



KeePass Password Safe - бесплатная программа для хранения управления паролями.

На сегодняшний день это самая удобная и безопасная программа для ведения своей базы учетных записей, которые используются для доступа на различные ресурсы, например веб-сайты, программы доступа, удаленного подключения VPN и много другого.

Общие сведения о программе

Особо стоит отметить, что **KeePass** работает не только на обычных стационарных компьютерах и ноутбуках, но и на мобильных устройствах, например на телефонах с операционной системой Android, обеспечивая быстрый и безопасный доступ к базе хранимых паролей.

Программа **KeePass** поддерживает алгоритмы Advanced Encryption Standard (AES (256-бит), Rijndael) и Twofish для шифрования паролей своих баз данных.

Программа KeePass переведена более чем на 40 языков, включая русский.

Программа KeePass имеет инсталляционную и портативную, не требующую установки, версию программы.

Программа KeePass может формировать отчеты и выполнять экспорт в форматы TXT, HTML, XML и CSV, а также импорт из множества различных форматов.

Официальная страница: <http://keepass.info/>

На сегодняшний день доступны и активно развиваются две версии программы. Основные отличия версий следующие:

1.xx - облегченная и менее функциональная. Работает быстрее и занимает меньше места. Для домашнего использования отличный вариант.

2.xx - более функциональная версия, является кроссплатформенной, работает без перекомпиляции в ОС Windows, Mac OS X и Linux, но требует для своей работы .NET Framework версии не ниже 2.0 или Mono версии не ниже 2.6. Данная версия больше подходит для использования в корпоративной среде. При этом никто не запрещает использовать ее в домашних условиях.

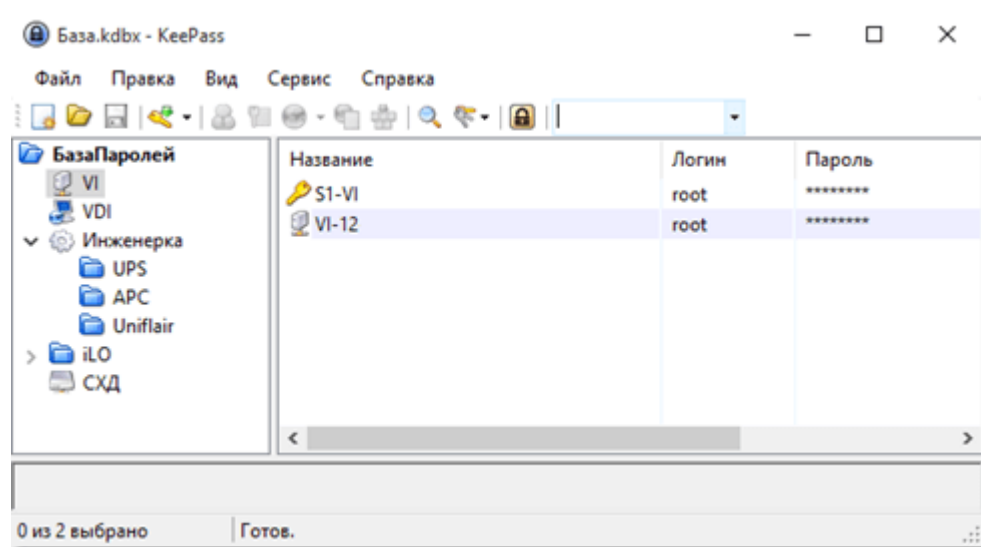
И первая и вторая версия работают отлично. Но лично я использую версию 2.xx


Использование программы KeePass

1. При первом запуске программы необходимо создать новую базу паролей. Для хранения используется файл формата ***.kdbx**
2. После создания базы, KeePass запрашивает пароль и подтверждение. В дальнейшем, указанный пароль будет необходим для доступа к базе.

При вводе пароля будет цветом показана устойчивость пароля к взлому методом перебора.

После ввода пароля и описания базы, откроется главное окно программ, которое представлено на скриншоте ниже.



 Для добавления новой записи, содержащей информацию об учетной записи и пароле, необходимо нажать кнопку в виде ключа (рисунок слева) либо щёлкнуть правой кнопкой мыши в поле справа и в контекстном меню выбрать пункт “Добавить”

запись”.

При этом откроется форма добавления записи, представленная на скриншоте ниже.

В поле **“Название”** вводим краткую информацию о назначении учетной записи.

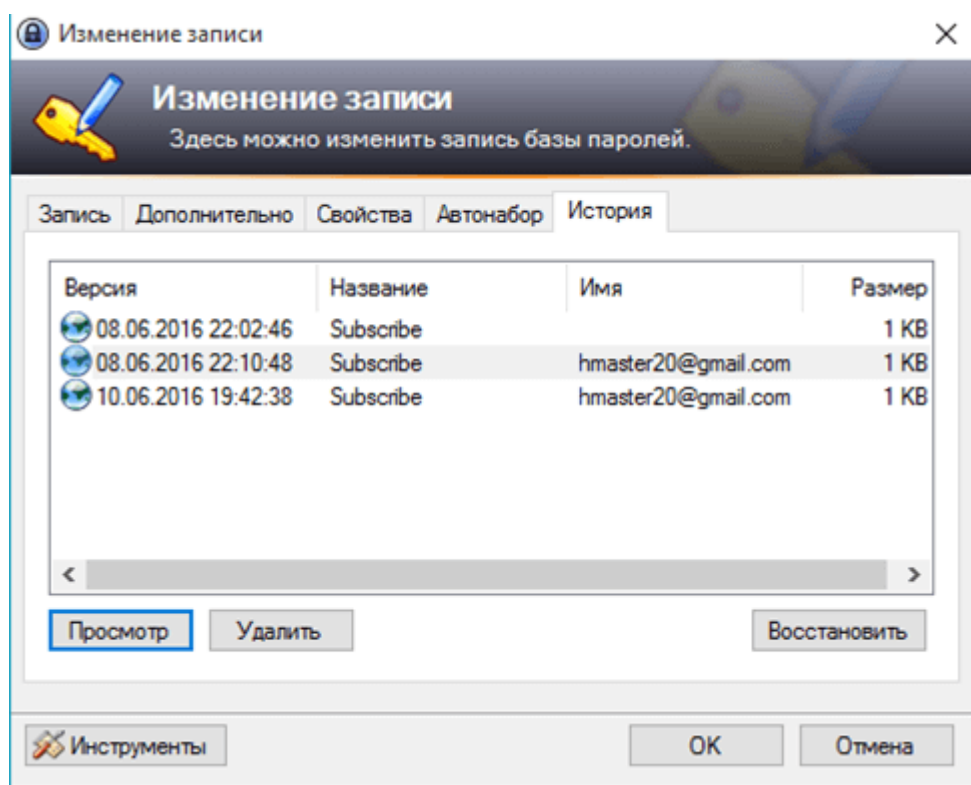
В поле **“Имя”** вводим учетную запись (логин).

В поле **“Пароль”** и поле **“Повтор”** вводим пароль и его подтверждение.

Поле **“Качество”** отобразит цветом стойкость пароля к взлому методом подбора, чем зеленее цвет, тем более стойкий пароль. Так что не поленитесь проверить ваш пароль перед использованием.

В поле **“Ссылка”** вводим веб-ссылку на сайт, это будет очень удобно использовать в дальнейшем.

Есть еще интересная вкладка в окне изменения учетной записи - это вкладка **“История”**. Скриншот ниже.



Вкладка **“История”** отображает всю информацию о любых изменениях учётной записи. Т.е. при любых изменениях можно узнать все, что происходило с учетной записью. Это бывает полезно.

Использование записей KeePass

Использование программы при заполненных учетных данных выглядит следующим образом.

Запускаете программу и открываете необходимый подраздел (группу), например подраздел **“Обучение”**, который представлен на скриншоте ниже.

Название	Имя	Пароль	Ссылка
APC Energy University	hmaster	*****	http://energy.schneideruniversities.com
MVA	hmaster@rambler.ru	*****	https://mva.microsoft.com/
SQL-ex.ru	hmaster	*****	http://sql-ex.ru/
ИНТУИТ	hmaster@rambler.ru	*****	http://www.intuit.ru
Специалист	hmaster@rambler.ru	*****	http://www.specialist.ru/account/logon

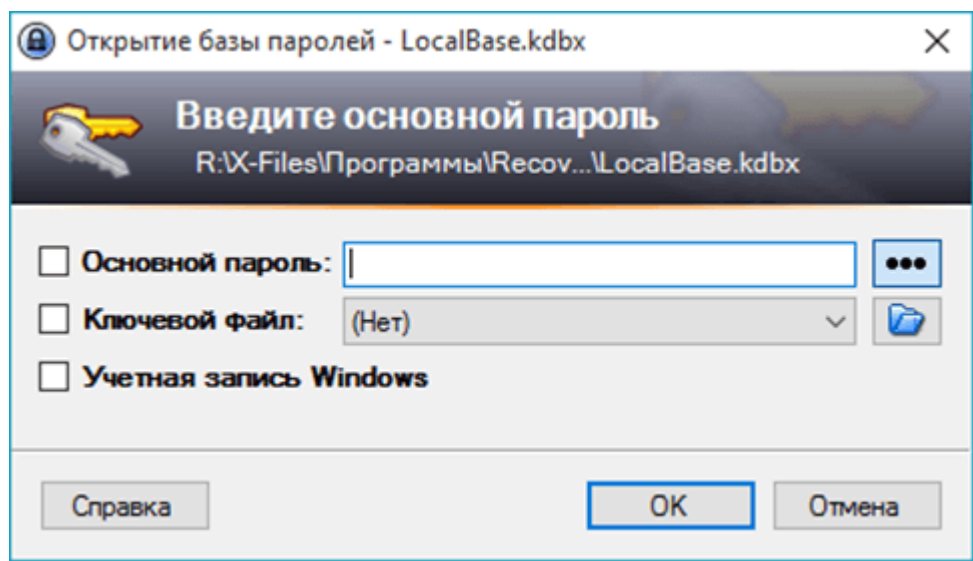
Далее:

1. дважды щелкаете по записи в поле **“Ссылка”** при этом выполниться переход на нужный сайт. На сайте переходим на секцию ввода логина и пароля;
2. переходим в KeePass и дважды щелкаем по записи в поле **“Имя”**, при этом логин будет скопирован в память;
3. переходим на сайт и вставляем **логин**:
 1. нажав сочетание клавиши Ctrl+V,
 2. либо щелкнув по полю правой кнопкой мыши и в контекстно меню выбираем вставить;
4. переходим в KeePass и дважды щелкаем по записи в поле **“Пароль”**, при этом пароль будет скопирован в память;
5. переходим на сайт и вставляем **пароль**:
 1. нажав сочетание клавиши Ctrl+V,
 2. либо щелкнув по полю правой кнопкой мыши и в контекстно меню выбираем вставить.

Первый раз может показаться сложно. Но на самом деле это самый эффективный способ работы с программой KeePass. И пару раз повторив описанную выше процедуру, работать станет вполне удобно.

Завершение работы с программой KeePass

Как только все изменения в базу будут внесены и выполнен выход из программы KeePass, при следующем входе будет запрошен пароль, указанный при формировании базы.



При необходимости изменить пароль к базе можно сделать это через пункт меню Файл – Изменить основной пароль.

Плагины KeePass

Для KeePass выпущено огромное количество плагинов, скачать которые можно перейдя в соответствующий раздел на официальном сайте разработчика, например [здесь](#).

Например я использую следующие плагины:

- Firefox to KeePass Password Importer
- Favicon Downloader

Firefox to KeePass Password Importer – позволяет импортировать все хранимые пароли в браузере Mozilla/Firefox. При первом использовании программы это устраняет от долгих часов формирования первичной базы паролей.

Favicon Downloader – позволяет загрузить иконку с сайта к которому осуществляется доступ через базу KeePass, таким образом делая более наглядным работу с базой паролей.

Установка плагинов заключается в распаковке файла плагина в корень программы, т.е. в ту же папку где находится запускаемый файл **KeePass.exe**, после этого необходимо выполнить перезапуск программы KeePass.

KeePass Password Safe — система хранения (менеджер) паролей