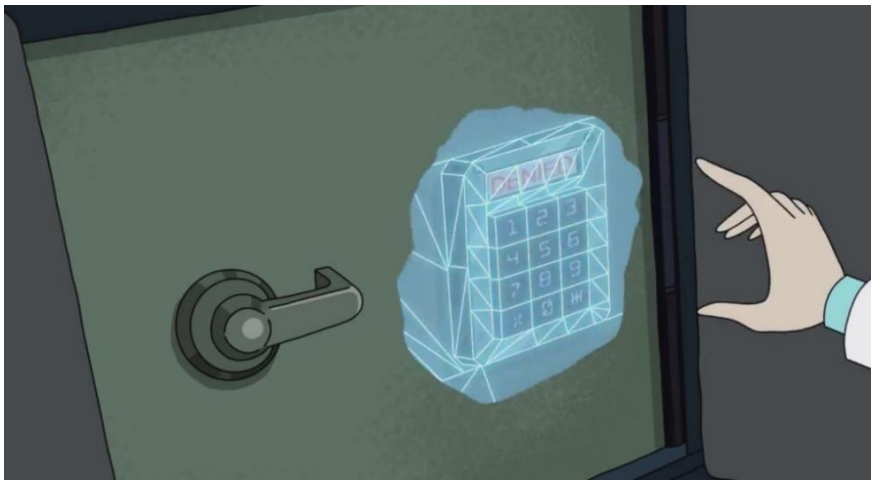
Ознакомься со статьей

Пароли: главные в системе безопасности. Как создать и запомнить надежный пароль на сайте Квалификация

https://hrdco.org/featured/paroli-i-ih-mesto-v-sisteme-bezopasnosti-kak-sozdat-i-zapomnit-nadezhnyj-parol/

В рамках темы безопасности правозащитников и активистов мы не можем обойти стороной такой вопрос, как компьютерная безопасность. В стремительно виртуализирующемся мире работа многих людей осуществляется исключительно через электронные устройства. Вопросов, которые стоит рассмотреть в этом направлении, великое множество. Мы решили начать с темы, с которой любой пользователь сталкивается ежедневно: с темы паролей. В рамках этой инструкции мы расскажем о важных нюансах, связанных с паролями, и рассмотрим тему их безопасного хранения.



Недооцененное значение пароля

Тема «хакерских атак» за последний год в СМИ стала привычной. Она небезосновательно поднималась и раньше, пусть и не с таким постоянством.

За последние два года о взломах или их попытках заявляли российские правозащитные активисты и оппозиционные политики, коммерческие компании и даже кандидаты в президенты нескольких стран.

В таких условиях у простого пользователя может сложиться представление, что защитить себя от попыток взлома со стороны опытного хакера невозможно. Позиция «захотят — взломают» порождает безответственное отношение к своей компьютерной безопасности и делает пользователя еще более уязвимым.

Однако важно знать, что в большинстве случаев компьютерные взломы представляют из себя ничто иное, как подбор или кражу пароля к электронной почте и соцсетям. И большая часть упомянутых выше хакерских атак заключалась именно в этом. То есть качественный пароль и его бережное хранение до сих пор являются краеугольными камнями компьютерной безопасности.

«Хакерские взломы» чаще всего связаны с подбором или кражей паролей.

Принципы создания надежного пароля

Прежде чем перейти к одному из способов создания сложного пароля, важно запомнить наиболее важные принципы, которыми стоит руководствоваться.

1. **Будьте сложнее.** Любые пароли, представляющие из себя простое слово, популярную фразу или простую последовательность цифр — быстро подбираются специальными программами. А если недоброжелатель может выяснить из сети или государственных баз данных информацию о вас, то использование в качестве пароля даты рождения вас или ваших родственников, их фамилий (в т.ч. девичьих), номеров телефонов и прочей доступной информации — небезопасно.
2. **Размер имеет значение.** Для подбора паролей некоторые взломщики могут использовать большие компьютерные мощности. Время на подбор короткого пароля (6-8 символов) уйдет очень небольшое. Но если пароль состоит из более чем 14 символов — на его подбор могут понадобиться годы, что сделает такую задачу бессмысленной.
3. **Один пароль — один сервис.** Нельзя использовать один пароль одновременно для двух соцсетей, почты и любимого форума. Иначе кража этого пароля на одном из сервисов будет значить взлом всех остальных.
4. **Легко запоминается, надежно хранится**. Смысла в пароле, который вы забудете, будет не много. Записывать его на бумажку очень ненадежно: вам легко потерять, другим легко найти. Поэтому лучше иметь один «главный» **мастер-пароль**. Его лучше использовать для входа в **программу хранения паролей**, где вы будете хранить все остальные ключи от ваших соцсетей и сервисов.

Как создать надежный и легко запоминающийся пароль

Способов создания паролей множество. Мы расскажем о том, который используем сами и считаем одним из наиболее удобных и надежных.

- Для основы пароля выберите любую фразу, которую вам легко запомнить. Требования к ней простые: не менее хотя бы 10 слов. Лучше всего, если это будет ваша собственная фраза, но вы можете использовать пару строк из песни или редкую цитату. Публиковать эту фразу где-либо, пока она используется в качестве основы вашего пароля, не рекомендуется.
- Создаете пароль по следующей схеме: первая буква каждого слова из фразы — один символ вашего пароля. Если фраза на русском, сначала переведите ее транслитом в латиницу, т.к. не все сервисы понимают кириллицу.
- Для примера мы возьмем цитату Альбера Камю, переведенную на русский язык: «Самой холодной зимой я узнал, что внутри меня — непобедимое лето». Итак, первые буквы слов транслитом: Самой («S») холодной («h») зимой («z») я («ya» — или просто «y») узнал («u»), что («4») внутри («v») меня («m») — непобедимое («n») лето («l»). Получаем «Shzyu4vmnl». При подборе символа для слова «что», мы сразу решили использовать цифру «4», так как она легко запоминается как аналог «ч/ch», а использование цифр настоятельно рекомендуется. Для большей сложности мы добавим в пароль и знаки препинания из этой фразы. Получаем «Shzyu,4vm-nl». Тире из фразы мы упростили до дефиса «-». Если у вас нет проблем с пунктуацией, расположение знаков препинания в цитате не сложно запомнить, а почти все серьёзные интернет-сервисы позволяют использовать их в пароле.
- Теперь при наборе пароля вы можете просто про себя проговаривать фразу, печатая соответствующие каждому слову символы на клавиатуре. Пароль можно усложнить и сделать длиннее, например, добавив в конце восклицательный знак или сделав строчные

буквы заглавными и наоборот. Главное, чтобы вы легко помнили все ваши «модификации».

Хранение паролей

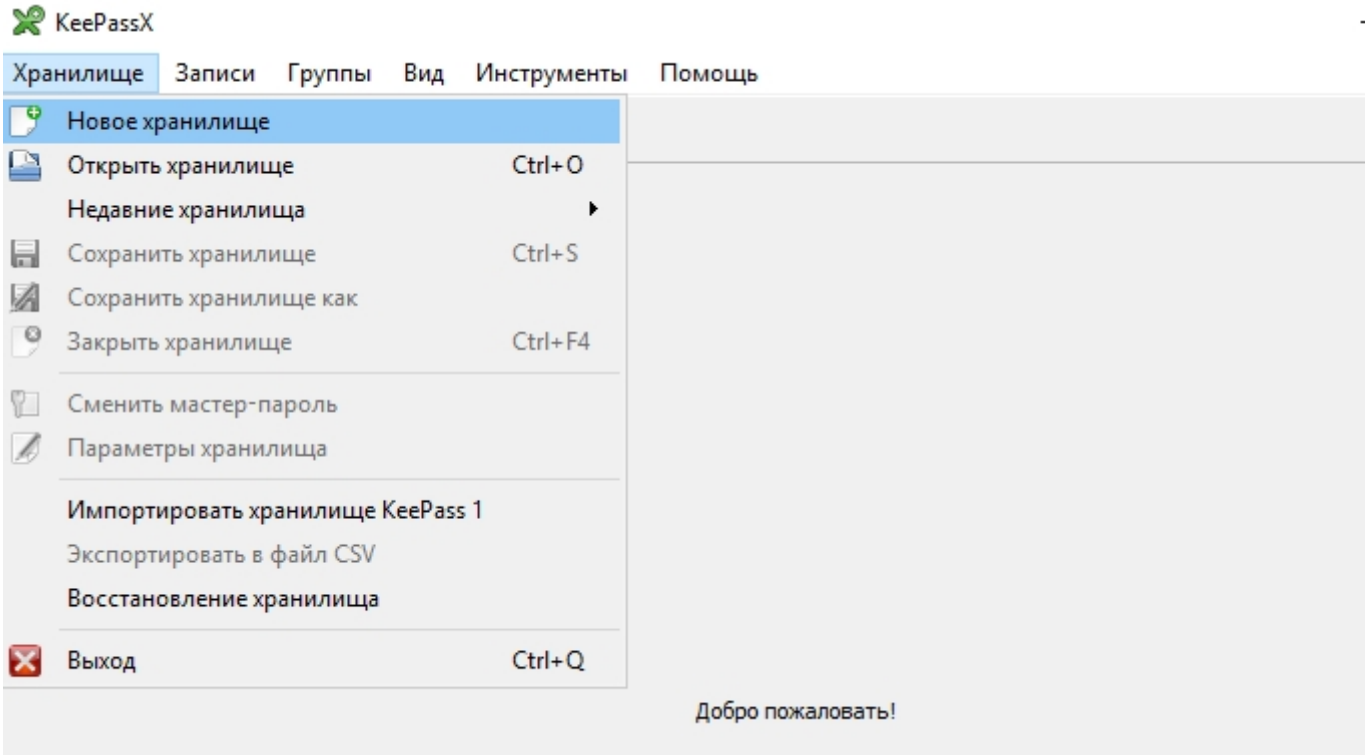
По вышеописанной схеме можно создать пароли для нескольких сервисов. Но риск забыть один из них повышается, особенно, если каким-то сервисом вы начнете пользоваться реже. Поэтому мы рекомендуем использовать специальные программы для их хранения: менеджеры паролей.

Менеджер паролей — это специальная программа, которая шифрует ваши электронные ключи в специальном файле-хранилище. Пользуясь такой программой, вам необходимо будет помнить лишь один главный мастер-пароль от хранилища. И, конечно, бережно хранить этот файл, скопировав на разные устройства на случай поломки или потери одного из них. Отныне это будет самым важным для вас файлом.

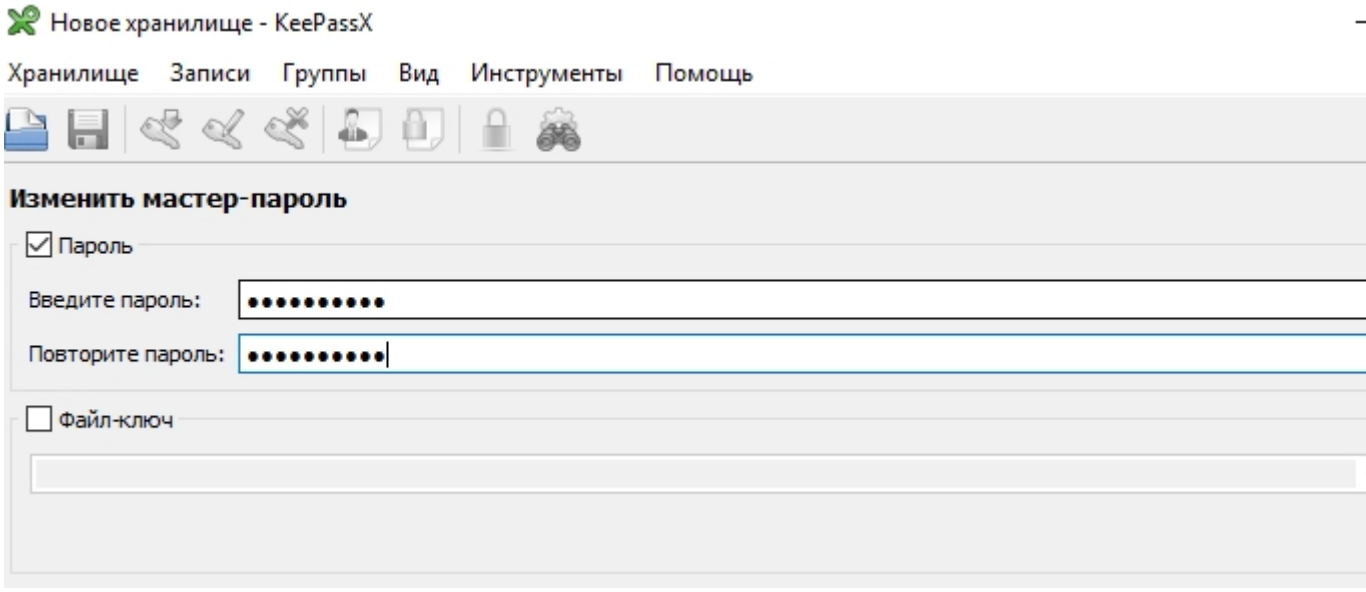
В качестве примера программы для хранения паролей используем **KeePassX.**

Скачать эту программу можно на официальном сайте. Аналоги для мобильных устройств можно найти в соответствующих магазинах приложений (Google Play или App Store) при поиске по запросу «KeePass».

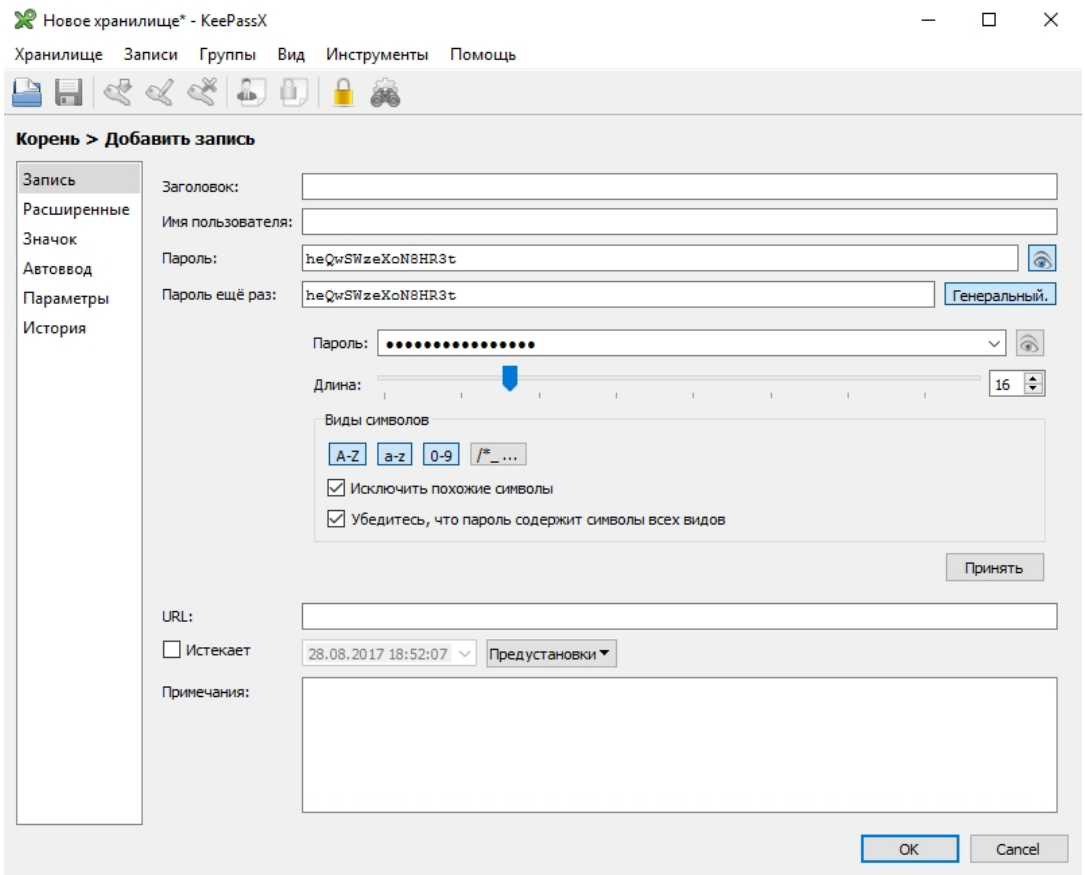
Открыв программу, создаете новое хранилище через меню.



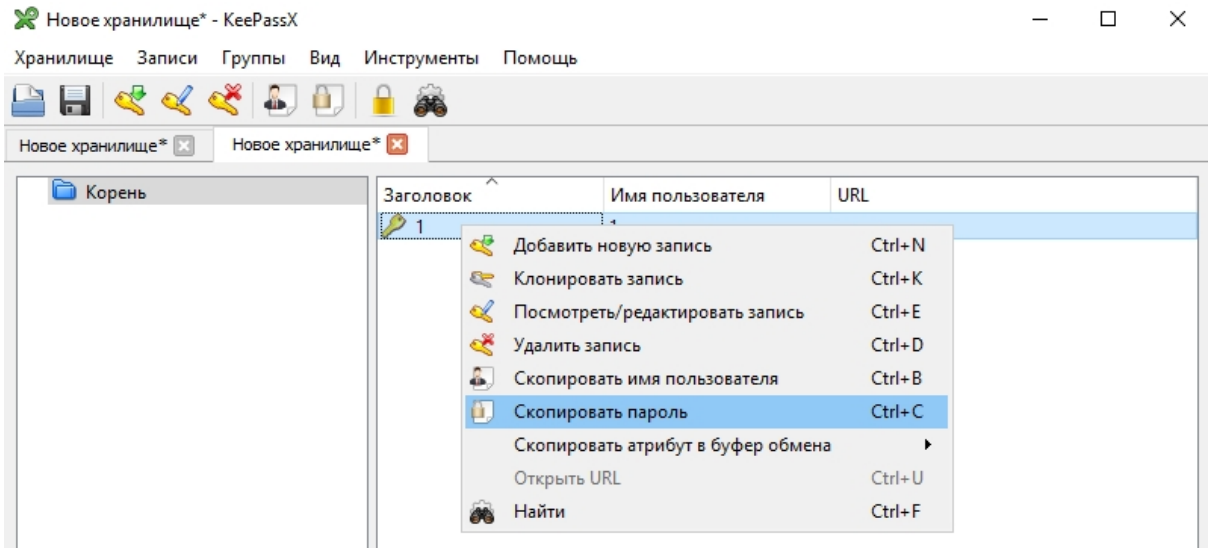
Далее программа попросит ввести придуманный вами мастер-пароль, которым вы и будете открывать хранилище.



Нажав в верхнем меню на иконку ключа с зеленой стрелкой, вы можете добавить или создать новый пароль для какого-либо вашего сервиса. Программа имеет встроенный генератор паролей: для его использования нажмите на кнопку «Генеральный».



Создав надежный ключ, вам не надо его запоминать. Для входа в нужный вам сервис его нужно будет копировать из этого хранилища.



Время хранения пароля в буфере обмена ограничено 10 секундами. В настройках этот параметр можно изменить.

Что удобно, программа позволяет хранить не только пароли, а вообще любые ценные и тяжело запоминающиеся текстовые данные. После того, как все изменения внесены, не забудьте сохранить файл хранилища и скопировать его новую версию на основные устройства.

В следующей инструкции мы расскажем о воровстве паролей — фишинге — и о том, как от него защититься.