МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О. Г. Локтионова
«_4_» _04_____ 2021 г.

МЕНЕДЖЕР ПАРОЛЕЙ: ПРОГРАММА PASSWORD COMMANDER

Методические указания по выполнению практических занятий и лабораторных работ для студентов направления подготовки 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02

Курск, 2022

УДК 004.056(076.5)
Составитель: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент М.А. Ефремов

Менеджер паролей: программа Password comander: методические указания по выполнению практических занятий и лабораторных работ/ Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко, Курск, 2022. 15с.: ил. 8, Библиогр. с. 15.

Содержат краткие теоретические положения о методике хранения, генерации и шифрования паролей, автоматического заполнения форм web-страниц с помощью программы password commander.

Методические указания соответствуют требованиям программы по направлению подготовки информационная безопасность, программная инженерия, информационные системы и технологии, прикладная информатика, фундаментальная и прикладная лингвистика и специалистов: экономическая безопасность.

Предназначены для студентов направления подготовки10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02 дневной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16
Усл.печ. л. Уч. –изд. л. Тираж 100 экз. Заказ 1248 Бесплатно
Юго-Западный Государственный Университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическое занятие

Менеджер паролей: программа Password Commander

Введение

Обычно за годы работы за компьютером у пользователей ска пливается множество логинов и паролей (от электронных почтовых ящиков, интернет-магазинов, форумов, рассылок и т.д.). Конечно, можно просто все пароли выписывать на бумагу (тетрадку, блок нот и т. п.) или в обычный текстовый файл, а затем его хранить на пример в защищѐнном контейнере программы TrueCrypt. Но это гораздо менее удобно, а самое главное – менее безопасно по срав нению со специализированной программой для хранения паролей. Наиболее популярными программами "хранителями паролей" яв ляются:

KeePass**(http://keepass.info)**,

PasswordSafe**(http://passwordsafe.sourceforge.net)**,

Password Commander (**http://www.passwordcommander.com**и**http://pascom.ru**). Все три программы бесплатны. Password Commander создана отечественными разработчиками, поэтому изначально имеет рус ский интерфейс. Для KeePass на еѐ домашней странице можно ска чать, а затем установить русский интерфейс и русскую справку помощи. Для программы PasswordSafe можно скачать файл помо щи на русском языке.

Password Commander не только позволяет хранить и управ лять паролями и логинами, но и имеет встроенный генератор слу чайных паролей, чтобы в случае необходимости вам не надо было их придумывать самому. Кроме того, Password Commander имеет очень удобную функцию автоматического заполнения веб-форм в браузере и различных текстовых полей.

Скачать Password Commander с русским интерфейсом можно со страницы http://pascom.ru. Для жителей бывшего СССР Password Commander распространяется бесплатно, для остальных пользова телей предоставляется бесплатно только облегчѐнная (Lite) версия; полнофункциональный вариант (Professional edition) стоит $37.95 (€29.95).

Краткие теоретические положения

Создание аккаунта

В Password Commander одновременно н независимо друг от друга могут хранить свои пароли сразу множество пользователей. Для этого каждый пользователь должен завести свой аккаунт в программе. Аккаунт – это база, где хранятся все пароли пользова теля, доступ в которую возможен только после авторизации (рис. 1). Программа сразу после установки имеет один аккаунт под названием **Пример (Пароль = 123)**. Это учебный аккаунт, который содержит пример хранения логинов и паролей; если вы введѐте па роль 123, то попадаете в него.

Рис. 1 Окно авторизации Password Commander

Для защиты от программ-кейлогеров Password Commander предоставляет возможность набора паролей на экранной клавиату ре.

Вам следует создать свой аккаунт. Для этого необходимо за пустить Мастер создания нового аккаунта. Сделать это можно либо из окна авторизации (**Действия...–>Создать новый аккаунт..**.),

либо из главного окна программы (**Файл –>Создать новый акка унт...**). Мастер создания нового аккаунта пошагово поможет вам создать новый аккаунт. Если по ходу работы с мастером будет что то не понятно, то всегда можно нажать кнопку **Справка** и почи тать

подробности.

В главном окне созданного аккаунта (рис. 2) можно создавать записи, однако записи должны обязательно находиться в какой нибудь группе. Поэтому перед созданием первой записи нужно создать хотя бы одну группу. Для этого нужно вызвать **Редактор групп (Правка – Добавить группу...)**.

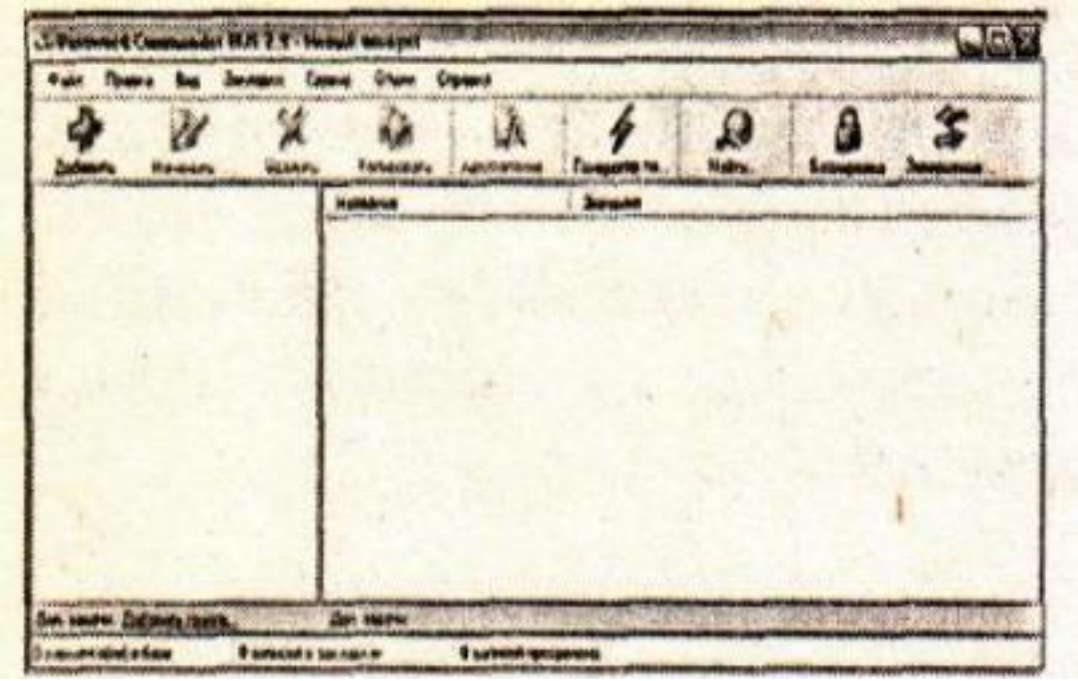

Рис.2. Главное окно созданного аккаунта

По умолчанию группа содержит два поля: **Login** и **Password** типов **Логин** и **Пароль** соответственно. Для большинства случаев этого достаточно, и после ввода названия группы можно просто нажать **OK**, но Password Commander предоставляет возможность добавлять новые поля разных типов. Например, для почтового ящика можно добавить два дополнительных поля: **Адрес pop3 сервера** и **Адрес smtp сервера**, оба типа **Текст**. Для добавления

полей существует кнопка **Добавить** в редакторе групп. В качестве примера создадим группу под именем "рассылка" (рис. 3).

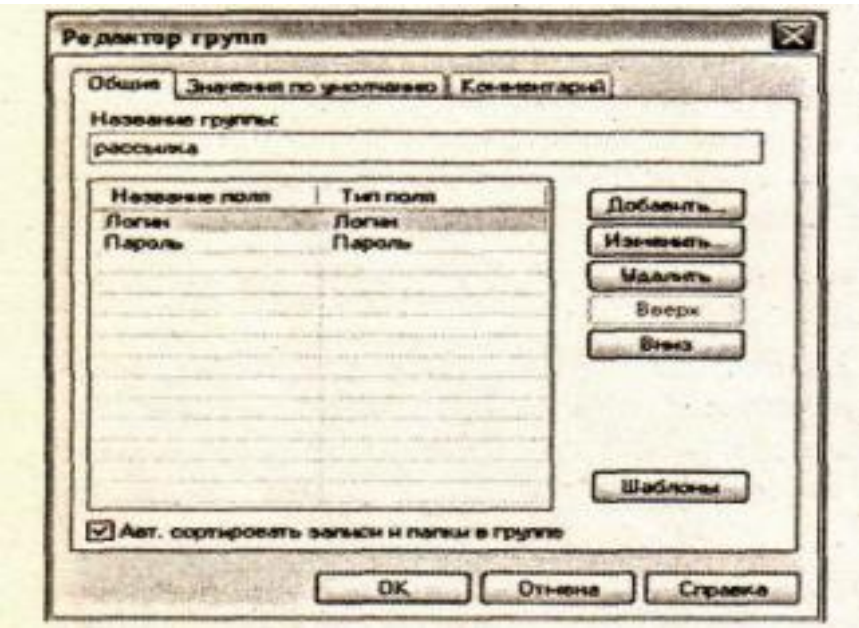

Рис. 3. Создание группы

Теперь в созданной группе можно создавать записи. Для этого нужно кликнуть по группе правой кнопкой мыши и выбрать в рас крывающемся меню пункт **Добавить запись...**. В появившемся **Ре дакторе записей** следует ввести данные в предложенные поля, за тем нажать кнопку **OK**. На рис. 4 показан пример создания записи под именем Subscribe.Ru.

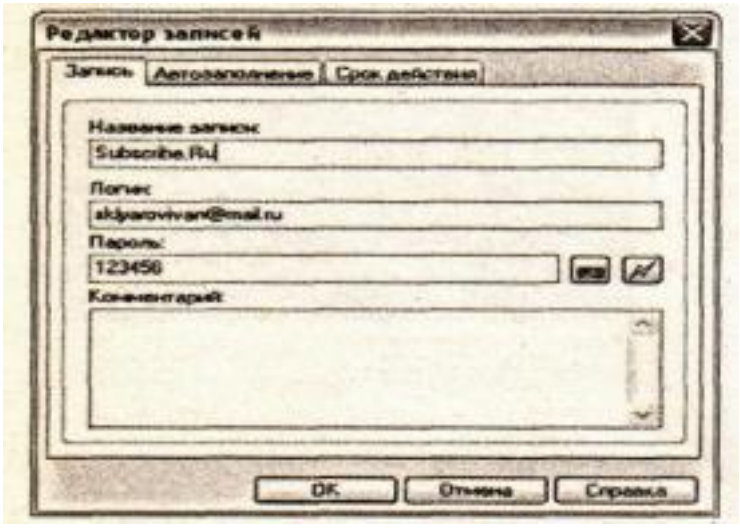

Рис 4. Создание записи

Записи в группе можно объединять в папки для облегчения навигации. Для этого нужно кликнуть по группе правой кнопкой мыши и выбрать в раскрывшемся меню пункт **Добавить подпап ку**. В появившемся диалоге следует ввести название новой папки. Далее можно перетаскивать мышью записи в нужную папку.

Все созданные элементы (группа папка, запись) вы можете изменять (удалять, перемещать, переименовывать и т.п.), для этого также имеются соответствующие пункты меню. На рис. 5 в качест ве примера показаны записи произвольного аккаунта, также не за бывайте обращаться за примерами к аккаунту **Пример (Пароль =**

123).

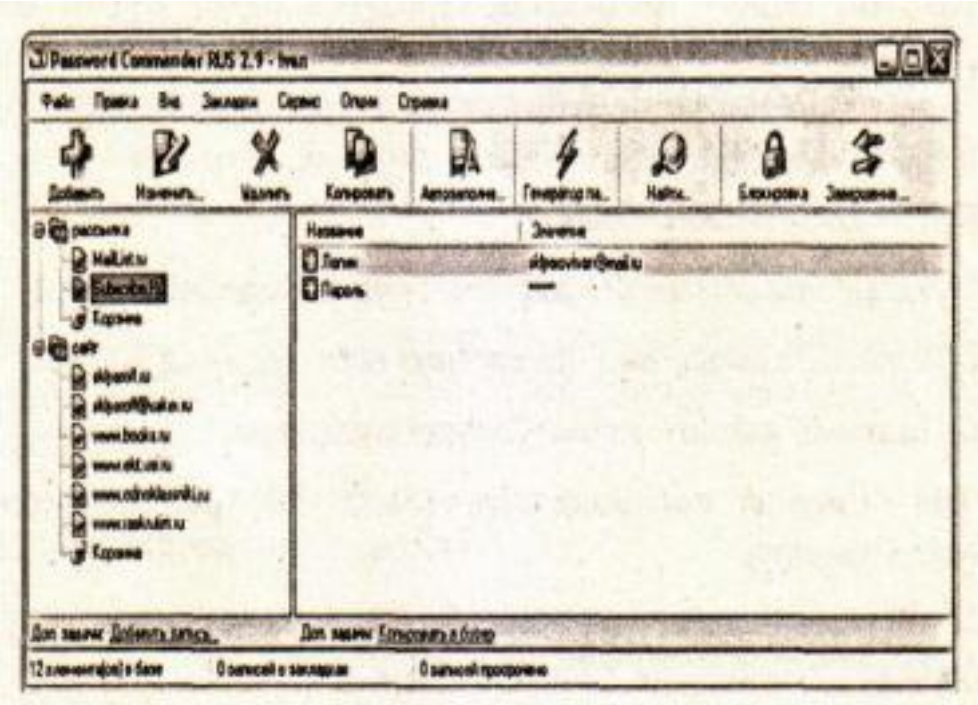

Рис 5. Записи произвольного аккаунта

Автозаполнение

Если вы хотите, чтобы Password Commander выполнял авто заполнение веб-форм и других текстовых полей, то необходимо сделать дополнительные настройки. С помощью функции автоза полнения вы можете вставить пароль (или другую информацию) в нужные поля всего одним щелчком мыши или нажатием "горячей клавиши".

Для этого надо в **Редакторе записей** перейти на вкладку **Ав тозаполнение** и нажать кнопку **Добавить**, затем, если вы собирае тесь заполнять веб-формы на сайте, то следует установить пере ключатель на **Автозаполнение в веб-страницу**. В поле **URL** сле дует ввести адрес страницы, на которой расположены нужные поля для заполнения (веб-форма) (рис. 6)

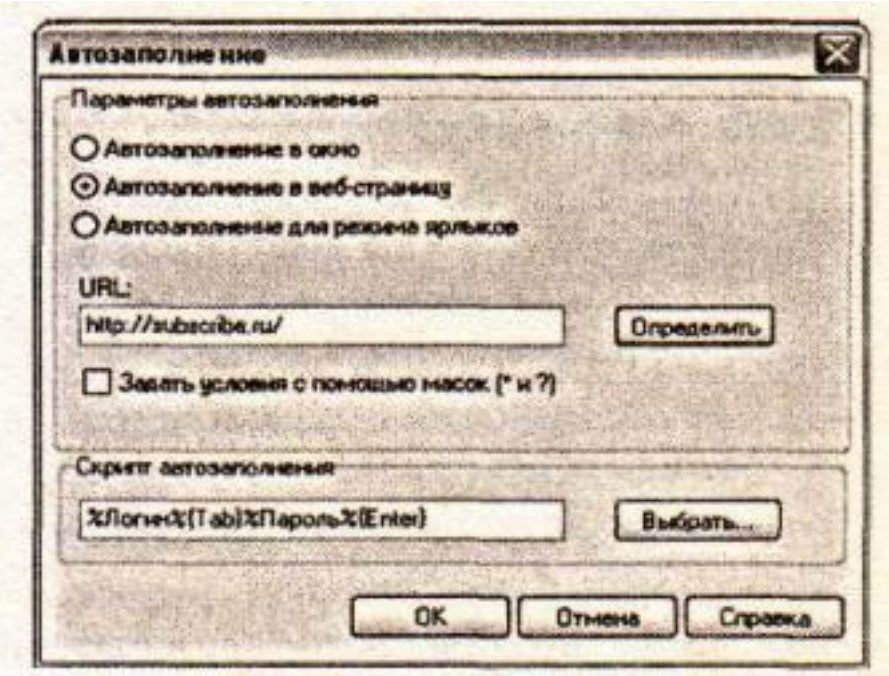

Рис. 6. Пример настройки автозаполнения в веб-страницу

В поле **Скрипт автозаполнения** вы можете видеть такую строку **%Логин%{Tab}%Пароль%{Enter}** это означает, что ав томатически будет заполняться поле **Логин**, затем поле **Пароль**, затем виртуально будет нажата клавиша <Enter>. Этот скрипт под ходит для большинства случаев, но вы можете настроить любой порядок заполнения полей для страницы. В **Справке** программы вы найдѐте подробное объяснение по тому, как составляются скрипты автозаполнения. Выражение, заключѐнное в знак процен та, означает, что Password Commander вставит в элемент ввода тек ста, на котором установлен курсор, содержимое поля, название ко торого обрамлено знаками процента. Выражения, заключѐнные в фигурные скобки, – это команды управления автозаполнением. Список команд автозаполнения:

{Clear} - Очищает содержимое текстового поля

{Tab} - "Нажимает" клавишу <Tab> (выполняет переход к следующе му элементу формы);
{Enter} - "Нажимает" клавишу <Enter>;
{Esc} - "Нажимает" клавишу <Escape>;
{Space} - "Нажимает" клавишу <Пробел>;
{Up} - "Нажимает" клавишу <вверх> (прокручивает вверх выпадаю щий список);
{Down} - "Нажимает" клавишу <вниз> (прокручивает вниз выпа дающий список);
{Right} - "Нажимает" клавишу <вправо> (смещает курсор вправо);
{Shift+Tab} - "Нажимает" комбинацию клавиш <Shift>+<Tab> (Выполняет переход к предыдущему элементу).

{mTabN} - "Нажимает" клавишу <Tab> N раз (выполняет переход к следующему элементу формы);
{mUpN} - "Нажимает" клавишу <вверх> N раз (прокручивает вверх выпадающий список);
{mDownN} - "Нажимает" клавишу <вниз> N раз (прокручивает вниз выпадающий список);
{mRightN} - "Нажимает" клавишу <вправо> N раз (смещает курсор вправо);
{mShift+TabN} - "Нажимает" комбинацию клавиш <Shift>+<Tab> N раз (Выполняет переход к предыдущему элементу).

Генератор паролей

Разработчики серьѐзно подошли к проблеме генерации паро лей и сделали генератор, который способен удовлетворить самые изысканные потребности пользователей.

Генератор паролей можно вызвать клавишей <F9> или меню **Сервис —> Генератор паролей** или соответствующей кнопкой напанели инструментов (рис. 7).

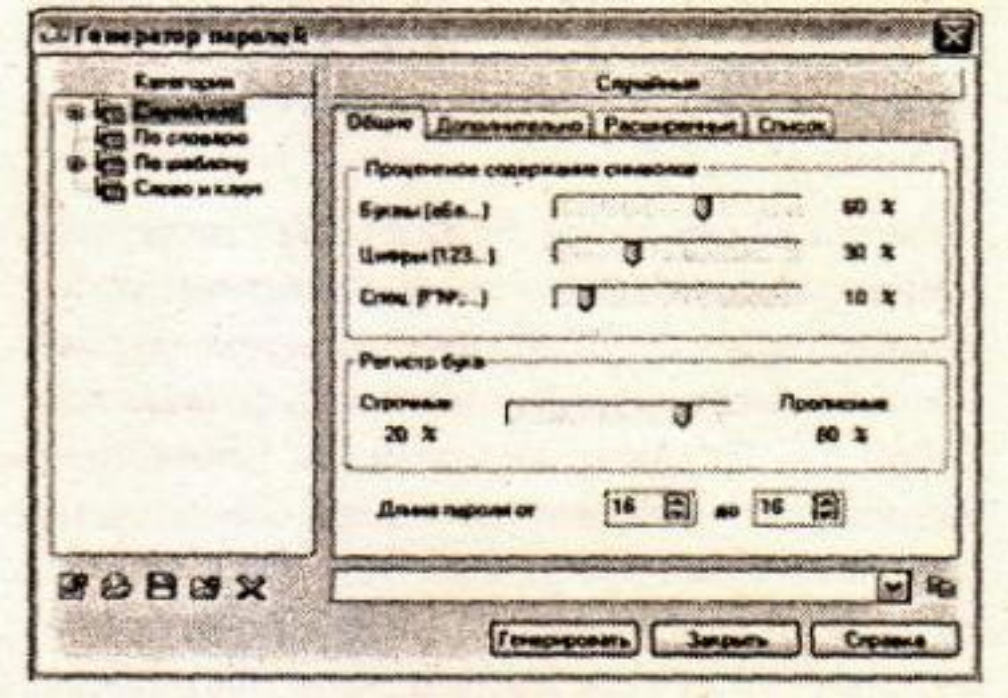

Рис. 7. Окно генератора паролей

С помощью генератора возможно создавать пароли четырѐх типов:

Случайные пароли, устойчивые к взлому. Генератор Pass word Commander обладает широким спектром настроек генерации случайных паролей. Вы можете выбрать длину, процентное содер жание тех или иных символов в пароле, регистр букв, добавить или

исключить свои символы, создать список паролей и сохранить его на диск.

Легко запоминаемые пароли по словарю. Вы можете под грузить любое количество дополнительных словарей, если словарь, поставляющийся с программой, вас не устроит, выбрать длину и тип генерации паролей, регистр букв в слове и т.д.

Генерация по шаблону. В программе представлено большое количество различных масок для генерации паролей. При создании паролей этого типа каждый специальный символ маски будет за менѐн по специальным правилам.

Генерация по слову и ключу. Специальная технология гене рации: достаточно ввести слово и ключ, и вы получите сложный пароль, который потом может быть легко восстановлен, достаточ но лишь снова запустить генератор и ввести слово и ключ.

Вам нужно выделить одну из категорий, при необходимости сделать настройки и нажать кнопку **Генерировать**. После чего сгенерированный пароль можно скопировать в буфер обмена.

Шифрование паролей

По умолчанию Password Commander хранит пароли поль зователя в незашифрованном виде. Как сказано в **Справке** программы, данные пользователя сначала проходят этап об фускации (т.е. запутывания, от англ, obfuscate—запутывать, озадачивать, сбивать с толку, ставить в тупик), а потом сжи маются алгоритмом LHA. Такая схема позволяет обеспечить защиту данных, т.е. не дает в явном виде увидеть пароли, но принципиально не является шифрованием, а потому может быть легко расшифрована спецслужбами и заинтересованны ми лицами. Конечно, вы можете просто установить Password Commander с базами данных паролей в контейнер программы TrueCrypt и обеспечить, тем самым, надежную защиту базы паролей. Однако программа Password Commander позволяет подключать плагины для шифрования базы паролей. На стра нице **http://pascom.ru/download.html** можно скачать архив с одним из самых надежных алгоритмов шифрования Blowfish или целый пакет PC Plugins Powerpack, который содержит около 40 различных плагинов симметричного шифрования: 3Way, Blowfish, Cost, IDEA, TEA, Twofish, Cast 128, Cast 256, DES Triple 24byte, RC2, RC4, RC5, RC6, Rijndael и др.

Плагины представляют из себя dll-библиотеки, разработанные по определенной спецификации! Для установки плагина шифрова ния достаточно скопировать его в папку **{Папка с про граммой}\Plugins\Encryption** (обычно это C:\Program Files\Password Commander\Plugins\ Encryption), после чего плагин готов к использо ванию.

Для установки **PC Plugins Powerpack** скачайте и разархиви руйте zip-архив, в нем окажется единственный exe-файл, который следует запустить. В появившемся мастере обычно ничего не тре буется от вас, кроме как нажимать кнопку Next (Далее). Мастер дол жен самостоятельно определить папку, в которую необходимо устано-

вить плагины, так что от вас даже не потребуется копировать их само стоятельно.

Теперь вы можете найти в меню программы **Опции —» На стройки** и в открывшемся окне перейти в раздел **Аккаунт.** Устано вив опцию **Использовать плагин,** вы можете выбрать в списке ал горитм шифрования (рис. 8).

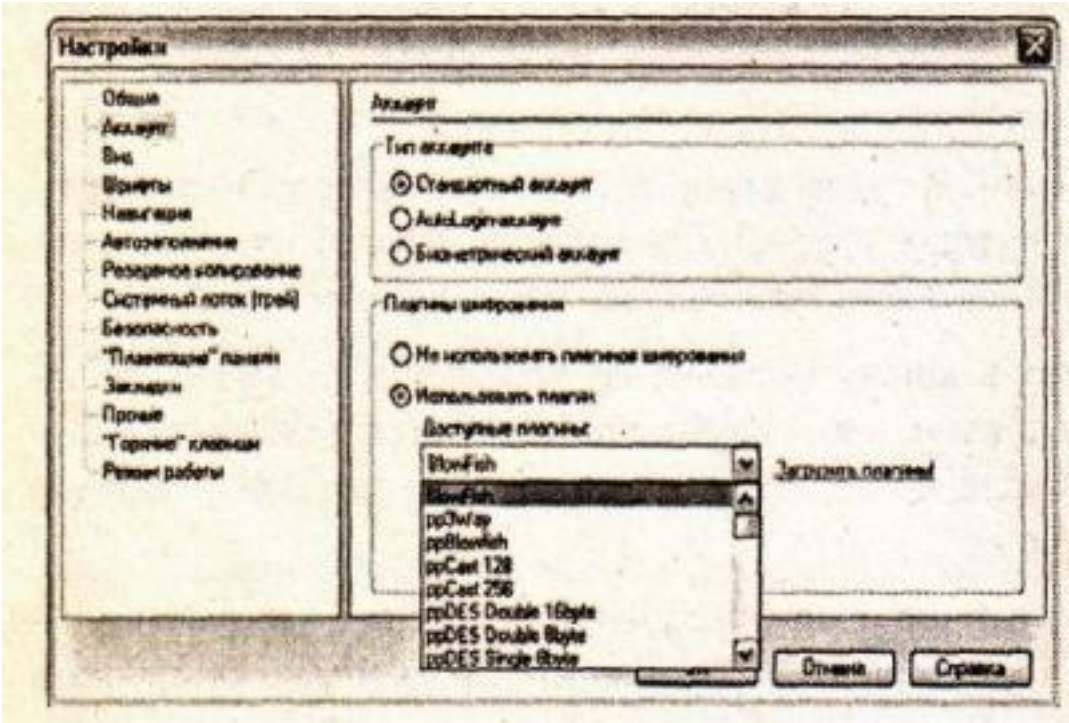

Рис.8 Выбор алгоритма шифрования паролей

После нажатия кнопки ОК плагин немедленно начнет рабо тать, т.е. зашифрует ваши пароли выбранным алгоритмом. Теперь база данных паролей на диске будет постоянно в зашифрованном состоянии. Даже если во время дальнейшей вашей работы про грамма завершится аварийно, например, отключится компьютер, база паролей все равно останется зашифрованной.

Для программистов разработчики программы предоставляют возможность написать собственный плагин шифрования для того, чтобы быть уверенным в полной безопасности своих данных. Для этого на странице **http://pascom.ru/download.html** можно скачать "Пособие по написанию плагинов шифрования".

Пасскарты

Пасскарта (Passcard) представляет собой файл, в который мо жет быть сохранена любая запись, папка или группа. Пасскарта за щищается паролем и может быть зашифрована с использвоанием любого установленного плагина шифрования.

Пасскарта — это удобный способ безопасного переноса дан ных между разными аккаунтами. В Password Commander реализо ваны механизмы синхронизации, позволяющие импортировать данные даже из разнотипных групп.

Для сохранения данных (записи, папки, группы) в пасскарту нужно воспользоваться меню **Правка —» Сохранить в Пасскарту.** Для извлечения данных из пасскарты воспользоваться меню **Файл — » Загрузить из Пасскарты.**

Практическое задание

Цель работы: изучить методику создании записей, генерации и шифрования паролей и автозаполнения форм web-страниц с по мощью программы Password Commander.

Порядок выполнения работы:

1) Создайте папку с именем **Аккаунт**.

2) Рассмотрите демонстрационный пример в программе Password Commander. Обратите внимание, какие графические обо значения имеют группы и записи.

3) Создайте новый аккаунт в программе Password Com mander под именем «**Электронная почта и сайты**» и сохраните его в папку с именем **Аккаунт**. При создании аккаунта используй те режим шифрования паролей с помощью алгоритма Blowfish.

4) В главном окне созданного аккаунта создайте новую группу с именем «**Электронная почта**».

5) В созданной группе создайте две записи с именами Ivan2010@mail.ru и Petr2010@mail.ru. При создании записи Ivan2010@mail.ru введите логин Ivan2010 и пароль **r123t235**. При

создании записи Petr2010@mail.ru введите логин Petr2010 и па роль

s367n861.

6) Создайте папку с именем «**Рассылка**» и перетащите мышью запись Ivan2010@mail.ru в данную папку.

7) Создайте новую группу с именем «**Сайты**».

8) В созданной группе создайте запись с именем **do.swsu.org.** При этом используйте логин и пароль, предназначен ные для входа в ваш личный кабинет на сайте ЮЗГУ.

9) С помощью режима «**Автозаполнение**» автоматически заполните логин и пароль формы Web-страницы, предназначенной для входа в ваш личный кабинет на сайте ЮЗГУ. Разберем данный пункт более подробно:

- сделайте нужную запись активной, затем выберите команду «**Изменить»;**

- выберите вкладку «**Автозаполнение**», затем нажмите кноп ку «**Добавить**»;

- выберите режим «**Автозаполнение в Веб-страницу**»; - через буфер обмена скопируйте URL адрес Web-страницы, предназначенной для входа в ваш личный кабинет на сайте ЮЗГУ; - с помощью кнопки «**Выбрать**» укажите скрипт автозапол нения **%Логин%{Tab}%Пароль%{Enter}**;

- загрузите страницу с Web-формой, а сверху загрузите окно с программой Password Commander;

- сделайте запись активной и в главном меню выберите ко манду **«Автозаполнение»;**

- при этом автоматически заполняется логин, пароль и загру жается нужная страница сайта, то есть вы входите в свой личный кабинет.

10) Сгенерируйте 4 пароля с помощью генератора паролей: - случайный пароль, устойчивый к взлому;

- легко запоминаемый пароль по словарю;

- генерация по шаблону, для этого сначала надо задать шаб лон, пользуясь кнопками;

- генерация по слову и ключу.

11) Сохраните запись Ivan2010@mail.ru в пасскарту. Для сохранения данных в пасскарту нужно использовать команду **Правка —» Сохранить в Пасскарту.** При этом надо указать путь,

где располагается файл пасскарты и указать пароль к файлу пасскар ты.

12) Удалите запись Ivan2010@mail.ru, а затем загрузите дан ную запись из пасскарты. Для извлечения данных из пасскарты ис пользовать команду **Файл —» Загрузить из Пасскарты.**

Список контрольных вопросов

1) Приведите примеры программ, предназначенных для хранения паролей? Какие из них имеют русский интерфейс? 2) Объясните, что такое аккаунт в программе Password Commander?

3) Для какой цели используются группы в программе Pass word Commander?

4) Какие поля по умолчанию используются в записях? Можно ли добавить дополнительные поля в записях? 5) Каким образом происходит автозаполнение форм в Web страницах?

6) Как будет выглядеть скрипт автозаполнения, если в Web-форме необходимо заполнить следующие поля: имя, фамилия, адрес e-mail, логин, пароль.

7) Какие типы паролей можно создавать с помощью гене ратора паролей? Дайте их краткую характеристику. 8) В каком виде хранятся пароли в программе Password Commander по умолчанию?

9) Как зашифровать пароли в программе Password Com mander? Какие алгоритмы шифрования могут быть при этом ис пользованы?

10) Объясните, что такое пасскарта в программе Password Commander?

Список литературы

1. Нестеров С.А. Основы информационной безопасно сти[Электронный ресурс] : учебное пособие / С.А. Нестеров - СПб : Издательство Политехнического университета, 2014. - 322 с. // Ре жим доступа -http://biblioclub.ru/index.php?page=book&id=363040

2. Грибунин В. Г. Комплексная система защиты информа ции на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

3. Тихонов В. А. Информационная безопасность: концеп туальные, правовые, организационные и технические аспекты [текст]: учебное пособие / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. - 528 с.

4. Садердинов А. А. Информационная безопасность пред приятия[Текст]: учебное пособие/ А. А. Садердинов, В. А. Трайнев, А. А. Федулов. 2-е изд. – М.: Дашков и К., 2004. - 336 с.

5. Игнатьев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография.- Ста рый Оскол: ТНТ, 2005. – 552 с.

6. Безбогов А. А., Яковлев А. В., Шамкин В. Н. Методы и средства защиты компьютерной информации [электронный ре сурс]: Учебное пособие. – Тамбов: Издательство ТГТУ, 2006.- 196 с. /Электронная библиотека «Единое окно доступа к образова тельным ресурсам» - http://window.edu.ru

7. Шаньгин В. Ф. Защита компьютерной информации. Эф фективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с.

8. Скляров И. С. Хакерские фишки. – М.: Лори, 2008. – 384 с.