Оглавление

Автозаполнение (Auto-Type)

Автозаполнение - Auto-Type
Мощная функция, отправляющая имитацию и последовательность нажатия клавиш в другие приложения.

Auto-Type Автонабор - Общая информация

Фунцмональные возможности Автозаполнения (Auto-Type) в KeePass.
Эта функция позволяет определить последовательность нажатий клавиш, которые KeePass сможет автоматически выполнять за Вас. Имитация нажатий клавиш, по Вашему выбору, может быть отправлена в любое другое в настоящий момент открытое окно (окна браузера, диалоговые окна авторизаций, ...).

По умолчанию, посылается последовательность нажатия клавиш `{USERNAME}{TAB}{PASSWORD}{ENTER}` т.е. сначала в выбранное окно передается Имя пользователя, а затем идет `Tab`, осуществляющий переключение на поле ввода пароля, вводится пароль и в завершени процедуры, нажимается `Enter`.

Для TAN записей, по умолчанию вводится `{PASSWORD}`, то есть в целевое окно впечатывается TAN, без последующего нажатия `Enter`

Только для KeePass 1.x
Вы легко можете определить свою собственную последовательность Автонабора: просто запишите последовательность в поле **комментарии** записи-входа, с префиксом `"Auto-Type:"`. Ваши заметки могут выглядеть следующим образом:

```
 Вы можете составить любое примечание.
Мой e-mail, который я использовал для регистрации: test@nowhere.com

Auto-Type: {USERNAME}{TAB}{TAB}Some fixed string{TAB}{PASSWORD}{ENTER}

Далее, если Вы захотите то можете продолжить заметки ...
```

Обратите внимание, что бы последовательность Автозаполнения с использованием префикса `Auto-Type:` была записана в одну строку, последовательность не сможет быть определена при записи в две строчки и более.

Если Вы установите две или более `Auto-Type` последовательности, то использоваться будет только первая строка.

Только для KeePass 2.x
Автозаполнение (Автонабор), может формироваться индивидуально для каждой записи входа с помощью функции *Auto-Type* закладка при входе в диалог (выберите запись -> *Edit Entry).* На этой странице, Вы сможете задать последовательность по умолчанию и настроить ассоциации для конкретного окна / последовательности .

Поддержка Двухканальной Auto-Type Обфускации (делает Автозаполнение (Auto-Type) устойчивым против клавиатурных шпионов).

Дополнительно, можно создавать настраиваемые ассоциации окно / последовательность, которые отменяют установленную по умолчанию последовательность. Вы можете определить различные последовательности нажатия клавиш для различных окон каждого входа. Например, представьте себе веб-ресурс, на котором Вам неоходимо Авторизоваться и что на этом ресурсе существует несколько страниц для авторизаций. Все эти страницы, могут немного различаться (например на одной из них, Вам дополнительно потребуется поставить флажок в некоторый checkbox - что часто бывает на форумах).. И вот задачи решает создание настроенных ассоциаций окна/последовательности: Вы просто определяете различные последовательности Автозаполнения (Auto-Type) индивидуально для каждого окна (идентифицируя их по названию).

Запуск Авто-Type:
Существуют три различных способа обращения к функции Автонабора:

- Вызов Автозаполнения для записи-входа с помощью команды контекстного меню *Выполнить Auto-Type,* при выбранно записи.
- Выберите запись и нажмите *Ctrl-V* (это "горячие клавиши" для контекстного меню выше).
- Использование общесистемных "горячих клавиш" для auto-type. KeePass будет искать все входы-записи в открытой в настоящее время базе данных для сравнения последовательностей.

Более подробно все методы рассмотрены ниже.

Контекстное меню: Команда *"Выполнить Auto-Type* '

Этот метод, требует наименьшее количество настроек и является наиболее простым, но его недостаток в том, что сперва Вам потребуется выбрать вход-запись в KeePass для который вы хотите использовать Автозаполнение (auto-type). Метод прост: правой кнопкой мыши нажимаете на запись в открытой на текущий момент базе данных и выбираете команду *"Выполнить Auto-Type* ', либо нажмите *Ctrl-V* (горячие клавиши для этой команды). Бывшее в фокусе окно (т.е. то, в котором вы работали до обращения к KeePass) будет опять переведено на первый план и KeePass в этом окне, выполнит Автозаполнение. Используемая для Автозаполнения последовательность, зависит от названия окна ввода. Если Вы не определили ассоциаций для окна / последовательности,

то для Автоввода будет выбрана последовательность установленная по умолчанию. Если же, Вы создали ассоциацию, то KeePass использует последовательность стоящую на первом месте в списке из соответствующих ассоциации. Если ни одна из ассоциаций не совпадает, используется последовательность установленная по умолчанию.

Применение Глобальных "горячих клавиш" Автозаполнения (Auto-Type)

Это более мощный метод, но он потребует немного больше подготовки и знаний, прежде чем он сможет быть использован.

Простой пример применения Глобальных "горячих клавиш" Автозаполнения (Auto-Type):

1. Создайте запись-вход в KeePass под названием *Блокнот* с указанием имени пользователя и пароля.
2. Откройте программу "Блокнот" - Пуск -> Программы -> Стандартные.
3. В прграмме "Блокнот" нажмите сочетание клавиш *Ctrl + Alt + A*. Имя пользователя и пароль будут введены в "Блокнот".

Название *Блокнот записи-входа* KeePass сочетается с заголовком окна программы "Блокнот" и по умолчанию вводится эта последовательность Auto-Type.

Как это работает - Подробная информация:

KeePass регистрирует общесистемные "горячие клавишы" для автозаполнения. Преимущество этих "горячих клавиш" состоит в том, что Вам не нужно, переключаться на окно KeePass и выберать запись-вход. А нужно просто нажать "горячие клавиши", в открытом целевом окне (т.е., в окне, которое будет получать моделируемые нажатия клавиш). По умолчанию, глобальное сочетание горячих клавиш *Ctrl-Alt-A* (т.е. удерживая Control и Alt нажмите на клавиатуре клавишу "A" и освободите все ключи). Однако, Вы можете изменить горячие клавиши в настройках программы менеджера паролей KeePass Password Safe откройте (Главное меню - "Инструменты" - "Настройка", вкладка "Расширенные", кнопка "Автонабор"): здесь, в текстовом поле ниже "Глобальная "горячая" клавиша для автонабора" введите горячий ключ, который Вы хотите использовать. Если данный горячий ключ доступен и не занят, он появится в текстовом поле. Когда Вы, нажмете горячие клавиши, KeePass будет смотреть на название открытого в настоящее время окна и начнет искать в открытой, в настоящее время базе данных, пригодные для использования записи-входы. Если KeePass находит несколько записей, которые можно использовать, он выводит диалоговое окно выбора. Для определения возможности, использования записи для текущего открытого окна, должно быть выполнено по крайней мере одно из следующих условий:

- Название записи-входа соответствует текущему заголовку активного окна.
- У записи-входа есть ассоциации окна/последовательности, которые соответствует названию открытому в настоящее время активному окну.

Второе условие уже было упомянуто, но первое является новым. При использовании названия записи-входа как фильтра для названия окна, количество конфигураций Автозаполнения практически сводится нулю: Вам только необходимо быть уверенным, что название записи-входа содержится в заголовке окна, в котором Вы хотите произвести Авто-вход с помощью Автозаполнения. Конечно, это не всегда возможно (например, если сайт имеет очень общее название, такое как *"Добро пожаловать"),* то здесь нужно использовать специальные средства ассоциаций для окон / последовательностей.

Только для KeePass 1.x
Пользовательские ассоциации, окно / последовательность, могут быть указаны с помощью полей для комментариев входов-записей.

```
 Мой адрес e-mail который я использовал для регистрации: test@nowhere.com

Auto-Type: {USERNAME}{TAB}{TAB}Some fixed string{TAB}{PASSWORD}{ENTER}
Auto-Type-Window: Some Website - Welcome*

Далее, если захотите, Вы можете продолжить свои заметки, ...
```

И теперь, если у Вас открыто окно, которое начинается с "Some Website - Welcome " и Вы нажмёте сочетание Глобальных "горячих клавиш", KeePass выполнит автозаполнение указенной выше Auto-Type последовательности.

Некоторые сайты, особенно банки, используют многостраничные схемы авторизации. Вы можете использовать строки `Auto-Type-Window` для автоматизации этих сайтов. Вы также можете использовать стоки `Auto-Type-Window` для стандартизации Вашего Входа в локальной сети и в одной записи KeePass.

Как и другие, строки `Auto-Type-Window` для каждой записи могут быть сформированы по Вашему желанию.

Кроме того, одна последовательность может быть использована в нескольких окнах. Для этого сначала определим пару окно / последовательность как нормальную, а затем продолжим путем добавления "-" и номеров, начиная с 1. Пример:

```
Auto-Type: {USERNAME}{TAB}{PASSWORD}{ENTER}
Auto-Type-Window: Some Dialog - *
Auto-Type-1: {USERNAME}{ENTER}
Auto-Type-Window-1: * - Editor
Auto-Type-Window-1: * - NotePad
Auto-Type-Window-1: * - WordPad
Auto-Type-2: {PASSWORD}{ENTER}
Auto-Type-Window-2: Some Web Page - *
```

В данном примере, последовательность `Auto-Type-1` будет использоваться для всех `Auto-Type-Window-1` Windows.

Только для KeePass 2.x
Пользовательские ассоциации, окно / последовательность, могут быть указаны в закладке *"Auto-Type"*" каждой записи-входа.

Последовательность нажатия клавиш Автозаполнения

Авто-последовательность нажатия клавиш заполняется одной строкой, которая может содержать заполнители и специальные коды клавиш.

Вы уже знаете, что по умолчанию установлена последовательность Автозаполнения `{USERNAME}{TAB}{PASSWORD}{ENTER}`.
Здесь, `{USERNAME}` и `{PASSWORD}` являются заполнителями: при выполнении Автозаполнения, они заполняют соответствующие поля в окне Авторизации. `{TAB}` и `{ENTER}` это специальные коды клавиш: они заменены нажатием соответствующими клавиш.
Специальные коды клавиш, это единственный способ задать специальные ключи, такие как стрелка-вниз, Shift, Escape и т.д.

Однако, последовательности нажатия клавиш могут также содержать и простые символы, которые так же будут отправлены. Например, следующая строка вполне соответствует строке последовательности нажатия клавиш:
`{USERNAME}{TAB}Данный текст будет передан!{ENTER}.`

Только для KeePass 1.x
Маркеры-заполнители и специальные коды клавиш чувствительны к регистру.

Только для KeePass 2.x
Маркеры-заполнители и специальные коды клавиш не чувствительны к регистру.

KeePass поддерживает следующие маркеры-заполнители:

Поле	Заполнитель
Название	{TITLE}
Имя пользователя	{USERNAME}
URL	{URL}
Пароль	{PASSWORD}
Комментарии	{NOTES}

Только для KeePass 2.x
На пользовательские строки можно ссылаться помощью `{S: Name }` Например, если у вас есть пользовательская строка с названием "eMail", вы можете использовать заполнитель `{S:eMail}`

Ссылки на поля других записей:
См. Ссылки на Поля. Auto-Type переименовывает эти ссылки перед вводом нажатий клавиш.

Специальные клавиши:
Поддерживаются следующие коды специальных клавиш:

Специальные Клавиши	Код
Tab	{TAB}
Enter	{ENTER} или ~

Arrow Up	{UP}
Arrow Down	{DOWN}
Arrow Left	{LEFT}
Arrow Right	{RIGHT}
Insert	{INSERT} или {INS}
Delete	{DELETE} или {DEL}
Home	{HOME}
End	{END}
Page Up	{PgUp}
Page Down	{PgDn}
Backspace	{BACKSPACE}, {BS} или {BKSP}
Break	{BREAK}
Caps-Lock	{CAPSLOCK}
Escape	{ESC}
Help	{HELP}
Numlock	{NumLock}
Print Screen	{PrtSc}
Scroll Lock	{ScrollLock}
F1 - F16	{F1} - {F16}
Клавиша +	{ADD}
Клавиша -	{SUBTRACT}
Клавиша *	{MULTIPLY}
Клавиша /	{DIVIDE}
Shift	+
Control	^

Alt	%

Только для KeePass 1.x

Специальный Клавиши	Код
Space	{SPACE}
+	{PLUS}
@	{AT}
%	{PERCENT}
Apps	{APPS}
^	{CARET}
~	{TILDE}
{, }	{LEFTBRACE}, {RIGHTBRACE}
(,)	{LEFTPAREN}, {RIGHTPAREN}
Windows Key: left, right Windows Key: влево, вправо	{LWIN} {RWIN} ЛВИН () () RWIN
Windows Key	{WIN} (equ. to LWIN)
Windows Key	@
Numpad 0 to 9 Numpad 0 до 9	от {NUMPAD0} до {NUMPAD9}

Только для KeePass 2.x

Специальные Клавиши	Код
+	{+}
^	{^}
%	{%}
~	{~}
(,)	{(}, {)}
{, }	{{}, {}}

Дополнительно, поддерживаются некоторые специальные команды:

Синтаксис команд	Действие
{APPDIR}	Будет заменен на текущий путь к каталогу приложений.
{DELAY X}	Задержка X миллисекунд.
{INTERNETEXPLORER}	Будет заменен на путь Internet Explorer, если он установлен.
{FIREFOX}	Будет заменен на путь Mozilla Firefox, если он установлен.
{OPERA}	Будет заменен на путь Opera, если она установлена.
{GOOGLECHROME}	Будет заменен на пути Google Chrome, если он установлен.

Только для KeePass 1.x

Синтаксис команд	Действие
{CLEARFIELD}	Очищает содержимое поля, которое в настоящее время находится в фокусе (содержимое только одной строки).
{VKEY X}	Отправляет VKEY со значением X.
{BEEP XY}	Подает звуковой сигнал с частотой X и продолжительностью в Y миллисекунд.
{DELAY=X}	Устанавливает задержку X в миллисекундах, на все последующие нажатия клавиш.
{APPACTIVATE WindowTitle}	Активизирует окно "WindowTitle".

Только для KeePass 2.x

Синтаксис команд	Действие
{GROUP}	Название родительской группы записи-входа.
{GROUPPATH}	Полный путь к группе записи-входа.
{PICKPASSWORDCHARS} {PICKPASSWORDCHARS *n* : *k* }	Показывает диалоговое выбора определенных символов пароля. См. ниже.
{NEWPASSWORD}	Генерирует новый пароль. См. ниже.
{DELAY=X}	Устанавливает задержку X в миллисекундах для всех стандартных клавиш в этой последовательности.
{URL:RMVSCM}	Вступлению URL без схемы описания.
{DB_PATH}	Полный путь к текущей базе данных.

{DB_DIR}	Директория текущей базы данных.
{DB_NAME}	Имя файла (включая расширение) текущей базы данных.
{DB_BASENAME}	Имя файла (без расширения) текущей базы данных.
{DB_EXT}	Расширение имени файла текущей базы данных.
{ENV_DIRSEP}	Разделитель каталогов (для Windows, / для Unix).
{DT_SIMPLE}	Текущее местное дата/время как простая, поддающаяся сортировке последовательность.
{DT_YEAR}	Года текущей местной даты / времени.
{DT_MONTH}	Месяц текущей местной даты / времени.
{DT_DAY}	День текущей местной даты / времени.
{DT_HOUR}	Час текущей местной даты / времени.
{DT_MINUTE}	Минута текущей местной даты / времени.
{DT_SECOND}	Секунды текущей местной даты / времени.
{DT_UTC_SIMPLE}	Текущие UTC дата / время как простые, поддающиеся сортировке строки.
{DT_UTC_YEAR}	Год компонента UTC текущей даты / времени.
{DT_UTC_MONTH}	Месяц компонента UTC текущей даты / времени.
{DT_UTC_DAY} DT_UTC_DAY ()	День компонента UTC текущей даты / времени.
{DT_UTC_HOUR} DT_UTC_HOUR ()	Час компонента UTC текущей даты / времени.
{DT_UTC_MINUTE} DT_UTC_MINUTE ()	Минута компонента UTC текущей даты / времени.
{DT_UTC_SECOND} DT_UTC_SECOND ()	Секунды компонента UTC текущей даты / времени.

Только для KeePass 2.x
Нажатие клавиш и спец-клавиш (не заполнителей или команд) может быть повторено с помощью добавления значения в пределах кода. Например, `{TAB 5}` нажмет клавишу табуляции 5 раз.

В заключении, несколько примеров:

`{TITLE}{TAB}{USERNAME}{TAB}{PASSWORD}{ENTER}`
Вводится Название Входа, Tab, Имя пользователя, Tab, соответствующий Пароль, и нажимается ENTER.

`{TAB}{PASSWORD}{ENTER}`
Нажимается клавиша Tab, вводится Пароль и нажимается ENTER.

`{USERNAME}{TAB}^v{ENTER}`
Вводится Имя пользователя, Tab, вводится сочетание Ctrl-V (которое вставляет данные из буфера обмена Windows в большинстве приложений), и нажимает ENTER.

Переключение Флажков:
Иногда, Вы находите на сайтах чекбоксы (например*: "Запомнить меня на этом компьютере"*). Вы можете проставлять флажки, отправив символ пробела (`' '`) при Автозаполнении. Например:
`{USERNAME}{TAB}{PASSWORD}{TAB} {TAB}{ENTER}`
Если есть веб-форма с полем Имя пользователя, Паролем и Чекбоксом, то последовательно будет введено Имя пользователя, Пароль и с помощью пробела идущего за паролем переключится Флажок в чекбоксе.

Нажатие нестандартный Кнопки:
Нажатие нестандартной кнопки работает так же, как и переключение флажков: отправляется символ пробела (`' '`) Заметим, что это может быть использовано только для нестандартных кнопок; для кнопок по умолчанию используется `{ENTER}`.

Высшее ANSI символы:
Функция Автозаполнения поддерживает отправку высших символов ANSI в диапазоне 126-255. Это означает, что Вы можете отправлять специальные символы вроде ©, @, и т.п. без каких-либо проблем, Вы можете записать их непосредственно в определение последовательности клавиш.

Только для KeePass 2.x
Выбор символов Пароля:
Диалог выбора символов Пароля, может быть вызван несколько раз в одной последовательности Автозаполнения. Первым используется `{PICKPASSWORDCHARS}`, а затем добавляются номера, начиная с 2, т.е. `{PICKPASSWORDCHARS2}`, `{PICKPASSWORDCHARS3}` , и т.д..

В KeePass ≥ 2,08, Вы можете дополнительно указать количество символов для выбора. Чтобы сделать это, добавьте `:k` в заполнитель, где `k` является количеством символов. Например, `{PICKPASSWORDCHARS2:5}` является заполнителем с идентификатором 2, и позволит выбрать 5 символов. Преимущество предопределенного количества символов в то, что после выбора необходимого количества, диалоговое окно закрывается автоматически, то есть Вам больше не нужно нажимать [OK] .

Только для KeePass 2.x
`{NEWPASSWORD}` - Генерация новых Паролей:
В KeePass ≥ 2,09, `{NEWPASSWORD}` заполнителя генерирует новый пароль для текущей записи-входа, основанный на генераторе профиля "Автоматически созданные пароли для новых записей".

Это заполнитель заменен один раз в процесса Автозаполнения, т. е. для типичного диалога "Старый Пароль - Новый Пароль - Повторить новый Пароль" Вы можете использовать последовательность
`{PASSWORD}{TAB}{NEWPASSWORD}{TAB}{NEWPASSWORD}{ENTER}`.

Фильтры для целевого окна

При создании пользовательской ассоциации окно / последовательность, вам нужно сообщить KeePass как выглядит соответствующее название окна. Здесь KeePass поддерживает простые символы:

Строка с Групповым символом	Значение
STRING	Соответствует всем заголовкам окон, которые названы именно "String".
STRING*	Соответствует всем заголовкам окон, которые начинаются с "String".
*STRING	Соответствует всем заголовкам окон, которые заканчиваются "String".
STRING	Соответствует всем заголовкам окон, у которых "STRING" где-то в заголовке окна. Включает в себя строки в начале или в конце заголовка окна.

Только для KeePass 1.x
Другие Групповые символы не поддерживаются. Групповой символ `*` не должны находиться в середине строки.

Например, `*Windows*Explorer*` не будет соответствовать `Windows Explorer` он будет соответствовать только `Windows*Explorer` т.е. средний `*` символ рассматривается не как подстановка, а как '*' текстовый символ.

Только для KeePass 2.x
В KeePass ≥ 2.06, групповые символы могут находится и в середине шаблона. Например, `*Windows*Explorer*` будет соответствовать `Windows Explorer`

Дополнительно, поддерживается соответствие с помощью регулярных выражений. Для того, чтобы показать KeePass, что шаблон является регулярным выражением, заключите его в `//`. Например, `//B.?g Window//` будет соответствовать `Big Window`, `Bug Window` и `Bg Window`

С помощью групповых символов (подстановочных знаков), Вы можете сделать свои ассоциации Автозаполнения независимыми от браузера. Для получения дополнительной информации, смотрите примеры использования.

Изменение дефолтной последовательности Автонабора

Последовательность Автозаполнения по умолчанию (т.е. та, которая используется, пока Вы не установили свою) `{USERNAME}{TAB}{PASSWORD}{ENTER}`. KeePass позволяет изменить, это значение последовательности по умолчанию. Обычно, Вам не нужно будет её изменять (вместо этого используются пользовательские настройки окна / последовательности!), но она весьма полезна, когда некоторые другие приложения вмешиваются в работу KeePass (например программное обеспечение безопасности, которое всегда спрашивает у Вас разрешение прежде, чем позволить KeePass произвести Авто-ввод).

Только для KeePass 1.x
Установленные по умолчанию настройки последовательности Автозаполнения можно изменить диалоговом окне настроек Автонабора. Это окно диалога можно найти в *меню "Инструменты" -> "Настройка" -> "Расширеные" -> "Автонабор"*.

Только для KeePass 2.x
По умолчанию, записи унаследуют групповые параметры Автонабора. Группы так же наследуют установки Автозаполнения от своих родительских групп. Существует только одна высшая группа (Первая группа содержит все другие группы). Следовательно, если Вы измените тип автоматической последовательности этой первой группы, то все другие группы, и их записи будут использовать эту последовательность. Практически, это глобальное изменение настроек.

Примеры использования

Теперь, давайте рассмотрим реальный пример: авторизации на веб-сайте. В этом примере, мы будем использовать глобальные горячие клавиши Автонабора, чтобы заполнить необходимые поля интернет страницы для входа в систему. Сперва открываем тестовую страницу, а затем создаем новую запись в KeePass с названием *Test Form*, Именем пользователя и Паролем по Вашему выбору.

Давайте предположим, что глобальная горячая клавиша Автонабора установлена в Ctrl-Alt-A (значение по умолчанию). KeePass работает в фоновом режиме, Вы открыли свою базу данных, и рабочее пространство разблокировано.

Теперь, когда Вы перейдете к тестовой странице на которой будет предложено ввести Имя пользователя и Пароль, просто кликните левой кнопкой мыши в поле *Имя пользователя* и нажмите *Ctrl-Alt-A*. KeePass введет Имя пользователя и Пароль для Вас!

Почему это работает? Название заголовка окна в окне Вашего браузера было *"Test Form - KeePass - Internet Explorer"* или же *"Test Form - KeePass - Mozilla Firefox"*, в зависимости от используемого Вами браузера. А поскольку название для записи-входа в KeePass мы дали "*Test Form" и это* название, содержится в заголовке окна тестовой страницы, поэтому KeePass и использовал эту запись-входа.

И так, Вы видите огромные преимущества Автозаполнения, оно не требует от браузера никакого дополнительного программного обеспечения (браузер ничего не знает о KeePass - и вспомогательные плагины для браузера не требуются), эта функция не зависит от

обозревателя,: одна запись-входа созданная в рамках KeePass, работает и для Internet Explorer *и для* Mozilla Firefox (и для других браузеров), не требуя каких-либо дополнительных изменений или настроек.

Когда Вы будете использовать настройки окна / последовательности (вместо Автонабора по точному совпадению заголовков), то используя групповые символы Вы сможете добиться того же эффекта браузер-независимости. Например: можно использовать, как окно фильтра, следующую запись "`Test Form - KeePass - *`" . Этот фильтр, будет соответствовать окнам браузеров, Internet Explorer и Mozilla Firefox, а так же подойдет и для многих других обозревателей.

Параметры Командной строки

Параметры Командной строки для автоматизации задач в KeePass.

Вы можете задать путь к файлу в командной строке и указать KeePass немедленно открыть этот файл после запуска.

Одновременно, Вы можете указать пароль и/или местоположение Ключевого файла для этой базы данных.
В качестве переключателей, могут быть использованы слэш (/) или минус (-).

Файл базы данных. Расположение файла Базы данных передается в качестве аргумента. Можно использовать только один файл базы данных. Если путь содержит пробелы, он должнен быть заключен в кавычки (").

Пароль. Пароли передаются с аргументом `-pw:`. Для того чтобы провести 'ABC', как пароль, вы должны добавить следующий аргумент для командной стоки `-pw:abc` . Обратите внимание, что не должно быть пробела между **':'** и паролем. Если Ваш пароль содержит пробелы, необходимо заключить его в кавычки. На пример: `-pw:"my secret password"` .

Ключевой файл. Для определения месторасположения Ключевого файла, используется переключатель `-keyfile:`. Применяются те же правила, как и в примере выше, только здесь, Вам потребуется прописать путь до Ключевого файла `-keyfile:D:pwsafe.key` Кроме того, адрес необходимо заключить в кавычки при наличии в нем пробелов, табуляций или других символов пробелов.

Предварительный выбор. Для того, чтобы просто предварительно выбрать ключевой файл, используется аргумент `-preselect:` . Например, если Вы заблокировали базу данных с помощью пароля *и* ключевого файла, а при запуске программы хотите просто вводить пароль (без Выбора вручную, ключевого файла), командная строка будет выглядеть так:

```
KeePass.exe "C:My DocumentsMyDatabase.kdb" -preselect:C:pwsafe.key
```

И тогда, KeePass выведет только запрос о вводе пароля для доступа к базе данных, так как ключевой файл по адресу, `C:pwsafe.key` уже был выбран. При использовании выключателя `-preselect:`, KeePass по умолчанию выбирает Ключевой файл и открывает окно диалога, для ввода пароля.

Обратите внимание на различия! При использовании переключателя `preselect`, для Вас происходит только предварительный выбор ключевого файла и отображается окно для ввода пароля. В отличие от него, параметр `keyfile` не запросит у Вас пароль (возможно, он и не требуется).

Параметр командной строки `-minimize`, заставляет KeePass свернуться при запуске.

Параметр командной строки `-auto-type,` указывает KeePass, включить глобальное Автозаполнение.

Только для KeePass 1.x

- Если аргумент `-readonly` указывается в командной строке, то KeePass откроет базу данных в режиме только для чтения.
- Аргумент `-lock` принуждает KeePass открыться в блокированном режиме (то есть, Вас немедленно не спросят относительно главного ключа, также как и о пути к базе данных).

Только для KeePass 2.x

- Дополнительно поддерживается переключатель `-useraccount`. Программа запустится, если подтверждены полномочия текущей учетной записи пользователя.

- Выключатель `-iocredfromrecent` заставляет KeePass загрузить учетные файлы системы (не ключ базы данных) со списком недавно использованных файлов. На ряду с этим, полномочия файловой системы могут быть определены, с использованием параметров `-iousername` и `-iopassword`.
- Параметр `-entry-url-open` принуждает KeePass искать другие записи-входы и открыть их URL. Запись определяет его UUID, который можно передать параметром командной строки `-uuid:`.

Порядок использования аргументов, является произвольным.

Примеры использования

Откройте файл базы данных ": Мои документы MyDatabase.kdb" (KeePass попросит вас ввести пароль и / или расположение ключевого файла):

```
KeePass.exe "C:My DocumentsMyDatabase.kdb"
```

Если у вас есть База данных, заблокированная с помощью пароля 'ABC', то открываете её так:

```
KeePass.exe "C:My DocumentsMyDatabaseWithPw.kdb" -pw:abc
```

Если Ваш USB Stick постоянно прикреплен к диску F: и у Вас заблокированная База данных с Ключевым файлом на USB Stick, то Вы сможете открыть её следующим образом:

```
KeePass.exe "C:My DocumentsMyDatabaseWithFile.kdb" -keyfile:F:pwsafe.key
```

Если Ваша База данных заблокирована с помощью Композитного ключа (пароль *и* ключевой файл), то Вы можете объединить эти два ключа и открыть базу данных следующим образом:

KeePass.exe "C:My DocumentsMyDatabaseWithTwo.kdb" -pw:abc -keyfile:F:pwsafe.key

Вы блокировали свою базу данных, используя пароль и Ключевой файл, а при открытии хотите иметь предварительно выбранный файл ключей, без авто-ввода пароля (то есть, Вы желаете получать запрос относительно пароля), тогда Ваша командная строка будет выглядеть бы следующим образом:

```
  KeePass.exe "C:My DocumentsMyDatabaseWithTwo.kdb" -preselect:F:pwsafe.key
```

Запуск KeePass с использованием Пакетных файлов

Для запуска KeePass, могут быть использованы Пакетные файлы. Главным образом, для объединения некоторых из упомянутых выше параметров. Теоретически, Вы можете просто поместить командную строку в командный файл (определить путь и параметры), но это плохой способ, поскольку окно командной строки останется открытым, пока не будет закрыт KeePass. Поэтому рекомендуется использовать следующий метод:

```
START "" KeePass.exe ..MyDb.kdb -pw:MySecretPw
```

Эта команда START выполнит KeePass (который откроет..MyDb.kdb файл, используя MySecretPw как пароль). По умолчанию предполагается, что Командный файл находится, в том же каталоге (рабочий каталог) где и KeePass иначе Вы будете должны определить другой путь.

`START` выполняет данную командную строку и немедленно закрывается, не ожидая завершения работы приложения. Следовательно, окно командной строки после запуска KeePass исчезнет.

Пожалуйста, обратите внимание на две кавычки ("") после команды START. Эти кавычки требуются, если прикладной путь содержит кавычки (в примере выше, кавычки не нужны). Если Вы хотите больше узнать, о синтаксисе команды START, выполните START /? в окне командной строки.

Закрытие / блокировка KeePass с использованим пакетных файлов

Чтобы закрыть все выполняющиеся в настоящее время процессы KeePass, выполните KeePass.exe с параметром "--exit-all" :

```
KeePass.exe --exit-all
```

Все рабочие окна KeePass начнут закрываться. Если База данных была изменена, то KeePass спросит Вас, хотите ли Вы сохранить изменения или нет. Если Вы хотите сохранять в любом случае (т.е. без вызова Диалога подтверждения), допустить *"Автосохранение базы паролей"*, то отметьте флажком пункт в *меню "Инструменты" -> "Настройка' -> 'Расширенные' -> "Автосохранение базы паролей при выходе и заблокировании"*.

Например действие KeePass, которое было инициировано командой выше, не видимо (т.е. она не отображается в главном окне) и немедленно закрывается после отправки всех запросов.

KeePass ≥ 1,17 и ≥ 2,10 поддерживают параметры командной строки `--lock-all` и `--unlock-all` для блокировки / разблокировки рабочей области KeePass для всех других случаев.

Композитный (Составной) мастер ключ

На этой странице подробно описывается, как менеджер паролей KeePass Password Safe блокирует доступ к своим Базам данных.

- Мастер - пароли
- Ключевые файлы
- Использование Учетной записи пользователя Windows
- Для администраторов: Определение минимальных свойств мастер-ключей

KeePass хранит Ваши пароли в надежно зашифрованном файле (базе данных). Эта база данных заблокирована с помощью Мастер-пароля, Ключевого файла и / или Учетной записи пользователя Windows. Для разблокировки Базы данных, **все основные** источники (пароль, файл ключей, ...) **являются** обязательными. При совместном использовании, эти источники ключей формируют очень надежный ***Композитный Мастер ключ.***

KeePass не поддерживает альтернативное применение ключей, то есть абсолютно исключено, что Вы сможете открыть базу данных с помощью пароля **или** ключевого файла. Либо Вы используете пароль, либо ключевой файл, либо оба одновременно (если так предустановлено), взаимозаменяемость недопустима.

Мастер пароли

Если для открытия Базы данных, Вы используете только мастер-пароль, Вы должны хорошо помнить один пароль или парольную фразу (с высокой степенью надежности!). KeePass прекрасно вооружен защитными функциями против брутфорса (brute force) и атаки по словарю (dictionary attacks) на мастер-пароль, более подробно читайте об этом на странице информационной безопасности в KeePass .

Если вы забудете этот мастер-пароль, потеряются все Ваши пароли находившиеся в этой Базе данных. Не существует никаких бэкдоров или универсальных ключей, которыми можно было бы открывать базы данных. Не существует никакой возможности восстановления паролей.

Ключевые файлы

При использовании Ключевого файла, Вам не потребуется запомнание длинного, сложного Мастер ключа. База данных может быть заблокирована при помощи ключевого файла. Ключевой файл является основным Мастер-паролем только содержится он не в голове, а в файле. Ключевые файлы, как правило гораздо надежнее, чем Мастер пароли, потому как, ключик может быть гораздо более сложным, но с другой стороны его труднее содержать в тайне.

- Ключевой файл может быть использован *вместо* пароля, или в *дополнение* к паролю (или Учетной записи пользователя в Windows, KeePass 2.x).
- Ключевой файл может быть любым файлом по Вашему выбору, хотя рекомендуется выбрать один с *большим* количеством *случайных* данных.
- Ключевой файл не должен быть изменен, иначе это помешает открытию базы данных. Если Вы захотите использовать другой ключевой файл, Вам прийдется изменить главный ключ и использовать новый / другой ключевой файл.
- Для Ключевых файлов необходимо проводить резервное копирование, иначе вы не сможете открыть базу данных в случае отказа или модификации / восстановления жесткого диска.Это то же самое, как и забыть главный пароль. **Бэкдоров не существует.**

Не резервируйте ключевой файл в том же каталоге, что и Ваша база данных, используйте другой каталог, а лучше диск. Для проверки резервной копии, проведите тестовое открытие Вашей Базы данных на другом компьютере. Боле детальную информацию по резервному копированию ключевого файла и баз данных, см. ABP (Another Backup Plugin for KeePass) FAQ.

Смысл ключевого файла состоит в том, что вы *получили* что-то для аутентификации (в отличие от Мастер пароля, где вы что-то *знаете*), например, файл на USB Stick. Содержимое Ключевого файла (например данные ключей, содержащиеся в ключевом файле) необходимо держать в тайне. Дело *не* в том, чтобы сохранить тайну местонахождения Ключевого файла - Выбор файла из тысяч, имеющихся на вашем жестком диске в принципе не повысит безопасность (его легко найти для malware/attackers, например, путем наблюдения за доступом к файлам в последнее время). Попытка сохранить Ключевой файл в тайном месте не очень эффективна.

Только для KeePass 1.x
База паролей может быть закрыта с использованием ключ-диска. Ключ-диск - это

обычный диск, содержащий файл с байтами пароля. (KeePass может создать такой диск для Вас). Если Вы хотите, Вы также можете вручную выбрать ключ-файл (который будет сохранен на Вашем ключ-диске), один диск может хранить несколько ключей для нескольких баз паролей. В этом случае, Вам необходимо указать программе KeePass какой файл следует использовать, а не просто выбрать диск (когда Вы просто выбираете диск, программа KeePass предполагает, что ей следует загрузить *"pwsafe.key"* из корневого каталога диска).
Если Вы потеряете ключ-диск (или более точно ключ-файл) и не имеете резервной копии ключ-файла, Ваши пароли, хранящиеся в базе паролей, также можно считать потерянными. Это равносильно тому, что Вы забыли главный пароль.
Чтобы зарезервировать ключ-диск, проведите резервное копирование файла *"pwsafe.key"*, который хранится в корневом каталоге Вашего ключ-диска. Если ранее, Вы установили ключевой файл вручную (а не использовали файл по умолчанию - *"pwsafe.key"*), то Вам необходимо скопировать этот файл, а не *"pwsafe.key"*.

Конечно, KeePass может сгенерировать ключевые файлы для Вас, но Вы также можете использовать любой другой, уже существующий файл (например, изображений JPG, DOC документ и т.д.).

Только для KeePass 1.x
Для того, чтобы использовать существующий файл как ключевой файл, зайдите в диалоговое окно создания мастер-ключа и выберите "Сохранить присоединенный файл как ", выберите существующий файл. Приняв этот диалог, KeePass спросит, хотите ли перезаписать или повторно использовть файл. Выберите подходящий ответ. (см. скриншот).

Только для KeePass 2.x
Для того чтобы использовать существующий файл как ключевой файл, нажмите кнопку "Обзор", в окне диалога по созданию мастер-ключа.

Использование Учетной записи пользователя Windows

Только для KeePass 1.x
KeePass 1.x не поддерживает шифрование баз данных с использованием Учетной записи пользователя в Windows. Только KeePass 2.x и выше поддерживают эту функцию.

Только для KeePass 2.x
KeePass может создать базу данных в соответствии с текущей Учетной записью пользователя Windows. Если Вы включите эту опцию, то сможете открывать базы данных, только когда войдете в систему под той же Учетной записью Windows, что и при создании этих баз данных.

Вы спокойно можете изменять пароль, для своей учетной записи пользователя Windows. Это не повлияет на базу KeePass.

Будьте очень внимательны при использовании этой опции. Если будет удалена Ваша

учетная запись пользователя Windows, Вы больше не сможете открыть свою базу KeePass. Кроме того, при использовании этой опции на домашней системе и при выходе Вашего компьютера из строя (например повреждается жесткий диск), то будет недостаточно, просто создать новую учетную запись Windows при новой установке с тем же именем и паролем, Вам понадобиться скопировать полную запись пользователя (т.е. SID, ...). А это не простая задача, поэтому если Вы не знаете, как это сделать, то настоятельно рекомендуем Вам не использовать эту опцию.

Если Вы решаете использовать эту функцию, строго рекомендуются не полагаться (в плане безопасности) исключительно на нее, а дополнительно использовать одну из двух других опций (пароль или файл ключей).

Защита с помощью учетных записей пользователей поддерживается в Windows 98 / ME.

 Для Администраторов: Определение Минимальных Свойств Главных мастер-ключей

Администраторы могут указывать минимальную длину и / или минимальную оценку качества, для применяемых паролей. Вы можете установить KeePass проверку этих двух минимальных требований путем добавления / редактирования соответствующих записей в INI / XML файлах конфигурации.

Только для KeePass 1.x
Значение параметра ключа `KeeMasterPasswordMinLength` может содержать минимальную длину мастер пароля в символах. Например, установив `KeeMasterPasswordMinLength=10`, KeePass будет работать с паролями, имеющими не менее 10 символов.

Значение параметра ключа `KeeMasterPasswordMinQuality` может содержать минимальную оценку качества пароля в битах. Например, задав `KeeMasterPasswordMinQuality=64` будут разрешаться только пароли с оценкой качества по меньшей мере в 64 бита.

Только для KeePass 2.x
Значение `MinimumLength` в настройках `Security/MasterPassword` может содержать минимальную длину пароля в символах. Например, установив это значение равным `10-ти`, KeePass будет принимать только пароли, имеющие не менее 10 символов.

А значение `MinimumQuality` в настройках `Security/MasterPassword` может содержать минимальную оценку качества пароля в битах. Например, установив это значение равным `32`, будут приниматься только пароли с оценкой качества по меньшей мере в 32 бита.

В KeePass ≥ 2,10, указав `KeyCreationFlags` и / или `KeyPromptFlags` (в узле `UI`) Вы можете задействовать различные состояния (включить, отключить, проверять, непроверять) параметров контроля ключей, создание и оперативные диалоги. Эти значения могут быть поразрядными комбинациями, одного или более из следующих флажков:

Флаг (Hex)	Флаг (Dec)	Описание
0x0	0	Не определяет никаких действий (по умолчанию).

0x1	1	Включить пароль.
0x2	2	Включить ключевой файл.
0x4	4	Включите учетную запись пользователя.
0x100	256	Отключить пароль.
0x200	512	Отключить ключевой файл.
0x400	1024	Отключить учетную запись пользователя.
0x10000	65536	Проверка пароля.
0x20000	131072	Проверка ключевого файла.
0x40000	262144	Проверка учетной записи пользователя.
0x1000000	16777216	Непроверять пароль.
0x2000000	33554432	Непроверять ключевой файл.
0x4000000	67108864	Непроверять учетную запись пользователя.

Например, если Вы захотели бы обеспечить использование опции "Учетная запись пользователя", то могли бы включить проверку и контроль (таким образом, что пользователь больше не сможет непроверить это) 263168, указав в качестве значения (0x40000 + 0x400 = 0x40400 = 263168).

Установки и настройки Конфигураций для KeePass

Здесь Вы найдете подробную информацию о возможностях используемых в KeePass файлах конфигураций, узнаете об их использовании, настройках и местах их расположения в системе.

В зависимости от условий применения, Менеджер паролей KeePass Password Safe, использует несколько мест для хранения информации о конфигурации:

- *Global - глобальный файл* конфигурации, располагается в каталоге приложения KeePass,
- *Local - локальный файл* конфигурации, находится в личной папке, Конфигурации пользователя,
- *Enforced - принудительный файл* конфигурации, расположен в каталоге приложения KeePass

Первый из них называется *Global* (*глобальным),* потому что все, кто использует эту установку KeePass будут записывать данные в этот файл конфигурации (и, возможна, перезапись с настройками других пользователей). Второй называется *Local* (*местным),* потому что все изменения, произведенные в этом файле конфигурации, затрагивают только текущего пользователя. Третий называется *Enforced* (*принудительный) и* используется в основном сетевыми администраторами.

Только для KeePass 1.x
Конфигурационные файлы хранятся в формате INI.

Конфигурация	Расположение	Типичный путь к файлу
Global	Application Directory	C:\Program Files\KeePass Password Safe\KeePass.ini
Global (Virtualized)	Windows Vista/7 Virtual Store	C:\Users*User Name*\AppDataLocal\VirtualStore\Program Files\KeePass Password Safe\KeePass.ini
Local	User Application Data	C:\Documents and Settings*User Name*\Application Data\KeePass\KeePass.ini
Enforced	Application Directory	C:\Program Files\KeePass Password Safe\KeePass.enforced.ini

Только для KeePass 2.x
Конфигурационные файлы хранятся в формате XML.

Конфигурация	Расположение	Типичный путь к файлу
Global	Application Directory	C:\Program Files\KeePass Password Safe\KeePass.config.xml
Global (Virtualized)	Windows Vista/7 Virtual Store	C:\Users\ *User Name* \AppDataLocal\VirtualStore\Program Files\KeePass Password Safe\KeePass.config.xml
Local	User Application Data	C:\Documents and Settings\ *User Name* \Application Data\KeePass\KeePass.config.xml
Enforced	Application Directory	C:\Program Files\KeePass Password Safe\KeePass.config.enforced.xml

Установка Администратором, использование Пользователем

Если, при установке KeePass, Вы будете использовать инсталлятор и установите программу с правами администратора, то каталог программы будет защищен от записи, как в режиме нормальных пользовательских ограничений. KeePass будет использовать Local (местные) файлы конфигурации, то есть сохранять и загружать конфигурационный файл в Вашем пользовательском каталоге.
Возможно многопользовательское использование, локально установленным KeePass. Параметры конфигурации не будут публиковаться и могут быть настроены индивидуально для каждого пользователя.

Портативная (Portable) версия

Если Вы, решили скачать и установить *portable* версию KeePass (ZIP архив), KeePass постарается использовать для хранения файлов своей конфигурации, каталог с установленным приложением. Параметры конфигурации не будут сохранятся в каталог пользователя (если глобальный файл конфигурации будет доступен для записи).

Создание Portable версии из установленного локально KeePass

Если вы используете локально установленную версию KeePass (установка KeePass с помощью Windows Installer EXE) и Вам захочется создать вариант portable, во-первых загрузите файлы KeePass для переносной (portable) версии. Затем скопируйте файл конфигурации из локального каталога пользователя (расположение конфигурационного файла, см. выше) и вставьте это файл конфигурации в KeePass portable.

Для сетевых администраторов: Принудительная Конфигурация

В некоторых случаях, специальные параметры конфигурации KeePass могут быть загружены принудительно. Принудительные настройки конфигурации загружаются из файлов: `KeePass.enforced.ini` (в KeePass 1.x) и `KeePass.config.enforced.xml` (в KeePass 2.x), которые находятся в каталоге с установленным `KeePass.exe`.

Элементы настроек, которые не присутствуют в параметрах файла Enforced, обычно загружаются из глобальных/локальных файлов конфигурации.

Обратите внимание, что этот метод является эффективным, если пользователи работают с KeePass, установленном на сетевом диске. Если пользователи загружают KeePass на свои жесткие диски и оттуда же его и запускают, то принудительные параметры не применяются (в этом случае, локально установленный KeePass ничего не знает о принудительном файле конфигурации на сетевом диске).

Техническая информация

В этом параграфе объясняется, как производится загрузка и сохранение Конфигураций.

При запуске KeePass проверяет, как глобальные, так и локальные конфигурационные файлы, одновременно устанавливается порядок, в котором KeePass будет загружать настройки элементов. Это контролируется выставлением флага для ключа `PreferUserConfiguration`, в глобальном файле конфигурации. Если его нет, то по умолчанию функция *ложна.*

Если флаг *включен,* в глобальном файле конфигурации установщика пакетов KeePass. А портативный (portable) ZIP-архив не содержит файла конфигурации, тогда по умолчанию значение флага *ложно.*

Только для KeePass 1.x
Загрузка:

- Постарайтесь настроить конфигурацию элементов из принудительного файла конфигурации. Если он установлен, используйте эго.
- Если элемент не представлен ни в *глобальном* файле конфигурации, ни в *локальном* то: Соотношение используется по умолчанию.
- Если элемент присутствует в *глобальном* файле конфигурации, но не в *локальном* то: используются настройки из глобальной конфигурации.
- Аналогично, если настройки находятся в *локальном* файле конфигурации, но не представлены в *глобальном* то: используется элемент из *локальной* конфигурации.
- Если же элемент настроек присутствует и в глобальном и в местном конфигурационном файле тогда:
    - Если включен флаг `KeePreferUserConfiguration`, использовать эти настройки из *локального* файла конфигурации, в противном случае использовать из *глобальной*.

Сохранение:

- Если включен флаг `KeePreferUserConfiguration`, то будем сохранять параметры конфигурации в *локальном* файле конфигурации. Если это не удается, попробуем сохранить параметры в глобальном файле конфигурации. Если и это не удается, то сообщаем об ошибке.
- `Если же флаг для KeePreferUserConfiguration` *выключен*, попробуем сохранить настройки в глобальном файле конфигурации. Если это не удается, попытаетемся сохранить эти настройки в локальном файле конфигурации. Если и это не удается, то сообщаем об ошибке.

Только для KeePass 2.x
Загрузка:

- Постарайтесь установить конфигурацию элементов из принудительного (enforced) конфигурационного файла. Если он установлен, используйте эго.
- Если включен флаг `PreferUserConfiguration`, используйте настройки из локального файла конфигурации, в противном случае используйте из глобального. Если же глобальных, так же не существует или они не содержат настроек то используется конфигурация по умолчанию.

Сохранение:

- Если флаг `PreferUserConfiguration` *включен,* старайтесь сохранять все элементы настроек в локальном файле конфигурации. Если это не удается, попытайтесь сохранить их в глобальном файле конфигурации. Еже ли и это не удается, просим Вас сообщить об ошибке.
- Если флаг `PreferUserConfiguration` *выключен,* постарайтесь сохранять все параметры в глобальном файле конфигурации. Если это не удается, постарайтесь сохранить их в локальном файле конфигурации. Ну а если и здесь потерпите неудачу, то Пожалуйста, непременно сообщите нам об ошибке.

Поля и Ссылки

Использование Полей и Ссылок
или
Как разместить ссылки на ресурсы в информационные поля других Акаунтов.

Введение

Менеджер паролей KeePass может вставлять сохраненные данные, в поля различных Аккаунтов. Это означает, что несколько различных записей могут использовать общие поля (имя пользователя, пароль, ...), таким путем изменяя фактический ввод данных, все остальные Аккаунты также будут использовать новые параметры.

Чтобы создать поле ссылки, вы можете использовать удобного мастера поля ссылки (в окне редактирования Входа, в левом нижнем углу, нажмите кнопку "Инструменты" и выберите "Вставить ссылку на поле'), или ввести заполнитель вручную (см. синтаксис ниже).

Синтаксис заполнителя

Синтаксис заполнителя для полей ссылок выглядит следующим образом:

`{REF:<WantedField>@<SearchIn>:<Text>}`

Части *WantedField* и *SearchIn* должны быть заменены 1-буквенными кодами, отождествляющими поля:

Код	Поле
T	Название
U	Имя пользователя
P	Пароль
A	URL
N	Заметки
I	UUID
O	Другие пользовательские строки *(только в KeePass 2.x)*

Часть *Text* представляет собой строку поиска, т.е. этот текст должен встречаться в указанной области соответствующего входа.

Если по указанному критерию поиска будет найдено несколько соответствий, то использоваться будет, первая запись. Чтобы избежать двусмысленности, записи могут быть идентифицированы по UUID, который, в свою очередь, уникален.. Пример: `{REF:P@I:46C9B1FFBD4ABC4BBB260C6190BAD20C}` вставит пароль для Входа используя 46C9B1FFBD4ABC4BBB260C6190BAD20C как UUID.

Только для KeePass 2.x
Ссылки на поля других записей работает только со стандартными полями, а не с заметками пользователя. Используя код `O` можно заставить KeePass искать поля с пользовательскими заметками (чтобы идентифицировать упоминаемый исходный Вход), но `O` не может быть использован для получения данных из пользовательских полей (т.е. код не может быть использован в качестве *WantedField).* Если вы хотите сослаться на строку пользовательских настроек, вам необходимо поместить перенаправление в стандартное поле с помощью `{S:<Name>}` а также ссылку на стандартное поле.

Пользовательские строки могут локально (то есть в пределах входа) ссылаться с помощью `{S:<Name>}`, за подробностями идем смотреть Автозаполнение Auto-Type (которое также работает в буфере обмена и с URL операциями).

Примеры

Предположим, у нас есть два аккаунта: один назовем "Mozilla Website" а другой пусть будет "Mozilla Forums", и необходимо вставить имя пользователя из учетной записи Website в URL аккаунта Forums. В URL записи Forums, мы могли бы обратиться к имени пользователя следующим образом:
`http://fictitious-forum.mozilla.org/?user={REF:U@T:Mozilla Website}`

Импорт / Экспорт

KeePass поддерживает импорт и экспорт данных из/в различные форматы файлов.

KeePass 1.x поддерживает импорт данных из **файлов CSV** (спец. форма), **CodeWallet, Password Safe,** и **Personal Vault.**

KeePass 2.x поддерживает импорт данных из **файлов CSV** (все), **KeePass 1.x (КДБ, XML и CSV), KeePass 2.x XML, 1Password Pro, Alle Meine Passworte, Any Password, CodeWallet, FlexWallet, Handy Safe, Handy Safe Pro, KeePassX, Mozilla Bookmarks PassKeeper, Passphrase Keeper, Password Agent, Password Depot, Password Exporter, Password Gorilla, Password Keeper, Password Memory, Password Safe, Passwort.Tresor, Personal Vault, PINs, RoboForm, Security TXT, CSV SplashID** , **Steganos Password Manager 2007, Whisper 32, ZDNet's Password Pro** и **Spamex.com.**

Для обоих версий KeePass 1.x и 2.x, существуют плагины, которые расширяют возможности программы по импорту файлов различных форматов.

- Для KeePass 1.x:
  - Формат файла: CSV
  - Формат файла: XML
- Для KeePass 2.x:
  - Универсальный инструмент для импорта CSV
  - Форматы, для импорта которых, пользователю необходимо предпринять некоторые настройки/шаги :
    - Как импортировать CodeWallet TXT 6,05
    - Как импортировать Password Gorilla CSV 1,42
    - Как импортировать PINs TXT 4,50
    - Как импортировать данные из RoboForm
    - Как импортировать данные из Steganos Password Manager 2007
    - Как импортировать данные из PassKeeper 1,2
    - Как импортировать 1Password Pro CSV

К сожалению, не существует стандартного формата для баз данных паролей. Каждый менеджер паролей использует файлы своего собственного формата. Так или иначе, почти все хранители паролей поддерживают экспорт БД в CSV или XML-файлы. На первый взгляд, это кажется не плохим вариантом, но CSV, и XML-файлы не предназначены для специализированных форматов Баз Данных паролей, они отображают низкоуровневневую разметку хранимых данных (в файлах CSV: поля данных разделяются запятыми; а в файлах XML: иерархия определяется тегами). Эти форматы не поддеживают специфику

высокоуровневого расположения данных (для CSV: порядок/значение полей; для XML: название тегов и структуру). Из-за этого многие пользователи оказываются в недоумении, когда приложение №1 экспортирует данные в файл CSV/XML а приложение №2 не может считать данные из CSV/XML файла, хотя утверждается, что файлы данного типа поддерживаются обоими программами.

На этой сраничке мы поподробнее рассмотрим форматы CSV и XML файлов. Зная форматы, которые использует KeePass, можно отредактировать CSV и XML-файлы, экспортируемые из других менеджеров паролей, чтобы привести в соответствие с требованиями KeePass. Файлы CSV могут быть переформатированы, с помощью OpenOffice Calc (см. ниже). XML-файлы могут быть переформатированы, с помощью XML-редактора.

KeePass может импортировать пароли из баз данных разичных программ (см. вверху этой страницы). Кроме того, для расширения возможностей по импорту БД различных форматов, существуют специализированные плагины KeePass (например, AnyPassword CSV, Oubliette files, PINs TXT, ZSafe files, и многие другие...). Используя эти плагины, Вам не придется вручную переформатировать данные полученые из других менеджеров паролей; вы можете сразу импортировать, экспортированные файлы

Если вы не смогли найти плагин для импорта данных из предыдущего менеджера паролей, то можете разместить запрос на KeePass Feature Requests и / или на форуме Open Discussion.

Файл формата: CSV (KeePass 1.x)

KeePass, импортирует и экспортирует данные CSV файлов, в следующем формате:

```
"Account","Login Name","Password","Web Site","Comments"
```

Для большей наглядности, можете скачать и просмотреть этот файл: FileSample_CSV.zip . Данный файл заархивирован только для того, чтобы обеспечить сохранность правильной кодировки (если не архивировать, то браузеры и менеджеры загрузок, могут автоматически преобразовать файл в другую кодировку). Однако, при импортировании файла CSV в хранитель KeePass, он *не* должен находиться в архиве!

Важная информация о формате:

- Файл должен быть закодирован с использованием UTF-8 (Unicode). Другие кодировки не поддерживаются.
- В CSV файле поддерживают только следующие поля: название, имя пользователя, пароль, URL и заметки. Другие же поля, такие как дата последнего изменения записи, срок действия, иконки, прикрепленные файлы и т.д. *не* поддерживаются. Если вы захотите передать и такую информацию, то потребуется использовать другой формат (например, XML).
- Все поля должны быть заключены в кавычки ("). Это условие является обязательными, поля без кавычек недопустимы.
- Кавычки (") в строках кодируются так `\"` (двумя знаками). Обратный слэш (\) кодируется как `\\` .

- Многострочный комментарий реализуется с помощью обычных строк. Использование в кодировке строк `\n` не поддерживается.

По умолчанию, Microsoft Excel не заключает поля в кавычки ("). Для создания правильного файла CSV, рекомендуется использовать OpenOffice Calc (см. ниже), или использовать Универсальный инструмент для импорта CSV в KeePass 2.x (импортировать CSV файл в KeePass 2.x, а затем экспортировать данные в файл KDB для KeePass 1.x), или же исправить файл CSV вручную добавив кавычки с помощью текстового редактора.

Если вы хотите передавать данные между БД KeePass 1.x, вы не должны менять установленные по умолчанию параметры экспорта из KeePass. Не экспортируйте дополнительные поля и снимите флажки у других доп. настроек, в противном случае KeePass не сможет повторно импортировать файл CSV, потому что он более не будет соответствовать спецификации.

Использование *OpenOffice Calc* для создания CSV файла:
OpenOffice Calc - табличный процессор на подобии MS Exel, входящий в состав OpenOffice.org может быть использован для создания CSV файлов, которые в последствии могут быть корректно импортированы в хранитель паролей KeePass. И так, выполните следующие действия:

- Убедитесь, что вы получили 5 столбцов как описано выше.
- Выделите все колонки, щелкните правой кнопкой мыши и выберите пункт *"Формат ячеек.* В открывшемся диалоговом окне выберите категорию *Текст*. Нажмите кнопку [OK].
- Теперь, выберите *'Файл' -> 'Сохранить как...'* , выберите место и убедитесь, что флажок *"Изменить настройки фильтра"* включен. Нажмите кнопку *"Сохранить"* .
- Выберите и установите кодировку набора символов *'Unicode (UTF-8)'* . Разделителем поля должен быть установлена запятая, а разделителем текста должна быть `"` . Убедитесь в том, что флажок *Фиксированная ширина колонки* не установлен. Нажмите кнопку [OK].

Файл формата: XML (KeePass 1.x)

В этом разделе описывается XML формат для KeePass 1.x. Обратите внимание, что этот формат отличается от формата XML используемого в KeePass 2.x (однако, KeePass 2.x можете импортировать XML-файлы из KeePass 1.x).

Подробный пример XML файла, Вы можете скачать здесь: FileSample_XML.zip . Данный файл помещен в архив с целью сохранения его оригинальной кодировки (как вы знаете, браузеры и даунлоадеры, могут автоматически изменить кодировку файла). Однако запомните, при импорте, XML-файл не должен находится в архиве!

Важная информация о формате:

- Файлы должны кодироваться с использованием UTF-8 (Unicode). Другие кодировки не поддерживаются.

- Следующие пять значков должны быть закодированы: `< > & " '` . Кодируются они так `< > & &quot; &apos;` .
- UUID представляет собой шестнадцатерично кодированную 16-байтную строку (т. е. 32 ANSI шестнадцатеричную строку символов в файле XML). Он уникален (даже между несколькими базами данных) и может быть использован для идентификации записей.
- Дата/время кодируется в стандарте XML формата даты/времяни (YYYY-MM-DDTHH:mm:ss): первой идет дата в виде YYYY-MM-DD, символ 'T', и время в виде HH:mm:ss.

Универсальный инструмент для импорта CSV

KeePass 2.x поставляется с универсальным импортёром CSV. Этот инструмент может импортировать в KeePass практически все форматы CSV. Файлы CSV загружены, и вы можете вручную указать кодировку/набор символов, назначить колонки для полей данных, а также указать, каким образом выглядит низкоуровневая структура данных (использование кавычек и т.п.).

Для запуска, Универсального инструмента для импорта CSV-файла, выберите *"Файл"* - *"Импорт....>"* и в открывшемся меню, выберите *"Общий импортер CSV*.

Как импортировать CodeWallet TXT 6,05

CodeWallet это менеджер паролей, поддерживающий различные типы карт (полей). KeePass не может знать, какие поля из CodeWallet соответствуют стандартным полям KeePass (название, имя пользователя, ...), так как они не имеют фиксированных названий (зависит от языка, настроек пользователя, ...). Поэтому все поля из файла CodeWallet импортируются в настраиваемые строки полей записи KeePass. После импорта файла, вы можете правильно переместить строки в стандартные поля (нажав кнопку *"Move/Отправить"* на второй вкладке в диалоге записи.

Как импортировать Password Gorilla CSV 1,42

Для того, чтобы успешно импортировать CSV файл из Password Gorilla, вам потребуется произвести некоторые настройки. Открываем Password Gorilla заходим в*'File - Preferences - Export'* и настраиваем следующие параметры :

- Включить *'Include password field'* .
- Включить *'Include notes field'* .
- Включить *'Save as Unicode text file'* .
- Установить разделитель полей в 'µ' (mu, нажать AltGr + M).
- Убедитесь, что вы не используете символ 'µ' где нибудь в вашей Базе Данных паролей.

Когда вы правильно выставите эти параметры, то экспортируйте данные в CSV файл, а за тем импортируйте его в KeePass с помощью команды *"Файл -> Импорт" в* KeePass 2.x.

Как импортировать PINs TXT 4,50

Для того, чтобы успешно импортировать файл PINs TXT, Вам необходимо сделать следующее:

- Переключить язык PINs на 'English'.

- В диалоге экспорта PINs: Включить *all* fields.
- В диалоге экспорта PINs: Установить разделитель *'tab'* .
- В диалоге экспорта PINs: Включить *'Quote texts'* .

После экспорта TXT файла с вышеуказанными настройками, импортируйте его с помощью *"Файл -> Импорт" в* KeePass 2.x.

Как импортировать данные из RoboForm

Прежде всего, необходимо экспортировать Пасскарты RoboForm-а в файл HTML. Для этого откройте RoboForm, а в нем *Редактор Пасскарт (*Windows => меню Пуск =>*'Edit Passcards'*), далее в основном меню редактора идёте *'Passcard' -> 'Print List'* . В открывшемся диалоговом окне, нажмите *на* кнопку *"Сохранить"*. Выберите место сохранения и имя файла, за тем нажмите кнопку *"Сохранить"*.

Откройте файл базы данных KeePass 2.x и перейдите *'Файл' =>'Импорт'* . Укажите в качестве формата *'RoboForm HTML'* и выберите файл HTML который вы только что экспортировали, а затем нажмите *'OK'*.

Как импортировать данные из Steganos Password Manager 2007

Внимание! Не исключена вероятность ошибки при передаче данных. Существует возможность того, что KeePass случайно перезапишет существующие пароли в Steganos Password Manager. Поэтому, перед началом импорта, создайте резервную копию файла SEF! В любом случае вы сможете восстановить ваши пароли, после неудачного импорта, восстановив только что созданную резервную копию! Даже если вы посчитаете, что KeePass ничего не изменил, все равно произведите восстановление из резервной копии!

К сожалению, в Steganos Password Manager (SPM) не хватает функционала для экспорта базы данных паролей. А поскольку формат файла SEF (в котором хранятся данные)

является частным, и никакая спецификация не доступна, то KeePass необходимо попытаться получить все данные из окон SPM.

Процесс извлечения базы паролей, будет происходить следующим образом. Сначала Вы запускаете SPM и открываете Вашу базу данных паролей. Основное окно управления паролями должно быть открытым (т.е. то, где представлен список записей в центре экрана и панели кнопки в верхней части). Убедитесь, что все Ваши записи отображены в списке (выберите правильный фильтр в выпадающем списке).

Теперь, переключитесь на KeePass 2.x и откройте базу данных KeePass. Открываете *"Файл -> Импорт"* и выбираете *Steganos Password Manager 2007*. Жмёте кнопку [OK]. Прежде чем продолжить извлечение паролей, внимательно ознакомьтесь с дальнейшей инструкцией.

После нажатия на кнопку [Yes] в диалоговом окне подтверждения импорта KeePass, у вас есть 10 секунд, чтобы перейти к окну SPM. Выберите самую первую запись в окне *Steganos Password Manager 2007* (но не открывайте, просто выберите её). Это важно! Первая запись должна иметь клавиатурный фокус и должна быть выбрана.

После окончания 10 секундной паузы, KeePass начнет импортировать записи. Вы увидите, как KeePass открывает SPM запись, копирует данные, закрывает окно элемента, выбирает следующую запись и т.д. Все происходит автоматически и теперь вы можете просто посидеть сложа руки и посмотреть. Иногда, Windows издает звук *"динь*", это нормально.

Обратите внимание, что импортирование записей может занять довольно много времени. **Не делайте** ничего, пока KeePass занимается импортом базы паролей! Одного щелчка мышью или нажатия клавиши, может оказаться достаточно, что бы испортить весь процесс импорта.

Последний пункт в списке записей, будет проверяться дважды. По окончанию работы, KeePass покажет сообщение "Процесс импорта завершен!".

Вполне возможно, что KeePass не удасться импортировать некоторые элементы (в основном, это вызвано непредсказуемо медленным реагированием Steganos Password Manager). Ну а в заключении, настоятельно порекомендуем вам, проверить каждую из импортированных записей.

Как импортировать данные из PassKeeper 1,2

Процесс импорта, визуально работает так же, как и метод импорта данных Steganos Password Manager. Пожалуйста прочитайте все инструкции в разделе для импорта данных из Steganos Password Manager.
Пожалуйста, прочтите эти инструкции Как импортировать данные из Steganos Password Manager 2007

Как импортировать 1Password Pro CSV

KeePass может импортировать CSV файлы, экспортируемые 1Password Pro.
При экспорте данных, убедитесь, что:

- Все поля, должны быть экспортированы.
- Выберите табуляцию (Tab), в качестве разделителя полей.
- Опция для окружения поля в кавычки, должна быть включена.

Интеграция

Как KeePass интегрируется в среду Вашей операционной системы.

Глобальные горячие клавиши для восстановления окна KeePass

Чтобы быстро переключиться от сторонней программы к хранителю паролей KeePass, вы можете использовать глобальные горячие клавиши, с помощью которых восстанавливается главное окно программы KeePass.

Если у вас, одновременно работает несколько экземпляров KeePass, то при нажатии глобальных горячих клавиш, будет восстановлено главное окно первого запущенного экземпляра.

Глобальные горячие клавиши - **Ctrl-Alt-K.**

Только для KeePass 1.x
Комбинацию горячих клавиш изменить нельзя, однако её можно отключить в настройках дополнительных параметров.

Только для KeePass 2.x
Комбинация горячих клавиш, может быть свободно изменена в различных вариантах (или отключена) в диалоговом окне "Настройки", на вкладке "Интеграция".

Ограничение на количество запущеных экземпляров

Если вы активизируете опцию *'Limit to Single Instance'* , то включиться запрет на запуск более одного экземпляра KeePass одновременно. Если же при этом, вы все равно попытаетесь запустить второй экземпляр KeePass, то запуск будет прекращен, а на первый план будет выведен уже работающий Хранитель паролей.

Только для KeePass 1.x
Если второй экзмпляр KeePass был запущен с помощью командной строки и с указанием базы данных для открытия, а первый (уже работающий) экземпляр не имеет открытых диалоговых окон, то Первый попытается закрыть текущую базу данных. Если эта попытка увенчалась успехом (или же, если не было открытой базы данных), тогда первый экземпляр открывает базу данных указанную при запуске второго экземпляра, используя такие параметры коммандной строки `-pw` или `-keyfile`. Все остальные параметры командной строки, при этом игнорируются.

Совместное использование KeePass

Многопользовательский режим

Подробная информация об особенностях совместного использования KeePass.

- **Совместное Использование и Редактирование Баз Данных:**
  - Общая информация о Совместо используемых Базах данных
  - KeePass 1.x: Офис-Стиль Блокировка
  - KeePass 2.x: Синхронизация или Замена

Общая информация о Совместно используемых Базах данных

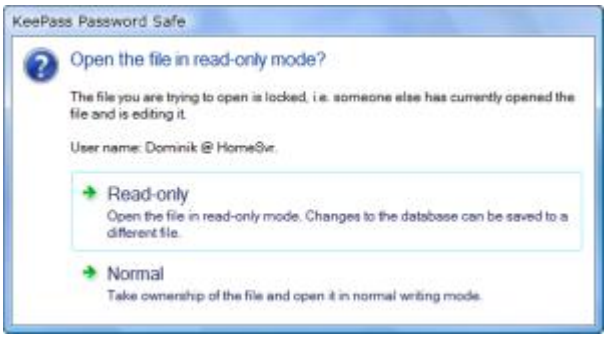
Оба KeePass, как 1.x, так и 2.x позволяют нескольким пользователям работать с одной базой данных, которая обычно хранится на сетевом диске или файловом сервере.

Все пользователи используют один Мастер-пароль и / или ключевой файл, для доступа к базе данных. Нет никаких списков по управлению контролем доступа, по записям или по группам (ACLs).

Для ограничения доступа на запись к файлу базы данных (то есть, только избранная группа пользователей, может изменить хранимые данные), используйте права доступа файловой системы.

KeePass 1.x: Офис-Стиль Блокировка

С KeePass 1.x, базы данных могут быть сохранены на сетевом диске и использоваться несколькими пользователями. Когда пользователь попытается открыть базу данных, которая уже кем-то открыта, появится запрос, открывать ли базу данных только для чтения или открыть в нормальном режиме (см. фото справа).



При открытии Базы данных в обычном режиме, текущий пользователь получает право собственности на файл (например, последующие попытки открытия покажут текущего пользователя в качестве владельца).

KeePass 1.x не обеспечивает синхронизацию, то есть сохраняя базу данных, Вы сохраняете на диск, свои текущие данные. Если другой пользователь, в это время, изменил запись (то есть, с уже загруженной базой данных), эти изменения будут перезаписаны.

Если вы хотите использовать KeePass 1.x с базой данных установленной на сетевом диске, то рекомендуется установить, права на запись файла БД только для администратора, а остальным пользователям разрешить только чтение (это можно обеспечить с помощью системы прав доступа к файлу). При использовании переключателя коммандной строки -readonly, KeePass автоматически откроет доступ к базе данных в режиме только для чтения (т.е. не покажет подсказку выбора режима запуска). Пользователи будут открывать Базу данных, используя ярлык, который уже содержит этот переключатель командной строки.

Если нет администратора осуществляющего центральное управление Базой Данных, пользователи должны быть очень осторожны, чтобы не переписывать друг другу изменения.

KeePass 2.x: Синхронизация или Перезапись

В KeePass 2.x, база данных может быть сохранена на совместно используемом сетевом диске и использоваться многочисленными пользователями. При попытке сохранить данные, KeePass сначала проверяет, был ли файл на диске изменен с тех пор, как был загружен. Если да, то KeePass спрашивает, синхронизировать или перезаписать файл, или же оставить без изменений (см. рисунок справа).

При синхронизации, изменения внесенные другими пользователями (файл на диске) и изменения, внесенные текущим пользователем будут объединены. После завершения процесса синхронизации, текущий пользователь так же видит изменения, сделанные другими (т. е. данные в текущей базе KeePass, являются современными).

При возникновении конфликта (когда несколько пользователей редактировали одну Запись), KeePass использует самую последнюю версию входа, основанную на последнем времени модификации.

Примечание: Оперативная синхронизация происходит только по команде "*Сохранить*", а не по команде *"Сохранить как*". При выполнении команды "*Сохранить как*" и выборе файла вручную, этот файл всегда будет Перезаписан.

Генератор паролей

Здесь, мы детально рассмотрим встроеный в KeePass генератор паролей, примеры и варианты его использования, наборы стандартных команд и различные способы конфигурации.

- Генерация Паролей, основанная на Наборах Символов
- Генерация Паролей, основанная на Шаблонах
- Генерирование Паролей по предопределенным Правилам
- Функции снижающие Надежность Пароля
- Создание и использование Профилей для Генератора паролей
- Конфигурирование настроек, Автоматического Генерирования паролей для Новых Записей

Описание Генерации Паролей базирующейся на Наборах Символов

Данный метод генерации пароля, является рекомендуемым способом для генерирования случайных паролей. Другие методы (генерация основанная на Шаблоне ...) должны использоваться только тогда, когда пароли необходимо создавать следуя заранее установленным правилам или выполняя определенные условия.

Метода генерации паролей, основанная на наборе случайных символов, очень проста. Вы просто сообщаете KeePass, какие символы могут быть использованы (то есть прописные буквы, цифры...), и KeePass в произвольном порядке выберет символы из обозначенного набора.

Определение Набора Символов:
Набор символов может быть задан непосредственно в окне генератора пароля. Для удобства, KeePass предлагает добавить в набор, наиболее используемые диапазоны символов, а Вы просто, отмечаете флажком соответствующий чекбокс. Дополнительно к этим предопределенным диапазонам символов, можно назначать символы вручную: Все символы, которые Вы введёте в поле окна редактирования "Также, использовать следующие символы" , будут непременно добавлены в общий набор символов.

Наборы символов являются Наборами:
В математических терминах наборы символов являются именно Наборами. Это означает, что символы не могут быть добавлены в набор дважды. Или символ находится в наборе, или его там нет.

Например, если Вы, в поле для дополнительных символов, вводите набор "AAAAB" это будет точно соответствовать набору "AB". Если Вы хотите, что бы в сгенерированом пароле символ "A" встречался в 4 раза чаще, чем "B", то вам следует использовать генерацию основанную на Шаблоне + перестановку символов.

KeePass "оптимизирует" Ваш набор символов, удаляя все двойные символы. Для эксперемента, Вы можете ввести сочетание символов "AAAAB" в дополнительное поле, а за тем закрыть и вновь открыть Генератор Пароля и вы увидите, что в поле остались, только символы "AB". Точно так же, если Вы поставите флажок в чекбокс "Цифры" , а в дополнительное поле введёте "3", то эта цифирь '3' будет проигнорирована, потому что уже включена в основной диапазон символов "Цифры".

Описание Генерации Паролей основывающейся на Шаблонах

Генератор пароля, может создавать пароли используя Шаблоны. Шаблон является строкой, определяющей условия формирования нового пароля.

Заполнитель	Тип	Наборы символов

a	Алфавитно-цифровой нижний регистр	abcdefghijklmnopqrstuvwxyz 0123456789
A	Алфавитно-цифровой смешанный регистр	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
U	Алфавитно-цифровой верхний регистр	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
c	Согласные буквы нижний регистр	bcdfghjklmnpqrstvwxyz
C	Согласные буквы смешанный регистр	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz
z	Согласные буквы верхний регистр	BCDFGHJKLMNPQRSTVWXYZ
d	Цифры	0123456789
h	Hex (шестнадцатиричные) символы нижний регистр	0123456789 abcdef
H	Hex (шестнадцатиричные) символы верхний регистр	0123456789 ABCDEF
l	Строчные буквы (нижний регистр)	abcdefghijklmnopqrstuvwxyz
L	Строчные и Заглавные буквы (смешанный регистр)	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
u	Заглавные буквы (верхний регистр)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
p	Пунктуация	, . ; :
b	Скобки	() [ ] {} <>
S	Печатуемые 7-Bit ASCI символы	A-Z, a-z, 0-9, !"#$%&'()*+,-./:;<=>?[]^_{|}~
v	Строчные гласные	aeiou
V	Смешанные (Заглавные и Строчные) гласные	AEIOU aeiou
Z	Заглавные гласные	AEIOU

`x`	High ANSI	начиная с '~' и по U255 (за исключением U255)
`\`	Escape (Fixed Char)	Использование следующих символов, как есть
`{ n }`	Escape (Repeat)	Повтор предыдущего символа *n* раз
`[ ... ]`	Установка Пользовательского набора символов	Назначение пользовательского набора символов

Специальный заполнитель \ : это - знак перехода. Символы, следующие за знаком \, будут непосредственно вписаны в сгенерированный пароль. Если вы хотите вставить символ \ в определенное место вашего пароля, вам потребуется написать \ \ .

Использование кода **{ *n* }** , поможет определить, сколько раз предстоящий заполнитель должен быть применён, при формировании пароля. А с помощью оператора **{ }** определяется количество повторов заполнителя, а не его генерирования. Например:

» `d{4}` эквивалентно `dddd`,
» `dH{4}a` эквивалентно `dHHHHa`
» `Hda{1}dH` эквивалентно `HdadH`.

Нотация **[...]** может быть использована для определения пользовательского набора символов, из которых генератор паролей выберет один символ случайно. Все символы между **[** and **]** скобками подчиняются тем же правилам, что и заполнители выше. Например:

» `[dp]` в генерации участвует только 1 случайный символ из данного набора + пунктуация,
» `[dm@]{5}` в генерации участвуют 5 символов из набора "0123456789m@",
» `[u_][u_]` для генерации берется 2 символа в верхнем регистре + '_'.

Другие примеры:

`ddddd`
Создает например: 41922, 12733, 43960, 07660, 12390, 74680, ...

`\H\e\x\:\ HHHHHH`
Создает например: 'Hex: 13567A ', ' Hex: A6B99D ', ' Hex: 02243C', ...

Общие Шаблоны Пароля:

Название	Шаблон
WEP Hex Key - 40 Bit	h{10}
WEP Hex Key - 128 Bit	h{32}

WEP Hex Key - 256 Bit	h{64}
Случайные MAC-адреса	HH\-HH\-HH\-HH\-HH\-HH

Создание Паролей, по определенным Правилам

Далее, идёт несколько примеров, как функция генерации Шаблонов может быть использована, чтобы сгенерировать пароли, которые создаются по определенным правилам.

Обратите Внимание! Для всех следующих примеров следует включить опцию "Случайно перемешать символы пароля"!

Правило	Шаблон
Должен состоять из 2-х заглавных букв, 2-х строчных букв и 2-х цифр	uulldd
Должен состоять из 9 цифр и одной буквы	d{9}L
Должен состоять из 10 алфавитно-цифровых символов, где по крайней мере 1 - буква, и по крайней мере 1 - цифра	LdA{8}
Должен состоять из 10 алфавитно-цифровых символов, где по крайней мере 2 символа находятся в верхнем регистре и по крайней мере 2 являются символами нижнего регистра	uullA{6}
Должен состоять из 9 символов взятых из набора "ABCDEF" и в любом месте содержать символ "@"	\@[\A\B\C\D\E\F]{9}

Описание Функций Снижающих Надежность Пароля

Генератор пароля поддерживает несколько опций, такие как "Без повторяющихся символов", "Исключать похожие символы", и поле "Исключать следующие символы", для явного определения символов, которые не должны появиться в сгенерированных паролях.

Эти функции, уменьшают безопасность сгенерированных паролей. Их следует использовать, если только Вы вынуждены следовать правилам, установленным веб-сайтом или приложением, для которого Вы генерируете пароль.

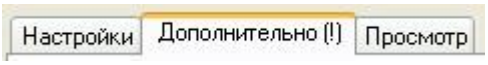
Опции находятся на вкладке *"Дополнительно"* в диалоговом окне "*Настройки генерации Пароля*".

Только для KeePass 1.x

Если Вы включаете опции уменьшающие безопасность, кнопка 'Дополнительно' в окне Генератора Паролей отображается красным цветом.

Только для KeePass 2.x

Если Вы задействуете настройки снижающие надежность Пароля, то на вкладке "Дополнительно" появляется восклицательный знак (!)



Создание и Использование Профилей Генератора Пароля

Настройки генератора паролей (набор символов, длина, шаблон...) могут быть сохранены как профили генератора пароля.

Создание / Изменение Профиля:

1. Откройте окно Генератора Пароля.
2. Определите все настройки нового профиля.
3. Щелкните на кнопку "Сохранить текущие настройки как Профиль".
4. Введите название нового профиля, или выберите существующее имя профиля из выпадающего списка, чтобы перезаписать или видоизменить его. Закройте диалоговое окно нажав "OK".
5. Если Вы захотите сразу создать пароль, используя новый профиль, щелкните по кнопке "OK". Или завершите работу с Генератором Паролей щелкнув по кнопке "Отмена" (созданый профиль не потеряется; управление профилем независимо от генерации пароля).

Использование Профиля:

Чтобы использовать профиль, просто выберите его из выпадающего списка профилей в окне генератора пароля. Автоматически будут загружены, все ранее сделаные настройки для этого профиля.

Конфигурирование настроек Автоматического Генерирования Паролей для Новых Записей

Когда Вы создаёте новую Запись, KeePass автоматически генерирует для неё случайный пароль. Свойства этих сгенерированных паролей могут быть сконфигурированы в диалоговом окне Генератора Пароля.

Для конфигурации, определите опции по своему выбору и перезапишите существующий профиль "Автоматически генерировать пароли для новых записей" (см. раздел выше).

Отключение Автоматического Генерирования Паролей:
Чтобы отключить автоматическое генерирование паролей для новых записей, выберите "Генерировать с использованием следующих символов" и в настройках длинны пароля поставьте "0". Перезапишите соответствующий профиль (см. выше).

Восстановление и ремонт Базы данных

В некоторых случаях,
KeePass способен восстанавливать поврежденные Базы данных.

Для предотвращения повреждения, файлов Базы данных, в работе KeePass используются дополнительные функции (запись транзакций Базы данных, сохранение в буфере обмена на диске, ...). Однако, нарушение целостности Базы данных, может произойти под воздействием других программ, а так же вследствии неустойчивой работы операционной системы или в результате сбоев при работе устройств для хранения (заметим, что KeePass по умолчанию проверяет целостность файлов Базы данных, немедленно после их записи, т.е. в данный момент времени, KeePass гарантирует целостность файлов, но понятно, что KeePass ничего не может сделать, если данные становятся поврежденными/нечитабельными в последствии в результате выше названных причин или банального "человеческого фактора").

Не дай бог конечно, но если данные таки окажутся поврежденными, Вам помогут функциональные возможности KeePass, предусмотренные для восстановления и ремонта Базы данных. При запуске этой функции отключаются любые проверки целостности и KeePass попытается выудить из поврежденного файла максимально возможное количество данных.

Для KeePass 1.x
В KeePass 1.x, процесс восстановления можно запустить в меню *"Инструменты"* - *"Починить файл с паролями..."*.

Для KeePass 2.x
Для того же, чтобы использовать функцию ремонта БД в KeePass ≥ 2,10, сначала, необходимо будет создать новый файл Базы данных. Затем, перейти в меню *"Файл"* -> *"Импорт"'* и импортировать поврежденный файл Базы данных, используя в качестве формата *'KeePass KDBX (2.x) (режим исправления)*.

Однако, возможности KeePass по восстановлению и ремонту Базы данных, окажутся бесполезны если Вы забыли (потеряли) Мастер-ключ или Композитный ключ. Кроме того, Вас ждет неудача, если поврежден заголовок Базы данных (несколько первых байт): функциональные возможности ремонта, для восстановления паролей, не смогут быть инициированы (потому что заголовок содержит информацию, необходимую для расшифровки данных).

К возможности KeePass, по восстановлению и ремонту Базы данных следует относится как к последней надежде. Для уверенности в сохранности Вашей Базы данных паролей, следует предпринимать превентивные меры безопасности, регулярное резервное копирование пока еще ни кто не отменял. Резервное копирование, ни как не влияет на криптографическую безопасность, а для автоматизации этого процесса существуют плагины представленные в разделе *плагины для KeePass.*

Безопасное редактирование

Средства Безопасного редактирования

KeePass поддерживает улучшенные средства безопасного редактирования.

KeePass является одним из первых менеджеров и хранителей паролей обладающих безопасными средствами редактирования. Средства редактирования, используемые в KeePass, являются стойкими к обнаружению паролей, и успешно противостоят шпионам за процессами управления паролями. Дополнительно, введенные пароли защищаются от атак на дамп памяти: пароли, не видимы даже в пространстве памяти процессов KeePass!

KeePass использует безопасные средства редактирования, только при включении функции сокрытия за звездочками! Если вы будете показывать пароли в виде простого текста, тогда они не будут защищены (средства безопасного редактирования будут просто выключены и их заменит стандартная функция редактирования Windows).

Только для KeePass 1.x
Ограничение выбора

Ограничением прав, при использование функции безопасного редактирования является то, что вы не можете выбрать диапазон символов. Вы например не сможете выбрать 3 символа и заменить их текущим содержимым буфера обмена, используя команду вставки.

Если вы захотите удалить все содержимое из Средств Безопасного Редактирования, нажмите *Shift-Home* или *Shift-End.* Это позволит удалить все введенные символы.

Техническая база

Если вы хотите узнать побольше о принципах работы Средств Безопасного Редактирования, советую прочитать эту статью автора KeePass CSecureEditEx - A More Secure Edit Control

Только для KeePass 2.x

Здесь нет ограничений по выбору. Средства Безопасного Редактирования ведут себя точно та же, как и стандартный редактор Windows.

Безопасность

Подробная информация об организации безопасности, методах и способах защиты паролей в *хранителе паролей KeePass Password Safe*.

Шифрование базы данных

Менеджер и хранитель паролей KeePass, шифрует файлы своей базы данных. KeePass шифрует всю базу данных полностью, т.е. не только ваши пароли. Имена пользователей, заметки, т.д., шифруются тоже.

Базы данных зашифрованы, с использованием одного из следующих блочных шифров:

Шифр	Размер блока	Размер ключа
Advanced Encryption Standard (AES / Rijndael)	128 bits	256 bits
Twofish	128 bits	256 bits

Эти алгоритмы хорошо известны, проанализированы и в криптографическом сообществе считаются очень безопасными (для примера см. [1] доклад NIST об AES).

Только KeePass 2.x
KeePass 2.x не поддерживает Twofish, но дополнительные алгоритмы шифрования могут быть предоставлены с помощью плагинов.

Блочные шифры используются в CBC (режим сцепления блоков шифртекста) блочный режим шифрования. В режиме CBC, шаблоны обычного текста скрыты.

Для обоих алгоритмов, 128-битный вектор инициализации (IV) каждый раз, когда вы сохраняете базу данных, генерируется случайным образом. Это позволяет, без обнаружения использовать несколько баз данных, зашифрованных с использованием тех же ключей.

Хеширование и Образование Ключей

Для формирования 256-битного ключа для блочных шифров, используется Secure Hash Algorithm SHA-256. Этот алгоритм сжимает предоставленный *пользовательский ключ* (состоящий из пароля и / или ключевого файла), до ключа фиксированного размера в 256 бит. Эта трансформация является односторонней, то есть обратное преобразование хэш-функции математически невозможно, как невозможно и найти второе сообщение, сжимающееся в такой же хэш.

Недавно обнаруженное нападение на SHA-1 [2] не влияет на безопасность SHA-256. SHA-256 по-прежнему рассматривается как очень безопасный [3].

Появление ключей:
Если используется только пароль (т.е. без файла-ключа), пароль плюс 128-битный *Random Salt*, хэшируются с помощью SHA-256 для формирования окончательного ключа (но заметьте, есть некоторая предварительная обработка: Защита от атаки по словарю). *Random Salt* предотвращает атаки, основанные на предварительно вычисленных хэшах.

При использовании и пароля и ключевого файла, окончательный ключ образуется следующим образом: `SHA-256(SHA-256(пароль), содержимое ключевого файла)` т.е. хэш мастер-пароля объединяется с байтами ключевого файла и получившаяся строка байт хэшируется с SHA-256 снова. Если ключевой файл не содержит точно 32 байта (256 битов), тогда он также хэшируется с SHA-256, чтобы сформировать 256-битовый ключ. Формула выше, тогда изменится на: `SHA-256(SHA-256(пароль), SHA-256(содержимое ключевого файла))`.

Генератор Случайных Чисел

Хранителю паролей KeePass, необходимо генерировать несколько случайных байт (для IV, *для Salt* главного ключа и т.д.). Для этого, используются несколько псевдо-случайных источников: текущий отсчет времени, счетчик производительности, системные дата / время, положение курсора мыши, состояние памяти (свободная виртуальная память и т.д.), активное окно, владелец буфера обмена, различные процессы и идентификаторы, различные состояния окна (активное окно, рабочий стол, ...), стек окна сообщений, статус множества процессов, информации о процессе запуска и некоторые структуры системной информации. Кроме того, KeePass использует случайные байты, по умолчанию предоставляемые системой CSP RNG (CryptoServiceProvider GenerateRandomNumbers).

Это псевдо-случайные данные, объеденненные в случайной динамической области. Чтобы сгенерировать случайные 16 байт, эта случайная динамическая область хэшируется (SHA-256) с использованием счетчика. Счетчик увеличивается после 16 сгенерированных байт. Таким образом, множество случайных байт будут эффективно производиться так, как требуется.

Защита от Атак по словарю

Менеджер паролей KeePass, поддерживает защиту от угадывания и атаки по словарю.

Реально, Вы не сможете предотвратить эти нападения: ничто не помешает злоумышленнику просто перепробовать все возможные ключи и просмотреть расшифрованую базу данных. Но то, что мы можем сделать (и KeePass делает) это максимально затруднить подбор: с помощью добавления постоянного рабочего фактора по ключевой инициализации, мы можем затруднить подбор на столько сильно, насколько захотим.

Для получения окончательного 256-битного ключа, который будет использоваться для блочных шифров, KeePass в первую очередь, хэширует пароль пользователя используя SHA-256, шифрует результат *N* раз с помощью алгоритма Advanced Encryption Standard (AES) (вызывая *key transformation rounds* в настоящее время), а затем хэширует его снова, используя SHA-256. Для AES, используется случайный 256-битный ключ, который хранится в файле базы данных. Поскрльку AES преобразование, не является предварительно вычислимым (случайный ключ), злоумышленнику тоже необходимо выполнить все этапы шифрования, иначе он не сможет проверить и посмотреть, является ли текущий ключ правильным.

Сейчас, атакующему потребуется гораздо больше времени, для подбора ключа. Если он сможет проверять лишь несколько ключей в секунду, то атака по словарю становиться не актуальной. *N* - является фактором работы и лишь косвенно фактором времени. Супер-ЭВМ может проверять ключи намного быстрее, чем стандартный PC, но в любом случае проверка одного ключа с *N* - количеством раундов, приведет к большему преобразований в *N* раз, чем проверка на супер-ЭВМ ключей без раундов преобразования.

По умолчанию, KeePass устанавливает *N* в 6000 раундов кодирования (подразумевается полное шифрование, *N* не имеет ничего общего с внутренними раундами шифрования AES). Это число было выбрано для того, чтобы обеспечить совместимость с портативными устройствами (процессоры КПК работают медленнее, поэтому вычисление ключей занимает больше времени).

Если вы используете KeePass только на ПК, настоятельно рекомендуется увеличить количество раундов преобразований ключей. Изменить этот параметр, Вы сможете в диалоге настроек базы данных. Кнопку настроек, Вы найдете справа от поля для раундов. При нажатии на эту кнопку, KeePass вычисляет количество раундов, при 1-секундной задержке. Подождать 1 секунду при открытии базы данных непроблематично, но для злоумышленника это создаст серьезные затруднения. Однако, количество раундов может быть свободно установлено по вашему выбору; кнопка только помогает Вам получить примерное представление о том, сколько раундов можно вычислить на компьютере за 1 секунду.

Эта функция защиты полезна только для Master паролей; ключевые файлы в любом случае являются случайными и нет необходимости трансформирования их содержимого. Отгадывание содержимого файла ключей, одинаково стойко выдерживает атаки брут-форсом против финального ключа.

Для вычисления преобразований *KeePass* использует многопоточность (*мастер-ключ,* разделяется на две части в 128 бит, что соответствует размеру блока AES). На компьютерах с двух-ядерными и более процессорами , вычисления соответственно будут происходить намного быстрее, чем на одно-ядерном процессоре.

В Windows Vista и выше, для ключевых преобразований *KeePass* может использовать API Windows CNG/BCrypt, что позволит работать на 50% быстрее, чем с кодом преобразования ключей встроеным в *KeePass*.

KeePassX: В отличие от *KeePass*, проект Linux port 'KeePassX' только частично поддерживает защиту от атаки по словарю и перебору.

Защита Памяти Процессов

Во время работы *KeePass*, деликатные данные (например, хэш мастер-ключа и пароли Записей) хранятся в памяти процесса в зашифрованном виде.

Это означает, что даже если сделать дамп памяти процесса *KeePass* на диск, вы не сможете увидеть пароли.

Только KeePass 2.x
По умолчанию, пароли записей в оперативной памяти защищены, в отличии от других областей (как в 1.x). Однако, в диалоге настройки базы данных, вы можете включить защиту в памяти и для других полей (что не рекомендуется, из соображений по потере производительности).

К примеру, когда вы копируете пароль в буфер обмена, *KeePass* сначала расшифровывает поле пароля, затем копирует его в буфер обмена и немедленно обратно зашифровывает с помощью случайного ключа.

Кроме того, по завершению процесов, *KeePass* стирает всю критичную с точки зрения *безопасности* память, т.е. он перезаписывает эти области памяти, прежде чем открыть их (и это относится ко всей критичной по безопасности памяти, а не только к полям с паролями).

KeePass ≥ 1,15 и 2.x, для шифрования конфиденциальных данных в памяти, использует Windows DPAPI. С помощью DPAPI, ключ для кодирования в оперативной памяти сохраняется в безопасной, невыгружаемой области памяти, которой управляет Windows. Если DPAPI не доступен или выключен (расширенные настройки *KeePass*, по умолчанию использование DPAPI включено), *KeePass* использует алгоритм шифрования ARC4 со случайным ключом. Однако отметим, что это менее безопасно, чем DPAPI, в основном *не* потому, что ARC4 криптографически не так силен, а потому, что зашфрованый в памяти ключ хранится в выгружаемой памяти процесса.

Блокировка рабочей среды

Блокируя рабочее пространство, *KeePass* закрывает файл базы данных и оставляет для просмотра только параметры последних настроек (какие группы и записи были выбраны, список позиций и т.д.).

Это обеспечивает максимальную безопасность: разблокировать рабочую область так же сложно, как и открыть файл базы данных закрытый обычным способом. Кроме того,

блокировка рабочей среды предохраняет от потери данных (работа компьютера может нарушиться, а при заблокированном *KeePass*, ущерба для баз данных не будет).

Плагины и Безопасность

Подробное освещение темы *Безопасности* при работе с *Плагинами* посвящены отдельные страницы:
плагины и безопасность в (KeePass 1.x),
плагины и безопасность в (KeePass 2.x).

Стартовый тест

Каждый раз, когда вы запускаете *KeePass*, программа выполняет быстрое самотестирование, чтобы проверить все ли блочные шифры и хэш-алгоритмы работают правильно и передают свои отчеты. Если один из этих алгоритмов не пройдет проверку, *KeePass* выведет окно сообщения об исключительной ситуации в безопасности.

Специализированное Шпионское ПО

Этот раздел дает ответы на типичные вопросы, следующего содержания:

- Произойдет ли повышение безопасности и недопущение воздействия вредоносными программами за счет шифрования файла конфигурации?
- Произойдет ли повышение безопасности и недопущение воздействия вредоносными программами за счет шифрования приложения (исполняемого файла, в конечном итоге вместе с файлом конфигурации)?
- Послужит ли улучшению безопасности, возможность предотвращения загрузки плагинов?
- Будет ли способствовать усилению безопасности, сохранение настроек по безопасности в базе данных (с отменой параметров настроек *KeePass*)?

Ответ на все эти вопросы: **нет**.

Добавление любой из этих функций не повысит *безопасность*.

Все *функции защиты в KeePass* направлены против универсальных угроз, таких как клавиатурные шпионы, мониторы буфера обмена, мониторы управления паролем, и т.д. (и против не динамических нападений на базу данных, анализаторы дампов памяти, ...). Однако во всех вышезаданных вопросах предполагается, что шпионские программы, запущенные в системе, специализируются на атаках против *KeePass*.

А при такой ситуации, да же *лучшие функции безопасности* со временем потерпят неудачу. Закон № 1 из 10 основополагающих законов безопасности: *"Если вы запустили на своем компьютере приложение злоумышленника, это больше не ваш компьютер". Подробнее об Основополагающих законах безопасности смотрим* [4] [5]

Для примера, рассмотрим следующую очень простую шпионскую програмvку специализирующуюся на *KeePass*: програмvка ожидает начала запуска *KeePass*, а затем скрывает запущенное приложение и имитирует себя взамен *KeePass*. Все взаимодействия (подобно вводу пароля для разблокировки конфигурации, и т.п.) могут быть смоделированы. Единственный способ обнаружить это шпионское ПО состоит в том, чтобы использовать программу, о которой шпионская програмvка не знает или которой не сможет манипулировать (Secure Desktop), в любом случае это не может и не должен делать *хранитель паролей KeePass Password Safe*.

Полезные ссылки и дополнительная литература

[1] Национальный Институт Стандартов и Технологии: *Доклад о развитии Advanced Encryption Standard (AES)* (PDF) (на английском).

[2] блог Брюса Шнайера: *SHA-1 сломан* (на английском).

[3] блог Брюса Шнайера: *Криптоанализ SHA-1*, (на английском) с комментариями по поводу последствий этого открытия и что теперь делать,

[4] Scott Culp, Microsoft TechNet Essay, 2000: *10 непреложных законов безопасности. (на русском).*

[5] Йеспер М. Йоханссон (Jesper M. Johansson), Microsoft TechNet Magazine, 2008: *Возвращаясь к 10 непреложным законам безопасности, часть 1 (на русском).*

Поддержка и создание TAN-кодов

Поддержка TAN-кодов
KeePass поддерживает Transaction Authentication Numbers (TANs). (проверку подлинности номеров (TAN-кодов)).

- Использование: *Тан Мастер* поможет добавить TAN-коды
- Использование TAN-кодов

KeePass поддерживает TAN-коды, т.е. пароли особого вида (разрешены только алфавитно-цифровые символы), которые могут быть использованы только однажды. Запись в списке TAN помечается как просроченная, когда Вы используете команду "скопировать пароль" такой записи. Эти специальные пароли, которые используются некоторыми банками: Вам

необходимо подтвердить, проведение транзакций с использованием таких TAN-кодов. Это обеспечивает дополнительную безопасность, поскольку шпион не сможет выполнить транзакции, даже если он знает пароль Вашего банковского счета.

 Использование *Тан Мастера* для добавления TAN-кодов

Вы можете использовать встроеный в KeePass, **TAN мастер,** который поможет добавить сразу несколько TAN-кодов к вашей базе данных. Просто откройте диалоговое окно Тан Мастер *(меню Инструменты -> Тап мастер)* и введите все ваши TAN-коды. Форматирование не играет роли, KeePass использует все алфавитно-цифровые символы, т.е. такие символы как новая строка, табуляторы, пробелы, точки и т.д. используются как разделители.

Затем, мастер создаст несколько TAN-записей из данных, которые Вы ввели в диалоговом окне. Каждый TAN представляет собой стандартную запись KeePass. Заголовок записи всегда "<TAN>". Это указывает программе KeePass, что эта запись, является TAN-записью и Вы не сможете изменить заголовок, имя пользователя или URL TAN-а (кроме того, это не имеет смысла). Но если захотите, то Вы сможете свободно добавлять комментарии к TAN-записи.

 Использование TAN-кодов

Когда Вы *используете* TAN (т.е. выполняете над ним команду "скопировать пароль"), поле "окончание" записи устанавливается в текущие дату и время, что помечает запись как просроченную. Запись получает пиктограмму **X**. Если Вы в дальнейшем захотите узнать, когда была использована конкретная запись TAN, Вам просто достаточно взглянуть на дату в поле "окончание".

При копировании TAN в буфер обмена, База данных помечается модифицированной. Вы должны сохранить файл, чтобы запомнить использование TAN.

Если Вы случайно, без необходимости использовали TAN, Вы можете сбросить его (т.е. удалить красные **X** и показать его снова, в качестве действительного TAN). Для этого откройте запись TAN (правой кнопкой мыши и выберите *"Изменить / Открыть Входы ..."*). Здесь, снимите флажок с чекбокса "Expires". Нажмите кнопку ОК для закрытия диалогового окна.

Возможности поля URL (Ссылка)

В KeePass Password Safe, поле URL поддерживает различные протоколы и специальные заполнители.

Возможности поля URL:

- Стандартные возможности
- Работа с Командной строкой
- Маркеры - Заполнители
- Изменение обработки URL (Отменить URL)

Используем Tips & Tricks (Советы и Приемы):

- Начинало сессии RDP / TS (Удаленный рабочий стол / Подключение к терминальному серверу)
- Выполнение встроенных команд Shell

Стандартные возможности

Поле URL может обработать и выполнить любой существующий адрес URL, для которого определен обработчик протокола. В основном, на большинстве систем используются протоколы: `http://` , `ftp://` и `mailto:`. *KeePass* поддерживает все зарегистрированные протоколы, которые поддерживает Internet Explorer.

Например, если на глобальном уровне (т.е. используя Windows Explorer) определить использование PuTTY для URL-адресов `ssh://`, то *KeePass* так же, будет автоматически применять PuTTY для URL-адресов `ssh://`.

Работа с Командной строкой

С помощью поля URL, вместо обычного открытия URL-адресов, Вы можете выполнять задания с использованием Командной строки. Для того, что бы *KeePass* понял, что Вы ввели задание для Командной строки, потребуется всего лишь добавить префикс `cmd://` . Например, если Вы захотите открыть Блокнот, то поле URL заполняется следующим образом:

```
cmd://C:\Windows\Notepad.exe C:\Test\MyTestFile.txt
```

Виртуальный протокол `cmd://`, в отличие от протокола `file://`, поддерживает применение параметров при запуске исполняемых файлов. Это послужило основным поводом для внедрения в *KeePass* протокола `cmd://`. Работая с протоколом `file://`, Вы не сможете запускать приложения с использованием дополнительных параметов. Для этого, используйте протокол `cmd://`.

Пути, для протокола `cmd://`, кодировать не нужно. К примеру, вам не потребуется заменять пробелы на `%20`, как это обычно происходит у других URL-адресов. При обработке поля URL, KeePass просто отнимает виртуальный префикс протокола `cmd://` и оставшуюся часть передает на исполнение *Командной строке* Windows.

Если же путь к файлу содержит пробелы, необходимо будет заключить его в кавычки (").

Переменные среды:
Поддерживаются переменные среды Windows . К примеру, `%TEMP%` заменяет временный путь пользователя.

Безусловные, UNC пути:
Полностью поддерживается стиль UNC путей Windows (начинающихся с `\\`), т. е. не требуется предварительно прописывать префикс `cmd://` .

Маркеры - Заполнители

В поле URL, можно одновременно использовать несколько заполнителей, которые будут автоматически вводится, при выполнении URL. Пример:

```
http://www.yoursite.com/default.php?user={USERNAME}&pass={PASSWORD}
```

После активирования ссылки, для авторизации на этой странице *KeePass* введёт данные (USERNAME) в поле *имя пользователя* и данные (PASSWORD) в поле *пароль*.

Таким же образом, заполнители применяются при использовании функции *Автозаполнения*. Полный список поддерживаемых заполнителей опубликован на странице *Автозаполнение - Auto-Type* в разделе *Последовательность нажатия клавиш Автозаполнения*

На ряду с обычными, поддерживаются и специальные заполнители. Например, заполнитель `{APPDIR}` заменяет путь к каталогу с установленным *хранителем паролей KeePass*. Это абсолютный путь, без обратной косой черты к директории содержащей исполняемый файл *KeePass*. Если бы, вы захотели запустить новый экземпляр KeePass, то поле URL, потребовалось бы заполнить таким образом:

```
cmd://"{APPDIR}\KeePass.exe"
```

При желании, Вы можете указать каким конкретным браузером необходимо открыть адрес для данной Записи. Вот несколько примеров, заполнения поля URL:

```
cmd://{INTERNETEXPLORER} "http://www.yoursite.com"
cmd://{FIREFOX} "http://www.yoursite.com"
cmd://{OPERA} "http://www.yoursite.com"
cmd://{GOOGLECHROME} "http://www.yoursite.com"
```

Маркер - Заполнитель, введет путь к исполняемым файлам Браузера (если тот установлен).

Только для KeePass 1.x

Изменение обработки URL (Отменить URL)

Поведение поля URL может определятся индивидуально для каждой Записи с помощью поля Комментарии. Это позволяет выполнять конкретные URL, используя при этом поле URL, только для хранения данных.
Просто укажите `Отменить-Url:` затем, введите командную строку в поле Комментарии. Теперь, если в главном окне Записи, дважды щелкнуть на поле URL, то будет выполняться указанная (в поле Комментарии) командная строка.

Использование другого браузера:
Если по умолчанию в KeePass Password Safe используется браузер Firefox, а вы хотите, открыть свой любимый сайт с помощью Internet Explorer, добавьте в поле для комментариев, следующую строчку:

```
Url-Override: cmd://{INTERNETEXPLORER} "{URL}"
```

KeePass автоматически откроет Internet Explorer и в качестве параметра передаст данные из поля URL. При этом используется маркер-заполнитель, *найти Internet Explorer*.

Запуск KeeForm:
Если Вы, захотите открыть какой либо сайт с помощью KeeForm и Internet Explorer, добавьте следующие строки в поле *Комментарии*:

```
Url-Override: cmd://"{APPDIR}\KeeForm.exe" "{URL}" "{USERNAME}" "{PASSWORD}"
{ENTERFORM}
```

KeePass автоматически откроет *KeeForm* и передаст данные из поля URL, а в качестве параметров отправит имя пользователя и пароль.

Изменение глобальных настроек URL:
Если же, Вы захотите изменить настройки выполнения URL *по умолчанию* (т. е. для *всех* URL-адресов), то вам потребуется добавить строку `KeeUrlOverride` в файл `KeePass.ini`.

Для использования KeeForm, в качестве обработчика URL по умолчанию, добавьте следующую строку в конце `KeePass.ini` :

```
KeeUrlOverride=cmd://"{APPDIR}\KeeForm.exe" "{URL}" "{USERNAME}"
"{PASSWORD}" {ENTERFORM}
```

Более подробные инструкции по установке и использованию *KeeForm*, можно найти в файле справки о *KeeForm*.

Начало сессии RDP/TS

Вы можете использовать поля-URL Записей и виртуальный протокол `cmd://`, чтобы подключиться к удаленному рабочему столу.

Для этого, потребуется ввести следующую комманду в строку поля URL:

```
cmd://mstsc.exe
```

И теперь, после двойного щелчка мышкой по полю URL в главном окне Записи, начнется подключение к удаленному рабочему столу Windows.

MSTSC это программа подключения терминального сервера Windows (подключение к удаленному рабочему столу). Вы можете указать путь к существующему файлу программы RDP, чтобы открыть его. Например: по следующей ссылке открывается указанный файл RDP:

```
cmd://mstsc.exe "C:My FilesConnection.rdp"
```

Более того, MSTSC поддерживает несколько параметров командной строки:

- **/v:<Server[:Port]>**
  Определяет терминальный сервер для подключения.
- **/console**
  Подключение к терминальной сессии на сервере.
- **/f**
  Запуск клиента в полноэкранном режиме.
- **/w:<Width>**
  Определяет ширину экрана удаленного рабочего стола.
- **/h:<Height>**
  Определяет высоту экрана удаленного рабочего стола.
- **/edit**
  Открывает для редактирования, указанный файл RDP.
- **/migrate**
  Перемещает старые файлы подключения к новым файлам RDP.

Выполнение встроенных команд Shell

В KeePass Password Safe, поле URL может быть использовано для запуска приложений / документов и URL-адресов. Если вы захотите выполнить встроенную команду оболочки, например `COPY`, то сделать это напрямую не получиться, потому что не существует *`COPY.EXE`* (в Windows 9x это было актуально, но на всех современных операционных системах Windows, такие команды реализуются в командной строке).

Для того, чтобы запустить встроенные в оболочку команды, вам необходимо передать их на интерпретатор командной строки `cmd.exe`.

Для команды `COPY`, необходимо указать `cmd.exe` в виде исполняемого файла, а '`/C COPY from to`' в качестве аргумента (где '`from`' и '`to`' являются путями). Параметр `/C` указывает `cmd.exe` выполнить следующую командную строку.

В поле URL, этот адрес будет выглядеть следующим образом:

```
cmd://cmd.exe /C COPY from to
```

В других местах, таких как командная строка в триггерной системе, вы можете не использовать URL префикс `cmd://`.

Использование хранимых в KeePass паролей

Каким образом, пароли хранящиеся в *KeePass,* можно перенести в другие программы или приложения и заполнить там необходимые поля.

Есть несколько способов, для копиования паролей хранящихся в KeePass в окна других приложений:

- Контекстно-зависимый список Записей
- Drag&Drop Перетащить и Вставить
- Auto-Type Автозаполнение
- KeeForm, интеграция. Панели инструментов для Браузеров и другие Плагины

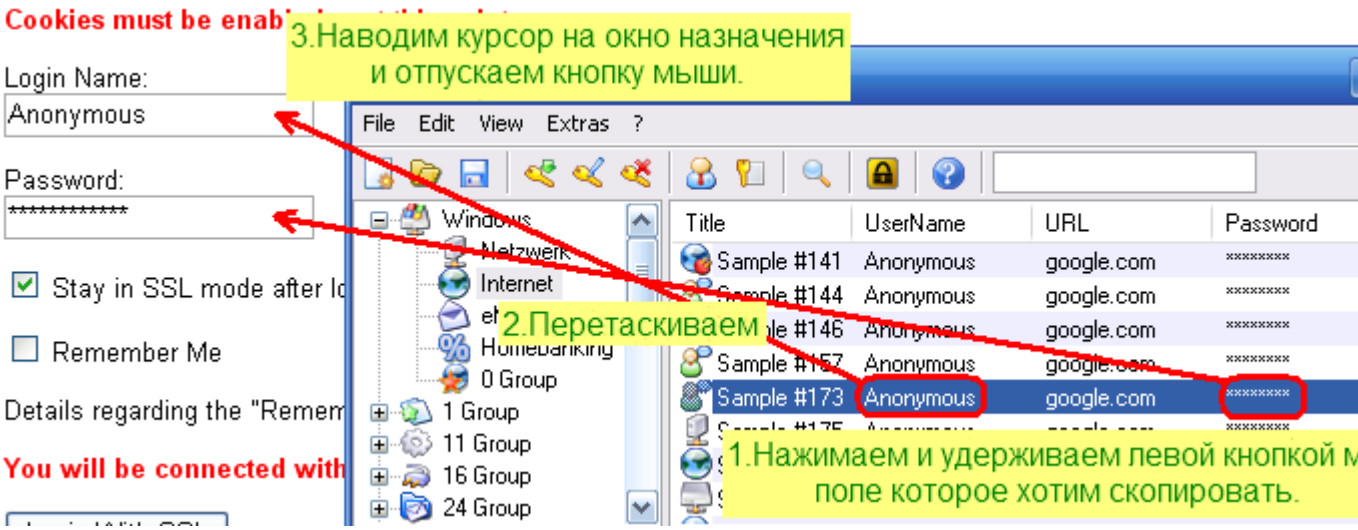
Контекстно-зависимый список Входов

После двойного нажатия мышкой на поле Записи (в меню главного окна), будет произведено действие, соответствующее свойствам и назначению этого поля.

- **Поле "Название":** откроет окно диалога, для редактирования параметров входа, к этой записи.
- **Поле "Имя":** скопирует имя пользователя, в буфер обмена.
- **Поле "URL":** откроет, содержащийся в нем адрес, в браузере или скопирует его в буфер обмена (необходимый вариант задается в настройках).
- **Поле "Пароль":** скопирует пароль пользователя в буфер обмена.
- **Поле "Комментарии":** комментарии будут скопированы в буфер обмена.
- **Поле "Присоединенные файлы":** в *KeePass 1.x* - будут скопированы в буфер обмена, а в *KeePass 2.x* - откроются во встроенном редакторе.
- **Остальные поля,** такие как *время, дата, идентификатор* (*UUID*) и т.д.: содержимое этих полей, будет копироваться в буфер обмена.

Drag&Drop (Перетащить и Вставить)

Любое поле Записи *KeePass*, можно перетаскивать и вставлять(Drag&Drop) в окна других программ и приложений.



Автозаполнение (Auto-Type)

Auto-Type, Авто-набор, Автозаполнение и Авто-ввод, все эти понятия, четко отражают суть мощного средства моделирования, которое имитируя действия оператора, посылает нажатия клавиш в целевые поля окон, других программ и приложений.

Более подробную информацию о функции *автонабора в KeePass*, Вы сможете почерпнуть посетив страницу докуметации: Автозаполнение (Auto-Type) .

KeeForm, панель инструментов браузера и другие плагины

Выпущено много плагинов, позволяющих интегрировать KeePass непосредственно с другими приложениями, например: *KeeForm* (для Internet Explorer и Mozilla Firefox) и *Browser Integration Toolbar* (только для Internet Explorer) которые полностью автоматизируют заполнение вебформ.

Эти и другие не менее интересные инструменты, обнаружете Вы, заглянув на страничку с *плагинами* для менеджера и хранителя паролей *KeePass Pasword Safe.*