ВИДЫ ИНФОРМАЦИИ. ОСНОВНЫЕ СВОЙСТВА.

31.10.2020

ПРЕПОДАВАТЕЛЬ: ГОЛОВЧЕНКО ДАРЬЯ АНДРЕЕВНА

ИНФОРМАЦИЯ – сведения, независимо от формы их представления.

Основной Федеральный Закон в области защиты информации – ФЗ 149 «Об информации, информационных технологиях и о защите информации».


Информация
Общедоступная информация
Информация с ограниченным доступом
Конфиденциальная информация
- Персональные данные
- Все виды тайн, кроме государственной
- Интеллектуальная собственность
Государственная тайна
- Секретно
- Совершенно секретно
- Особая важность

КАКИЕ СВЕДЕНИЯ ДОЛЖНЫ БЫТЬ ВСЕГДА ОБЩЕДОСТУПНЫМИ?

1) Чрезвычайные происшествия и катастрофы;
2) Состояние окружающей среды;
3) Золотой запас РФ;
4) Состояние здоровья высших должностных лиц;
5) Нарушение прав и свод граждан;
6) Привилегии и компенсации;
7) Факты нарушения законности органами гос. власти.

ГОСУДАРСТВЕННАЯ ТАЙНА

- сведения, защищаемые государством в области:

1) военной;

2) внешнеполитической;

3) экономической;

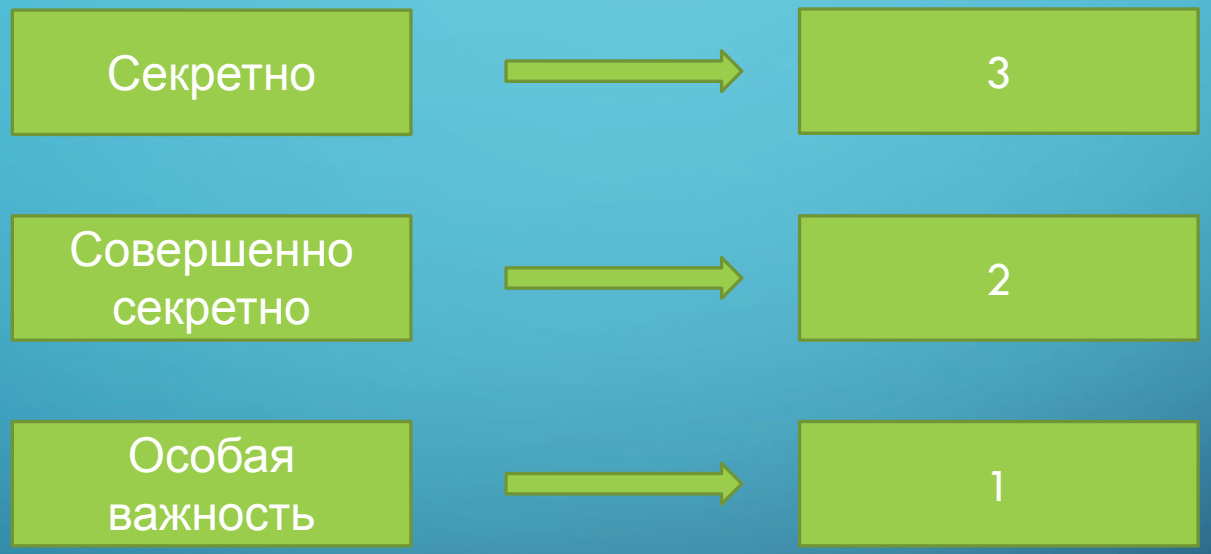
4) разведывательной;

5) контрразведывательной;

6) оперативно-розыскной

деятельности, распространение которых может нанести ущерб безопасности РФ.

ГРИФ СЕКРЕТНОСТИ И ДОПУСК



ПАРОЛЬНАЯ ЗАЩИТА ИНФОРМАЦИИ. *«НИКТО КРОМЕ ВАС»*

31.10.2020

ПРЕПОДАВАТЕЛЬ: ГОЛОВЧЕНКО ДАРЬЯ АНДРЕЕВНА

Пароль представляет собой последовательность символов некоторого алфавита и специальных знаков. Последовательность должна удовлетворять ограничению на наименьшую и наибольшую длину.

ИДЕНТИФИКАЦИЯ. АУТЕНТИФИКАЦИЯ. АВТОРИЗАЦИЯ.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Идентификатор доступа - уникальный признак субъекта или объекта доступа.

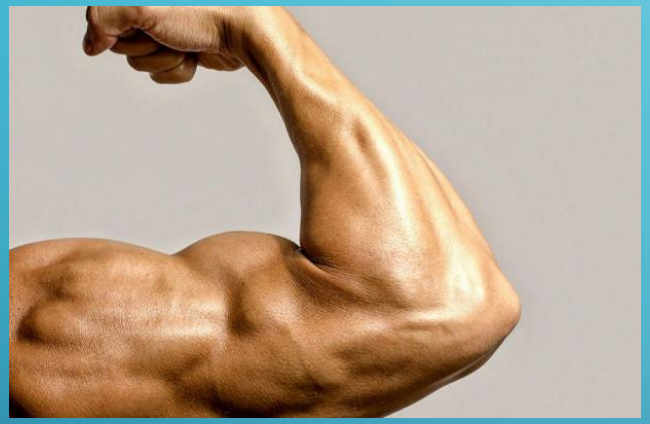
Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Авторизация – предоставление доступа.

ИНТЕРЕСНЫЙ ФАКТ

Швейцарскому исследователю Филиппу Ёкслину удается взламывать алфавитно-цифровые пароли Windows в среднем за 13,6 секунды. Для взлома использовался компьютер на базе процессора Athlon XP 2500+ с 1,5 Гб оперативной памяти. Таблица, в которой хранились варианты паролей, занимала 1,4 Гб и полностью загружалась в оперативную память компьютера, что позволило существенно поднять скорость взлома. При размере таблицы в 20 Гб и наличии в пароле букв, цифр и 16 спецсимволов пароль взламывается, в среднем, за 30 секунд.

КАК ЖЕ СДЕЛАТЬ ПАРОЛЬ СИЛЬНЫМ?



1. Длинный пароль
2. Использование разного регистра
3. Использование специальных символов
4. Использование цифр
5. Случайный (без системы)
6. Не использованный ранее
7. Нигде не фиксировать пароль
8. Обновлять
9. Не повторять при обновлении
10. Ограничение числа попыток ввода

НЕ РЕКОМЕНДУЕТСЯ

1. Использовать своё идентификационное имя в пароле в каком бы то ни было виде
2. Использовать своё ФИО
3. Имена близких родственников и питомцев
4. Информацию о себе, которую легко можно получить. Она включает номера телефонов, номера лицевых счетов, номер вашего автомобиля, название улицы, на которой вы живете, и т.д.;
5. Пароль из одних цифр или из одних букв;
6. Слово, которое можно найти в словарях
7. Записывать свой пароль
8. Научитесь быстро набирать свой пароль (не глядя)

СПОСОБЫ СОСТАВЛЕНИЯ ХОРОШЕГО ПАРОЛЯ

1. *выберите строку или две строки из песни или поэмы и используйте первую букву каждого слова, добавьте цифры (спецсимволы);*

Иван Родил Девчонку

Велел Тащить Пелёнку

нРуВьП1

Мороз и солнце

День чудесный

Ещё ты дремлешь

Друг прелестный

МисД4ЕтдДп

СПОСОБЫ СОСТАВЛЕНИЯ ХОРОШЕГО ПАРОЛЯ

2. выберите известное изречение (поговорку, слоган и т.п.) и используйте каждую четвертую букву, добавьте цифры (спецсимволы);

Посеешь привычку - вырастишь характер.

Ев-АА4

Всё приходит вовремя для того, кто умеет ждать.

Ёивяг,оеА

СПОСОБЫ СОСТАВЛЕНИЯ ХОРОШЕГО ПАРОЛЯ

3. замените в слове одну согласную и одну или две гласных, добавьте цифры (спецсимволы);

Исходное слово: Антананариву

Меняем буквы: а-у; т-ч; в-ф

Цифра: количество букв А в исходном слове.

Пароль: **Унчунунурифа4**

СПОСОБЫ СОСТАВЛЕНИЯ ХОРОШЕГО ПАРОЛЯ

- 4. *выберите два коротких слова и соедините их вместе со знаком пунктуации между ними, добавьте цифры (спецсимволы).*
  Исходные слова: мир, мастер, виза
- Цифры: 3 (так как 3 исходных слова)
- Пароль: **Мир3Мастер-Виза**

ЗАКЛЮЧЕНИЕ

В заключение необходимо отметить существование "парадокса человеческого фактора". Состоит он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Действительно, необходимость ввода пароля каждый раз при входе в систему, не говоря уже о необходимости запоминать сложную знаковую последовательность, удобством не является. Единственной мерой противодействия указанному обстоятельству является формирование у пользователей грамотного подхода к вопросам обеспечения безопасности информации.

ЗАДАНИЕ:

1) Придумайте пароль на основе этих 4-х способов.

2) Придумайте свой собственный способ, не забывая правил составления пароля

МЕНЕДЖЕР ПАРОЛЕЙ

Менеджер паролей – программное обеспечение, которое помогает пользователю работать с паролями и PIN-кодами от различных информационных систем, не запоминая их.

ДЛЯ ЧЕГО СОЗДАВАЛИСЬ?

Приложения для управления паролями изначально разрабатывались чтобы помочь пользователям организовать и шифровать пароли для учетных записей в Интернете на нескольких устройствах. Это лучшая безопасная альтернатива повторному использованию тех же двух или трех паролей.

ПРЕИМУЩЕСТВА МАСТЕРА-ПАРОЛЕЙ

- защита от фишинга

- использование уникальных паролей для разных сервисов и приложений - защита от «случайного пользователя» удобство

- кроссплатформенность

- менеджеры паролей работаю с самыми популярными браузерами (Firefox, Safari,Chrome, Internet Explorer и др.);

- чтобы повысить уровень безопасности менеджера паролей, на некоторых современных приложениях можно включить двухфакторную аутентификацию;

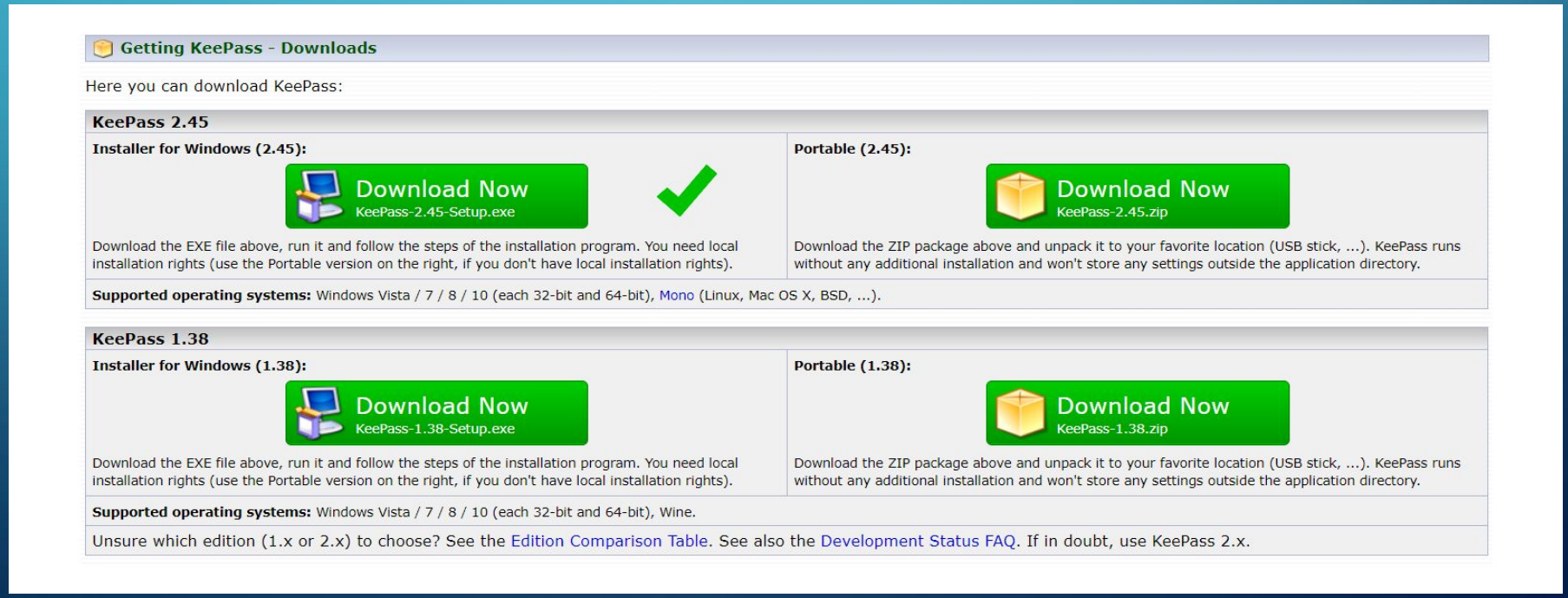
- менеджеры могут хранить все виды данных

НЕДОСТАТКИ МАСТЕРА-ПАРОЛЕЙ

- использование только одного основного пароля для входа в менеджер паролей
- основной пароль может быть атакован и обнаружен при использовании кейлоггера
- генератор паролей в менеджере не использует криптографически безопасный генератор случайных чисел. Этот фактор есть в некоторых менеджерах, не во всех

ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

Скачать плагин и произвести установку можно с официального сайта: https://keepass.info



Getting KeePass - Downloads

Here you can download KeePass:

KeePass 2.45

Installer for Windows (2.45):

Download Now
KeePass-2.45-Setup.exe

Download the EXE file above, run it and follow the steps of the installation program. You need local installation rights (use the Portable version on the right, if you don't have local installation rights).

Portable (2.45):

Download Now
KeePass-2.45.zip

Download the ZIP package above and unpack it to your favorite location (USB stick, ...). KeePass runs without any additional installation and won't store any settings outside the application directory.

Supported operating systems: Windows Vista / 7 / 8 / 10 (each 32-bit and 64-bit), Mono (Linux, Mac OS X, BSD, ...).

KeePass 1.38

Installer for Windows (1.38):

Download Now
KeePass-1.38-Setup.exe

Download the EXE file above, run it and follow the steps of the installation program. You need local installation rights (use the Portable version on the right, if you don't have local installation rights).

Portable (1.38):

Download Now
KeePass-1.38.zip

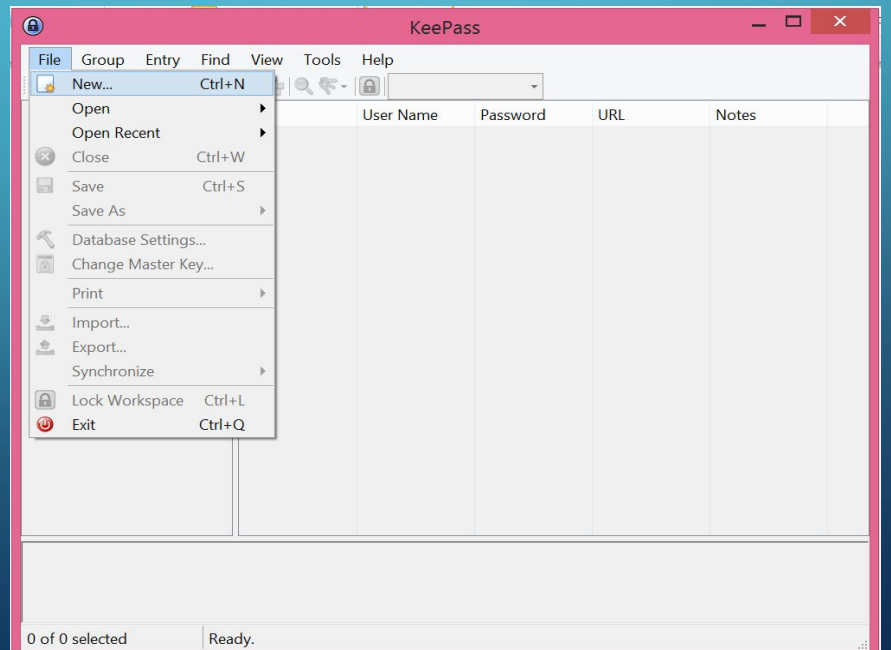
Download the ZIP package above and unpack it to your favorite location (USB stick, ...). KeePass runs without any additional installation and won't store any settings outside the application directory.

Supported operating systems: Windows Vista / 7 / 8 / 10 (each 32-bit and 64-bit), Wine.

Unsure which edition (1.x or 2.x) to choose? See the Edition Comparison Table. See also the Development Status FAQ. If in doubt, use KeePass 2.x.

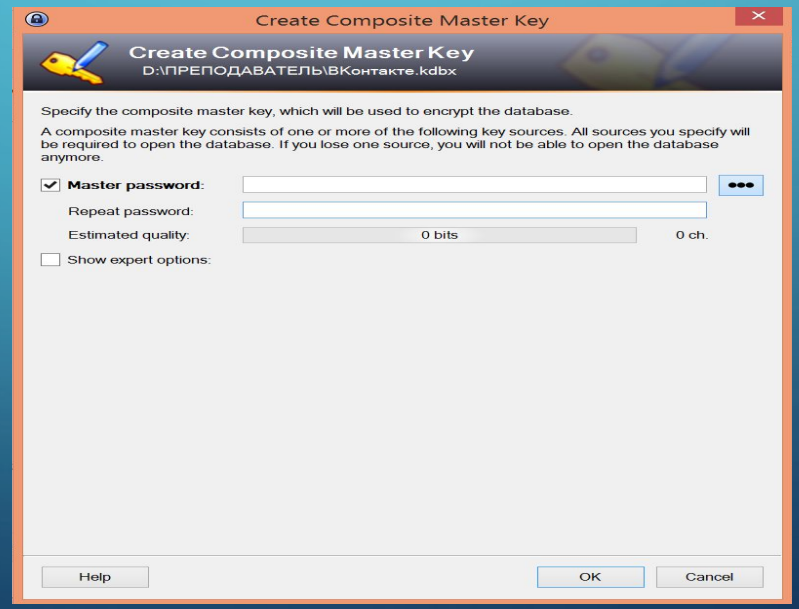
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

Интерфейс предельно лаконичен. Начинается все с создания базы данных. Сохраняем базу в любом месте. Можно сразу назвать её, если баз будет несколько. Это упростит задачу поиска.



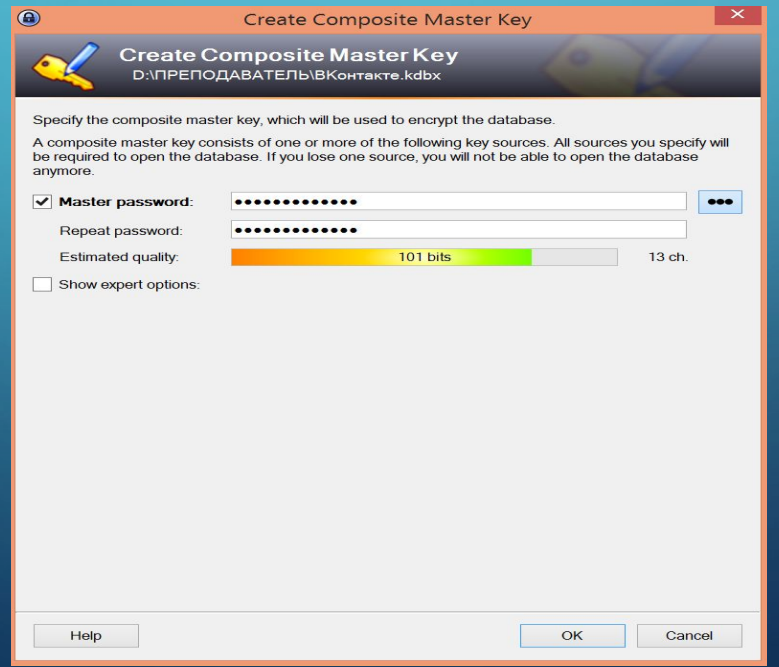
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

После того, как выбран корень сохранения у вас появится окно с мастером-паролей. Это единственная защита, поэтому пароль должен быть предельно сложным, но запоминающимся.



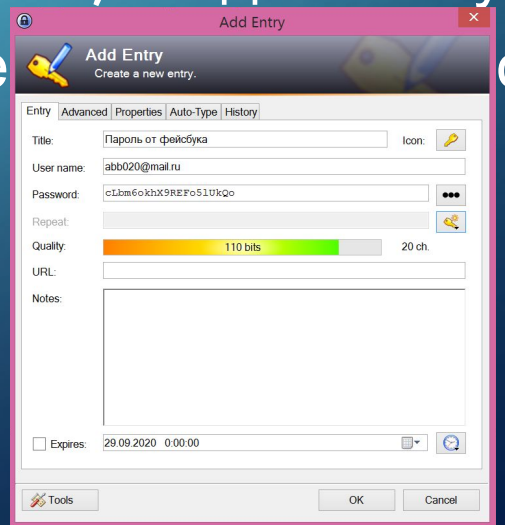
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

Если забыть мастер-пароль, то все остальные пароли будут более недоступны. Обратите внимание, что когда вы будете создавать мастер-пароль, то увидите степень стойкости вашего пароля.



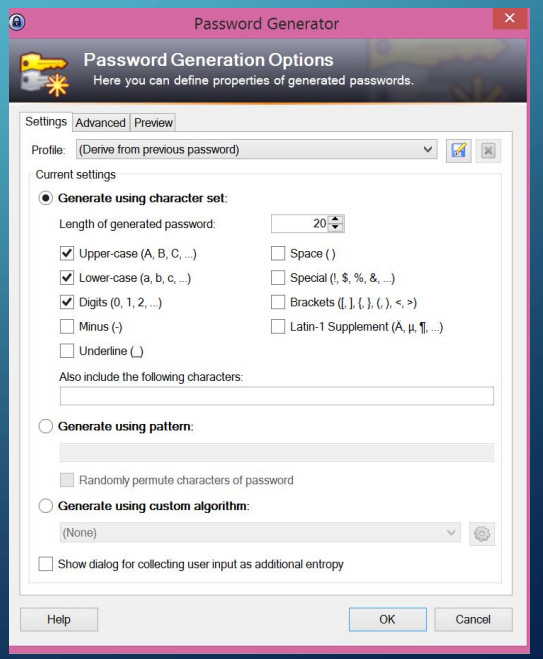
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

Чтобы начать использовать программу вам необходимо нажать правой клавишей мыши и выбрать «Add Entry». В окне «Title» название, чтобы понимать какой пароль к чему относится. В окне «User name» записываем логин с сайта (обычно это или электронная почта или номер телефона). Будьте внимательны, вы должны уже быть зарегистрированы. «Password» - уже сгене оль



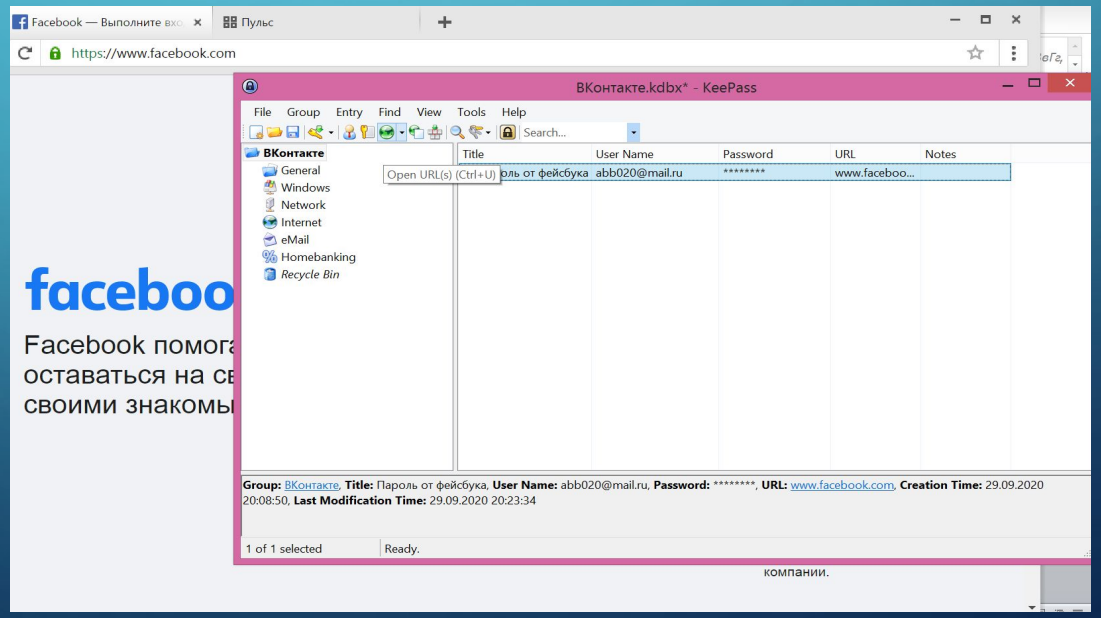
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

- Если он не подходит, то можно сгенерировать новый. Причем есть настройки самого генератора, которыми вы можете управлять URL адрес лучше занести в одноименную строку, так как это облегчит в дальнейшем использования пароля.
-



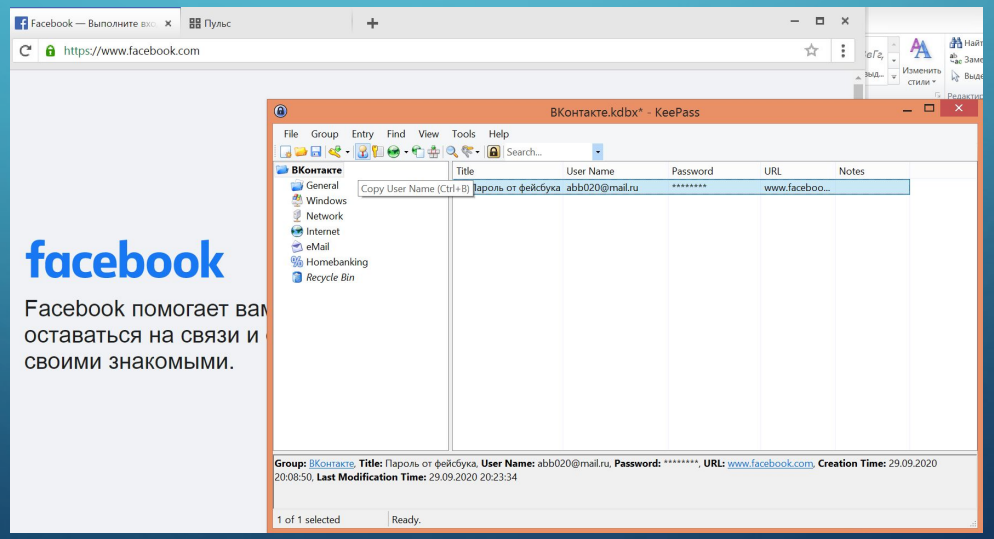
ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

После сохранения пароля попадаем на главную страницу нашей программы. Нажимаем на только что созданный пароль и в окне меню видим значок в виде земного шара. Нажимаем на него и попадаем на сайт



ПРАКТИЧЕСКАЯ РАБОТА. МЕНЕДЖЕР ПАРОЛЕЙ KEEPASS

На сайте нас просят для авторизации ввести логин и пароль. Возвращаемся в KeePass и находим на панели управления значок с изображением человека, это и будет логин



ЗАДАНИЯ

- 1. Скачайте KeePass, произведите установку.
- 2. Создайте базу данных в которой будет пароли от почтового ящика.
- 3. Перенесите из корневой установочной папки базу данных к себе на флеш-карту.
- 4. Попробуйте использовать KeePass с флеш-карты.
- 5. Попробуйте не работать с программой KeePass в течение 6 минут. Что произойдет?

ВОПРОСЫ

- Для чего нужны менеджеры паролей?
- Найти еще 2 менеджера паролей с криптографическим генератором случайных паролей.
- Назовите уязвимости и преимущества менеджеров паролей.
- Что будет, если скопированный логин и пароль из KeePass вставить не сразу на URL-адресе?
- Для чего есть правило 12 секунд в KeePass?
- Как восстановить мастер-пароль в KeePass?

ВЫВОДЫ

На сегодняшний день общая безопасность менеджеров паролей является дискуссионной. С одной стороны, в целях безопасности настоятельно рекомендуется использовать уникальные безопасные пароли для разных учетных записей. С другой стороны, если один мастер-пароль скомпрометирован или может быть восстановлен, злоумышленник получает доступ к полной базе данных, содержащей все пароли пользователя и учетные данные аутентификации.

ТЕМЫ РЕФЕРАТОВ

1. Как избежать вирусных атак на свой компьютер?
2. Фрод – мошенничество с использованием технологий.
3. Киберискусство – настоящие ли искусство?