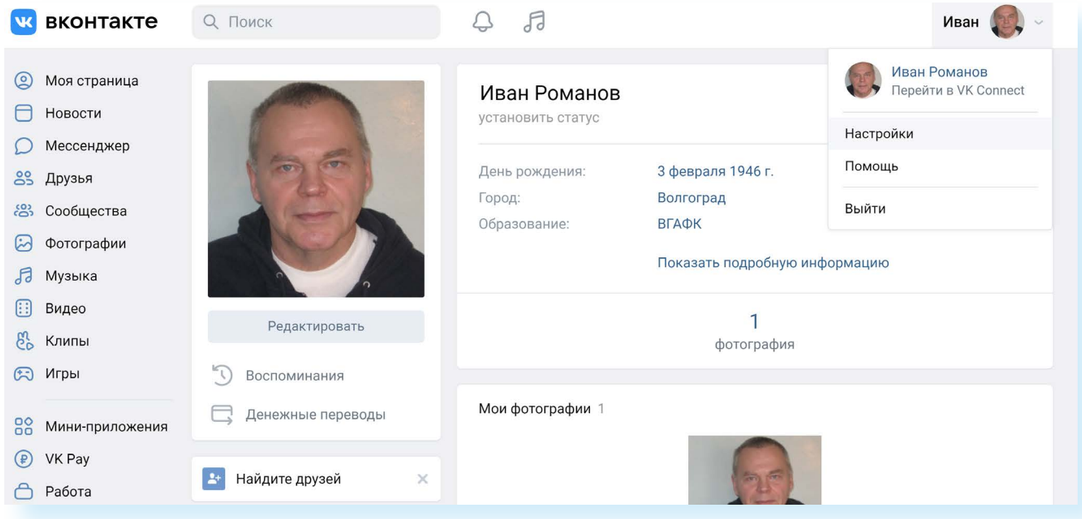
Доступ в банковские приложения часто осуществляется через систему двухфакторной аутентификации. Чтобы зайти в аккаунт, нужно ввести пароль и код, пришедший в смс.

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 в ВКонтакте, нужно:

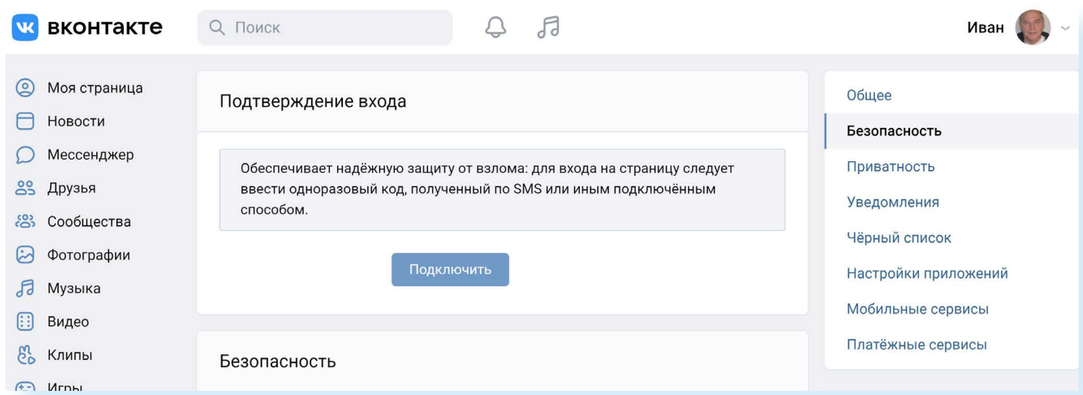
- нажать на значок профиля вверху справа;
- выбрать раздел «Настройки» 5.4;

5.4



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

5.5



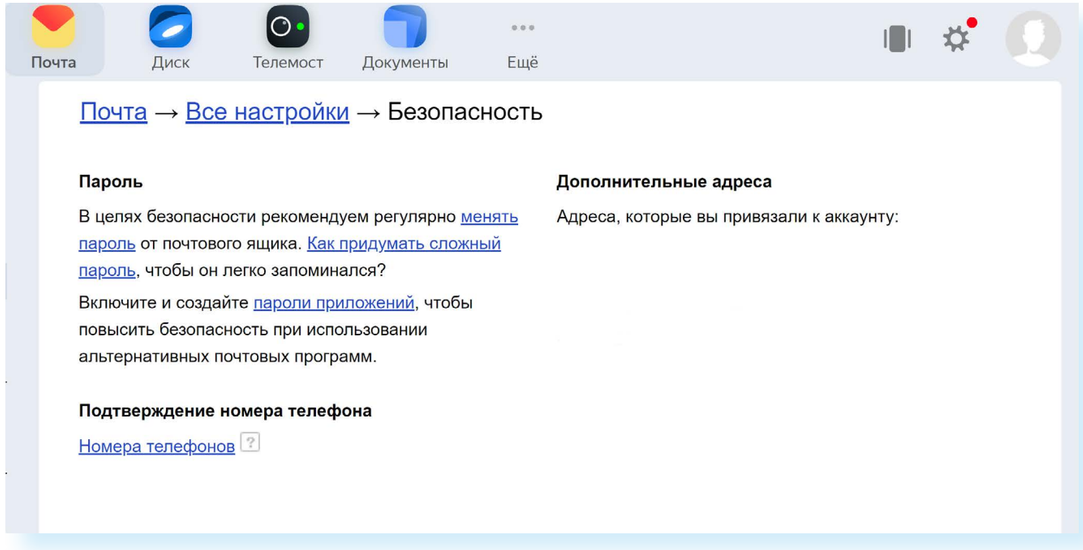
- и далее приступить к настройке.

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

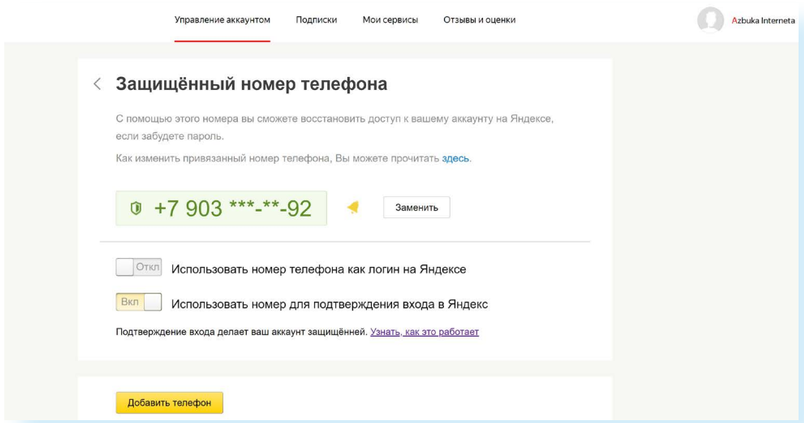
Также можно подключить проверку по смс-коду и к Яндекс.Почте:

- 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).

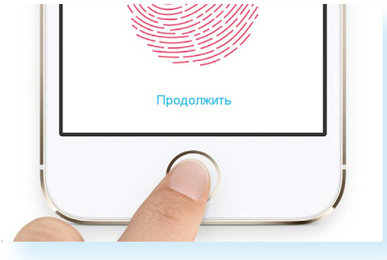
Биометрия и QR-коды

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

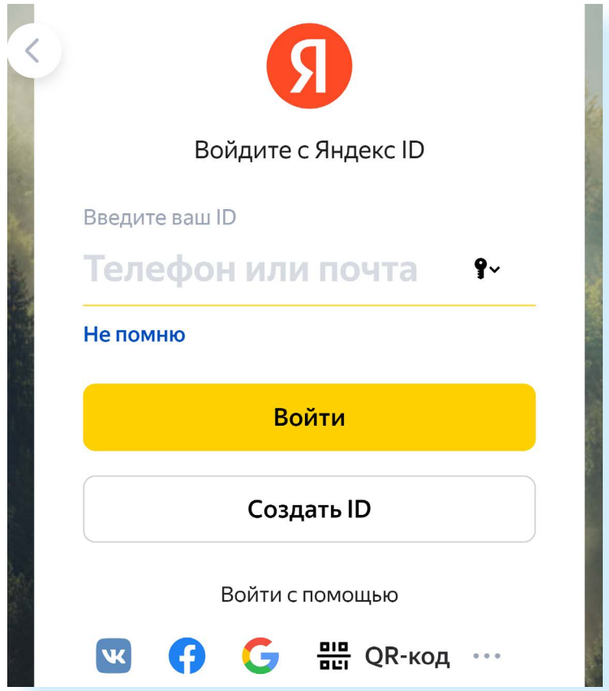
В Айфонах применяется технология **FaceID** (ФейсАйди) – распознавание лица. Если у вас установлена такая функция, то вход в приложение онлайн-банка или в приложение Госуслуги будет по биометрическим данным. Пароль вводить не потребуется.

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 отсутствии 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 подбирать 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.

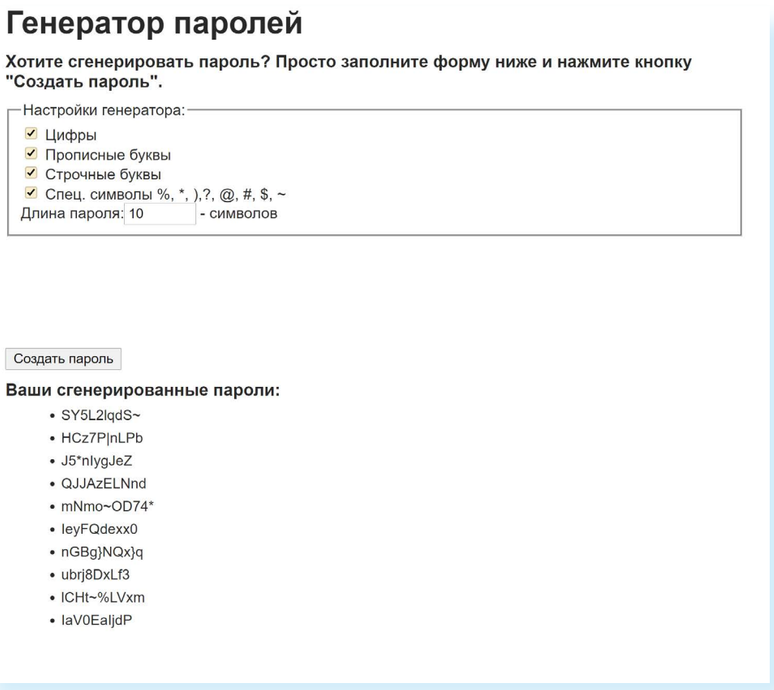
Не думайте, что сможете провести взломщиков, если наберете русское название на клавиатуре в латинской раскладке. Такие уловки брутфорс быстро распознает. Лучше, если в вашем пароле используются необычные или нелогичные сочетания.

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?PoKr. 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



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.

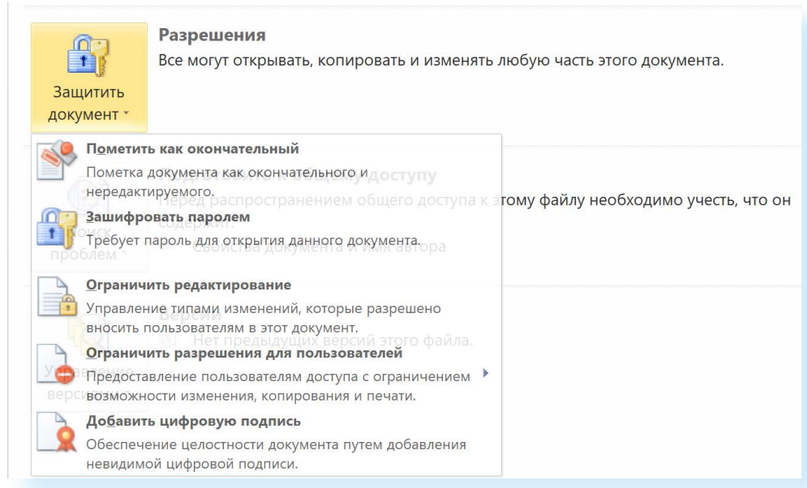
Шифрование файла с паролями

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

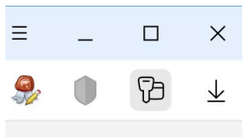


- затем ввести пароль и нажать «ОК».

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.

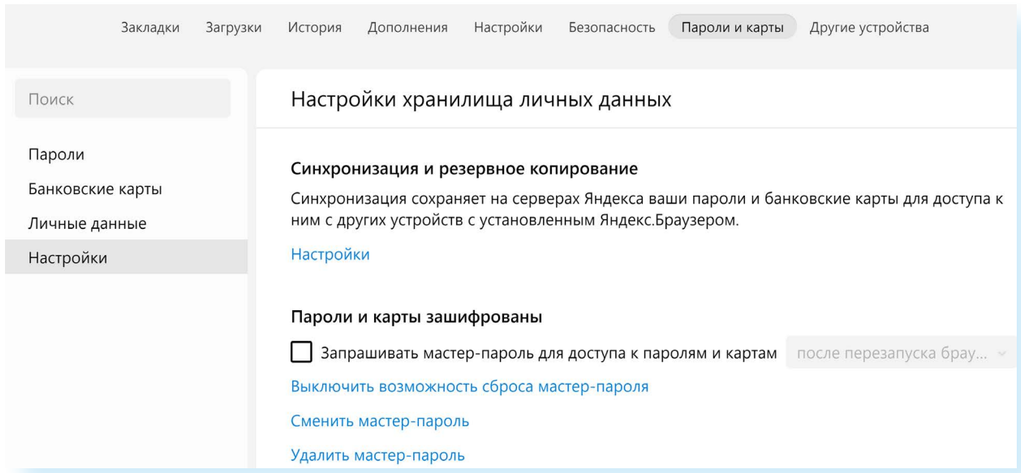


В Яндекс.Браузере вкладка «Пароли и карты» по умолчанию выведена в панель управления вверху справа. (Если такого значка у вас нет, к вкладке «Пароли и карты» можно перейти через «Настройки» браузера).

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 паролям 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?