Тема: 3.7 Аппаратное и программное обеспечение защищенных компьютерных систем.

Учебные вопросы:

1. Организация безопасного хранения паролей в защищаемых компьютерных системах.
2. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения. Порядок удаления информации программными способами без возможности ее восстановления.
3. Проверка и удаление следов активности пользователя в системе.

1. Организация безопасного хранения паролей в защищаемых компьютерных системах

Краткие теоретические сведения:

Рано или поздно каждый пользователь или администратор информационной системы (ИС) сталкивается с проблемой безопасности при хранении и использовании множества паролей (учетных записей) от различных защищенных информационных ресурсов (базы данных, архивы, зашифрованные файлы, криптоконтейнеры, электронные кошельки, облачные сервисы, веб-сайты, тематические форумы, социальные сети, мессенджеры, электронная почта, службы удаленного доступа к ПК и т. д.).

Использование одного сложного, но единого (универсального) пароля от всех ресурсов приведет к тому, что в случае его компрометации будут автоматически скомпрометированы и все остальные защищенные ресурсы ИС либо его компоненты.

При использовании множества несложных и легко запоминающихся паролей злоумышленник сравнительно легко сможет их подобрать или восстановить, получив тем сам несанкционированный доступ к любому из компонентов ИС.

Хранение сложных, и при этом, как правило, плохо запоминающихся паролей в каком-либо ненадежном или незащищенном месте (текстовый файл, электронная таблица, обычный бумажный блокнот и пр.) также существенно снижает уровень информационной безопасности, поскольку указанные носители и средства хранения информации не обладают достаточными атрибутами защищенности от обычной компрометации и риска утраты, утечки, несанкционированной передачи и уничтожения.

Для организации безопасного хранения и использования паролей в защищаемых ИС рекомендуется использовать специальные программы – менеджеры паролей (например: «Keychain», «LastPass», «Dashlane», «1Password», «OneSafe», «Bitwarden», «Keeper», «KeePass» и др.). Их основными функциями являются: безопасное создание, хранение и использование паролей, мультифакторная аутентификация пользователя,

защита от кейлоггеров и программ, следящих за экраном пользователя при вводе паролей, синхронизация на нескольких устройствах и др.

Вместе с тем, менеджеры паролей могут значительно отличаться друг от друга по удобству использования, методам шифрования, вариантам мультифакторной аутентификации и степени общей безопасности приложения.

Одной из наиболее безопасных и функциональных программ, предназначенных для хранения и использования паролей в защищаемых ИС, является бесплатная и распространяемая по лицензии GPL кроссплатформенная программа «KeePass» (https://keepass.info/). Основными преимуществами этой программы являются следующие:

открытый исходный код;

портативность (не требует установки);

защищенный ввод мастер-пароля;

быстрая разблокировка коротким паролем (плагин *KeePassQuickUnlock*);

автонабор паролей с защитой от слежения за клавиатурой;

копирование паролей с частичной защитой от слежения за буфером обмена;

автоматическое резервное копирование без плагинов;

автоматическая облачная синхронизация без плагинов;

двухстраничная авторизация,

интеграция в браузеры, не требующая их настройки (плагин *WebAutoType*);

автоматический переход к подходящей записи (плагин *AutoTypeShow*);

меню выбора браузера (в т.ч. портативного или браузера в песочнице);

запуск из «KeePass'a» приложений с одновременным автонабором (монтирование томов «TrueCrypt», удаленный доступ к ПК и др.);

защищенный процесс «KeePass'a» (запрет чтения памяти и т.п.);

возможность «KeePass'a» работать с правами администратора, но понижать права открываемых им браузеров и других приложений;

работа с несколькими базами, в т.ч. автооткрытие нескольких баз;

использование «KeePass'a» как менеджера закладок;

возможность открывать базу «KeePass'a» без ввода пароля.

Все пароли хранятся в шифрованной базе данных (AES-256), доступ к которой осуществляется по паролю или файлу-ключу (возможно использовать оба варианта одновременно). База паролей хранится в файле, который можно синхронизировать любыми удобными способами (облачные сервисы, сменные носители информации и др.). Возможно использование многоходового преобразования ключа, за счет чего время, необходимое для расшифровки базы, увеличивается, однако это увеличивает и устойчивость к brute-force атакам.

«KeePass» обладает встроенной функцией AutoType (автонабор), позволяющей автоматически вводить пароли в браузерах и других программах. «KeePass» также обладает множеством плагинов, которые в том числе

обеспечивают более тесную интеграцию со всеми основными браузерами (IE, Firefox, Chrome), и предоставляют множество дополнительных функций.

За счет открытости «KeePass» написано множество ПО под различные платформы. На мобильных устройствах есть клиенты «KeePass» на следующих платформах: iOS, Android, WM Classic, Windows Phone 7, Blackberry, и J2ME. Более подробные списки плагинов и стороннего ПО доступны на официальном сайте «KeePass».

Базовый алгоритм работы с программой «KeePass» под ОС Windows можно представить в виде следующей последовательности действий.

1. Установка «KeePass» и русификация

1.1. Скачивание последней версии программы «KeePass» с официального сайта (https://keepass.info/download.html). Рекомендуется выбрать портативную версию последней модификации (в архиве *.zip) (рис. 1).

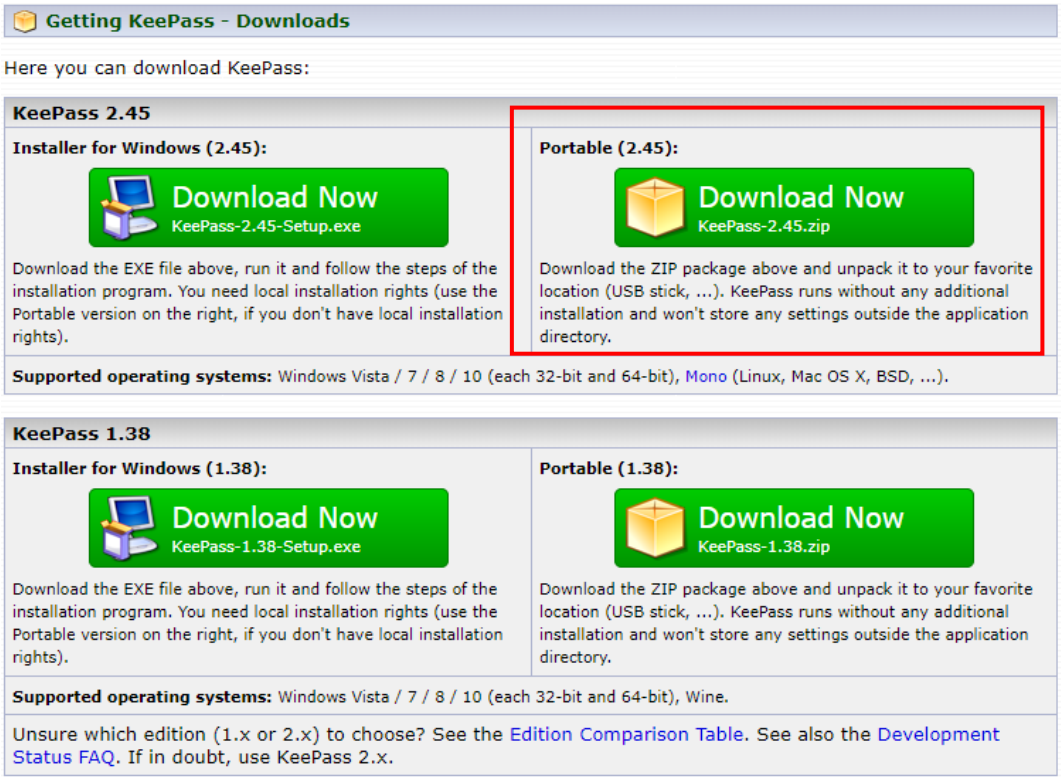


Рис. 1. Скачивание программы «KeePass» с официального сайта

Затем, архив с программой следует распаковать в место предполагаемого запуска программы (HDD, USB и пр.). Для удаленной работы также возможна установка программы на любой облачный диск (Google Drive, Яндекс диск и пр.).

Для русификации программы следует скачать соответствующий файл с переводом с официального сайта (https://keepass.info/translations.html) (рис. 2) и сохранить его в папку с программой (файл имеет вид Russian.lngx).

После этого программу «KeePass» следует запустить (*..\KeePass-2.45\KeePass.exe*), в меню «**View**» выбрать «**Change Language…**» и в

открывшемся окне выбрать *Russian*. Программа предложит перезапустить ее. После подтверждения согласия русификация будет завершена.

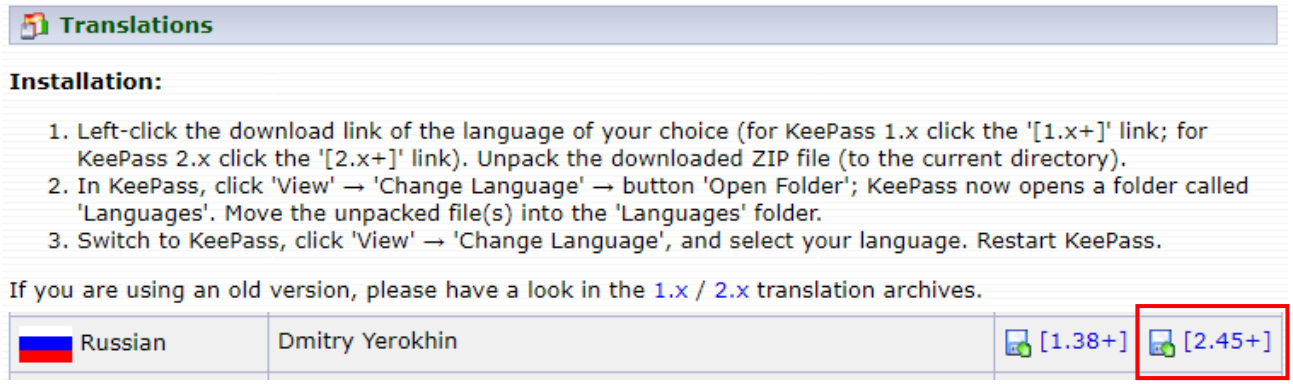


Рис. 2. Скачивание русификатора для программы «KeePass» с официального сайта

2. Проверка подлинности

Для того, чтобы убедиться, что программа не обфусцированная (не скомпрометированная), необходимо проверить цифровые подписи основных ее файлов. У каждого файла *.exe и *.dll в папке *..\KeePass-2.45* следует открыть окно свойств, перейти на вкладку «Цифровые подписи» и удостовериться, что имя подписавшего – *Open Source Developer, Dominik Reichl*. Затем, необходимо выбрать вкладку свойств «Сведения» и удостовериться, что цифровая подпись действительна. При этом следует иметь ввиду, что не иметь подписи могут только файлы плагинов в папке *..\PluginCache*.

3. Создание базы паролей

3.1. Запустите программу «KeePass» (*..\KeePass-2.45\KeePass.exe*).

3.2. Выполните команду **Файл > Создать..** (рис. 3). В открывшемся окне выбираете место где будет храниться ваш файл *.kdbx (база данных) с паролями.

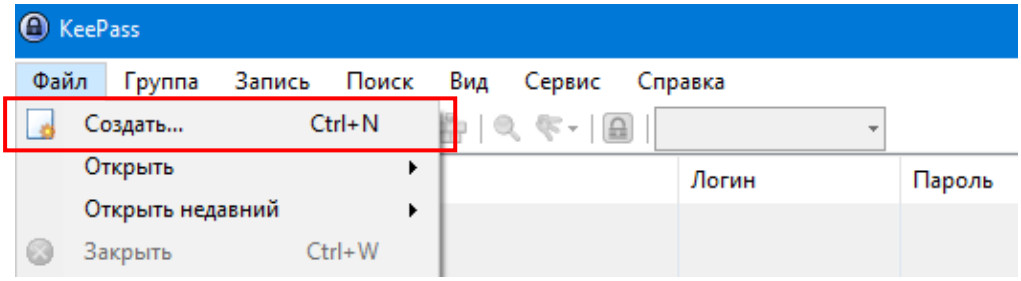


Рис. 3. Создание базы данных «KeePass»

3.3. Создайте составной мастер-ключ для доступа к базе данных паролей (рис. 4).

Для защиты базы данных «KeePass» предлагает 3 варианта, каждый из которых можно использовать по отдельности или же для полной и максимальной защиты – все вместе. Так, введите и подтвердите основной пароль для доступа, который вам необходимо будет запомнить один раз для доступа ко всем паролям. При необходимости выберите либо создайте

средствами программы ключей файл. Можно также дополнительно добавить учетную запись как метод идентификации. Однако, в этом случае вы не сможете получить доступ к файлу паролей с другого компьютера, отличного от того, на котором создавали.

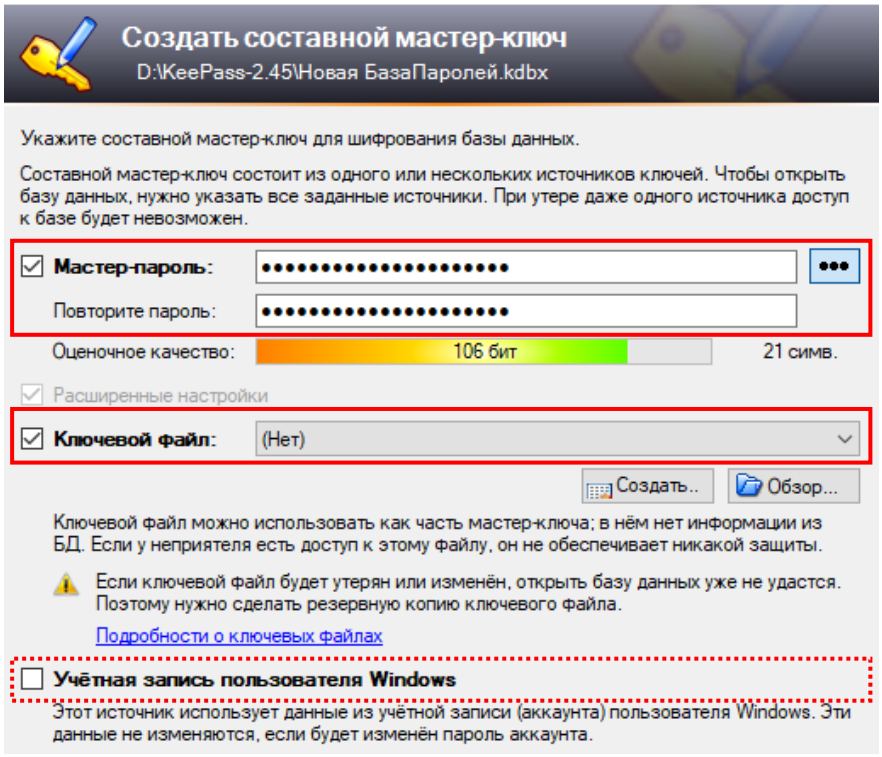


Рис. 4. Создание мастер-пароля от базы данных «KeePass»

После успешного создания базы данных программа «KeePass» автоматически откроет эту базу и в главном окне уже будут созданы примеры записей (рис. 5).

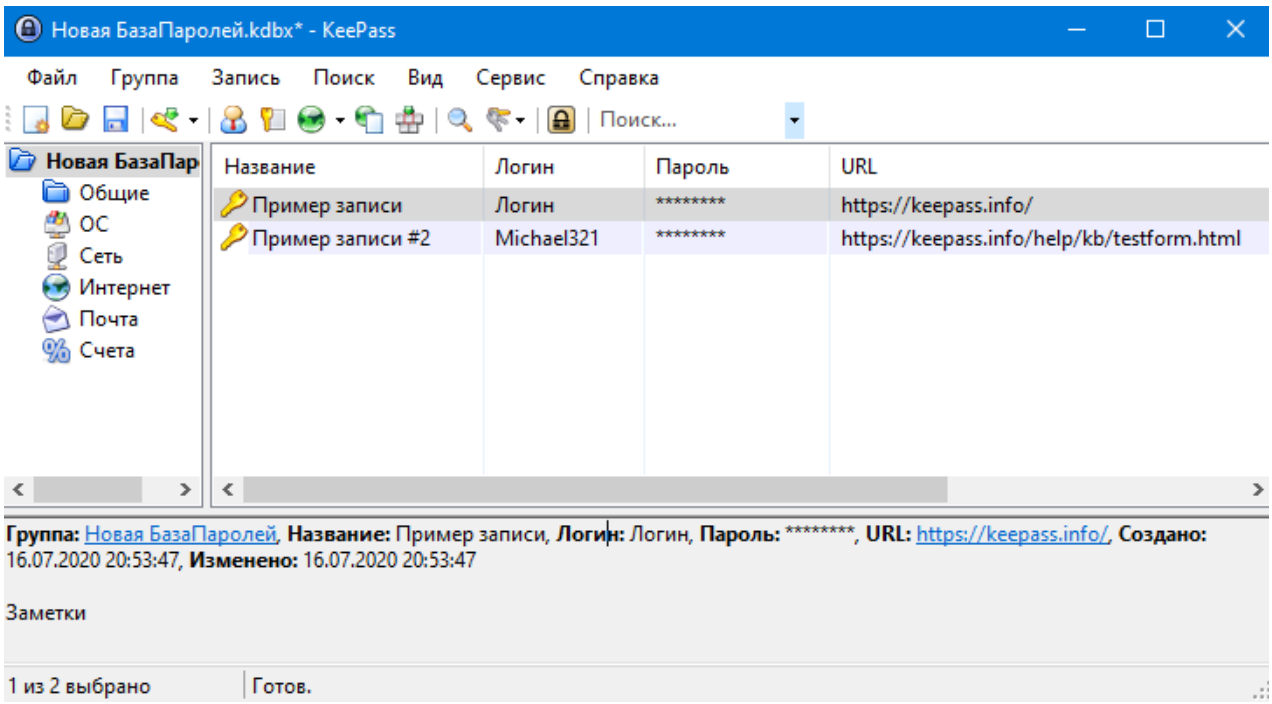


Рис. 5. Основное окно программы «KeePass»

4. Настройка и создание записей

4.1. Перед созданием записей о паролях рекомендуется определить структуру данных для их хранения, а затем – создать необходимое количество групп (каталогов).

Для создания новой группы следует нажать правой кнопкой мыши на той папке, внутри которой необходимо ее создать, и в выпадающем меню выбрать пункт «**Добавить группу**». Затем, в окне добавления группы во вкладке «Общие» ввести имя группы и нажать кнопку «Ок» (рис. 5).

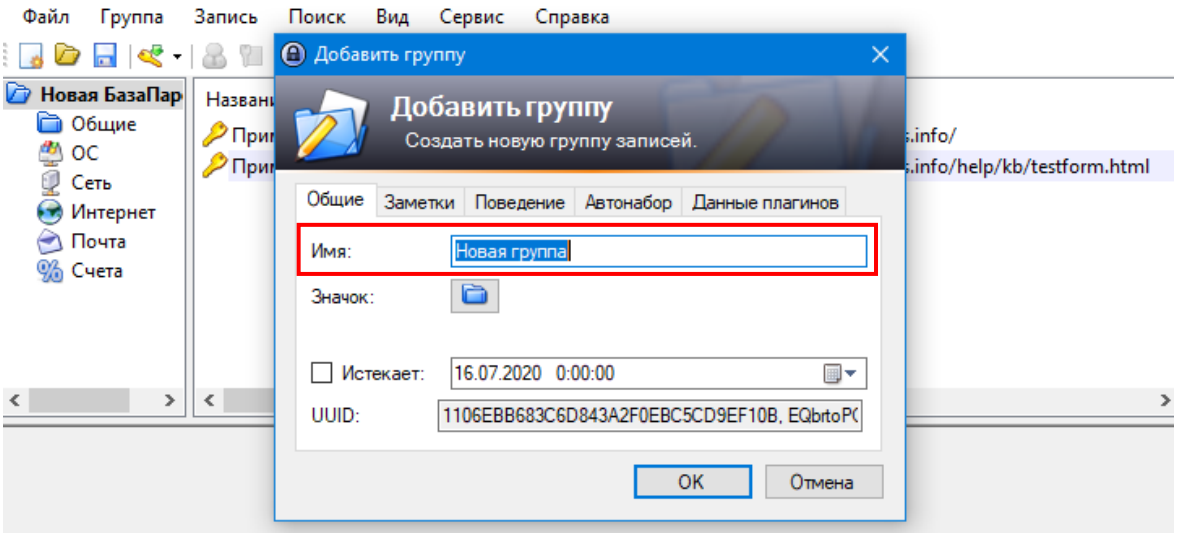


Рис. 5. Добавление новой группы для хранения записей о паролях.

4.2. Для создания новой записи, которая будет хранить все данные о логине, пароле и иную информацию пользователя, следует выполнить следующие действия:

левой клавишей мыши выделить соответствующую папку с записями;

правой клавишей мыши нажать в область программы, отображающую список выбранных записей;

в появившемся контекстном меню выбрать пункт «**Добавить запись..**» (рис. 6).

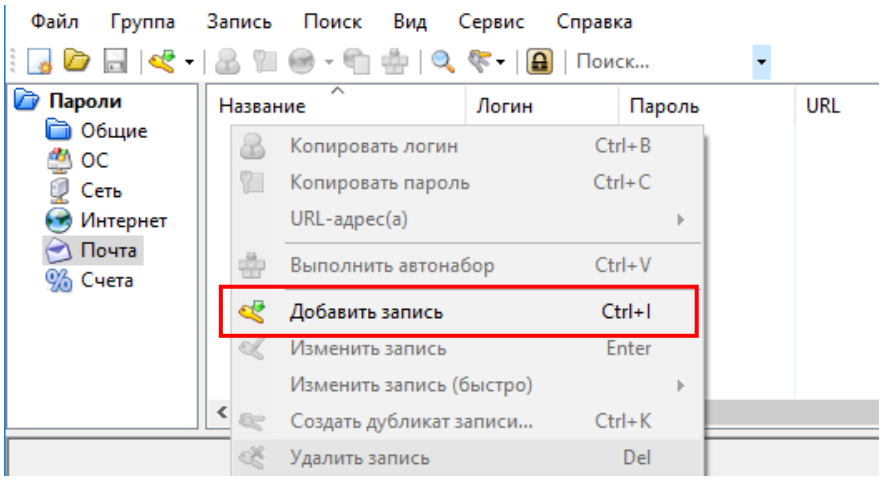


Рис. 6. Добавление новой записи о паролях.

Откроется окно для заполнения данных записи (рис. 7). Основные поля для заполнения доступны на вкладке «Запись».

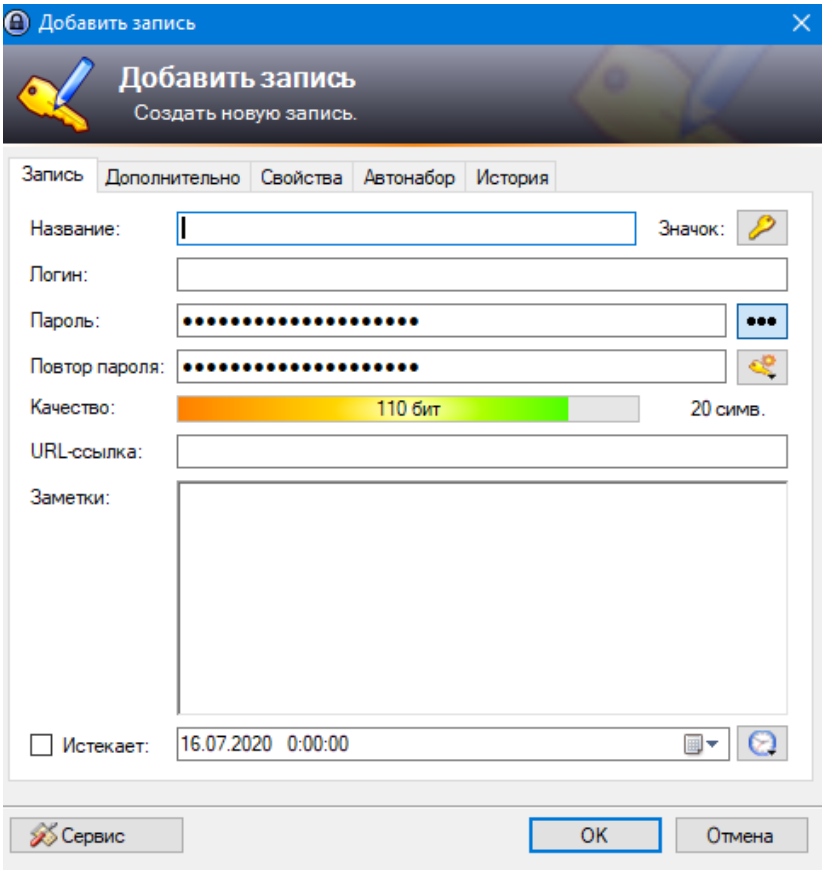


Рис. 7. Добавление новой записи о паролях.

Так, в качестве имени профиля для создаваемого пароля следует заполнить поле «Название», указать логин, вести и подтвердить пароль.

Поле «URL-ссылка» – это либо сайт, на котором будет использоваться логин и пароль либо ссылка на исполняемый файл, требующий ввода логина и пароля в программе.

Кроме того, можно указать срок действия пароля, чтобы своевременно получить напоминание о смене пароля.

4.3. Если создается новая запись и пароль необходимо придумать, в этом случае рекомендуется воспользоваться встроенным генератором паролей (кнопка  справа от поля «Повтор пароля»).

Чтобы воспользоваться этим инструментом без открытия формы создания записи следует выполнить команду **Сервис > Генератор пароля…**

В настройках генератора паролей (рис. 8) можно указать какие символы, буквы прописные и строчные, цифры и специальные символы следует использовать в генерации. Также указывается длина пароля.

После задания настроек генератора пароля необходимо открыть вкладку «Просмотр» и выбрать любой из предложенных в списке вариантов. Если при этом необходимо исключить какой-либо символ из генерации, это можно сделать на вкладке «Дополнительно».

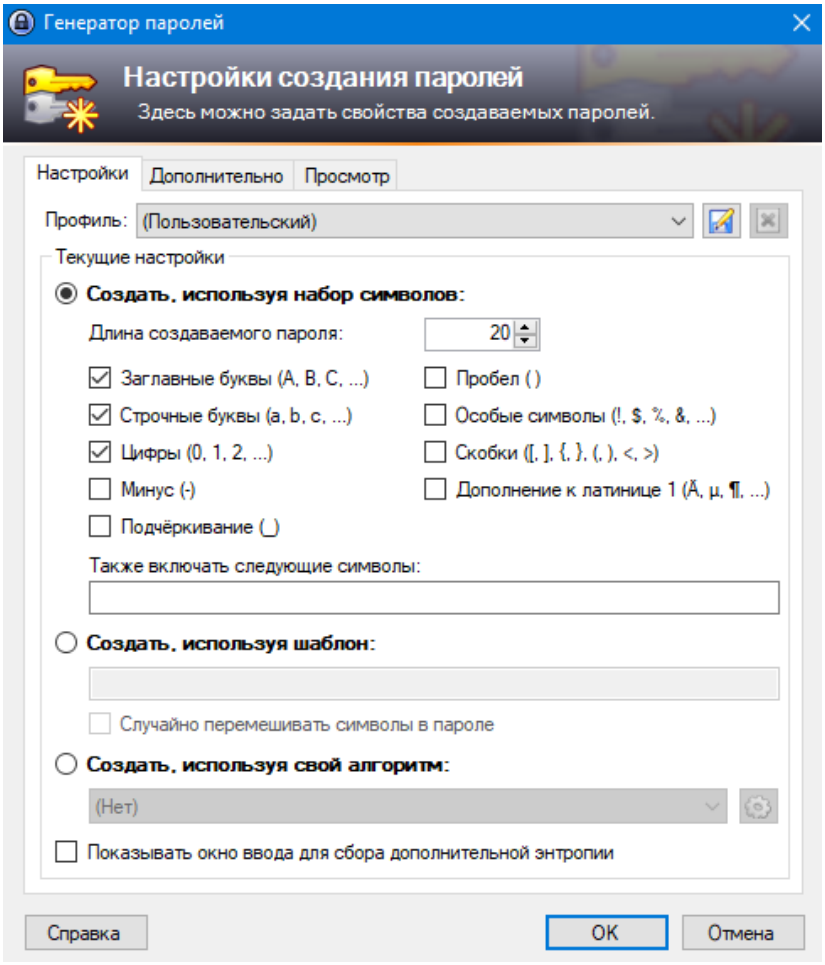


Рис. 8. Генератор паролей в программе «KeePass»

5. Использование записей о паролях в режиме автонабора

Основной алгоритм работы с программой «KeePass» состоит из следующей последовательности действий:

1. Запуск URL выбранной записи либо исполняемого файла с формой для ввода (**Запись > URL-адрес(а)** либо комбинация клавиш **Ctrl+U**) (рис. 16).

2. Возврат фокуса к программе «KeePass» (можно воспользоваться комбинацией клавиш **Ctrl+Alt+K**).

3. Активация функции «Автонабор» (**Запись > Выполнить автонабор** либо комбинация клавиш **Ctrl+V**) (рис. 16).

При необходимости содержимое записи (пароль или логин) можно скопировать в буфер обмена, который через 12 секунд (время по умолчанию) будет очищен (рис. 16).

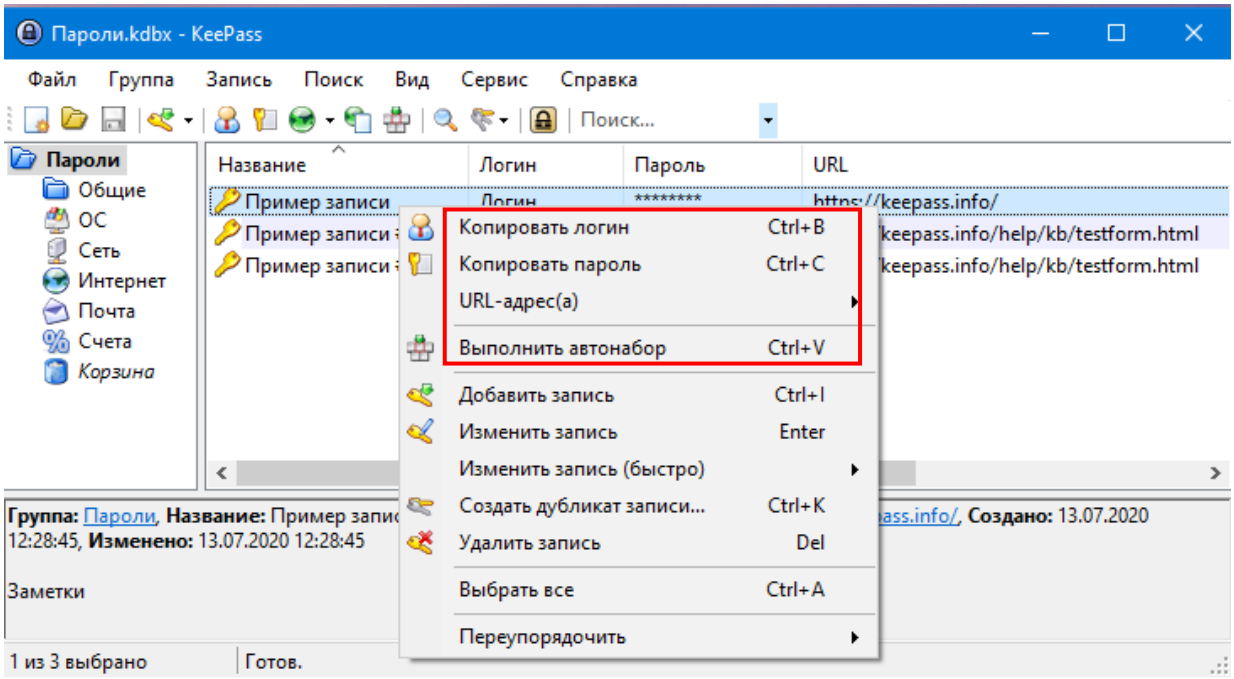


Рис. 16. Использование записей в программе «KeePass»

6. Настройки основных параметров безопасности.

Несмотря на то, что мастер-пароль базы данных «KeePass'a», его хеш и пароли записей защищены в памяти программы шифрованием, а также ключом, которым владеет только операционная система, вредоносная программа, способная изменять память «KeePass'a» или хотя бы взаимодействовать с его оконным интерфейсом, сможет получить и несанкционированный доступ к записям программы.

Для минимизации либо нейтрализации указанных уязвимостей рекомендуется применять следующие защитные меры:

1. Запускать «KeePass» только с правами администратора. Для того, чтобы «KeePass» всегда требовал повышение прав, следует открыть свойства файла *KeePass.exe* и отметить на вкладке «Совместимость» опцию «Выполнять эту программу от имени администратора».

2. Защитить от изменений файлы «KeePass'a», включая конфигурацию и базу. Для этого в свойствах папки программы на вкладке «Безопасность» следует оставить *Полный доступ* только *Системе* и группе *Администраторы*, а группе *Пользователи* – только *Чтение*, *Выполнение* и *Список содержимого папки*.

Альтернативный вариант – поместить папку программы в папку *%ProgramFiles%*.

3. Отключить опцию «Помнить зашифрованный мастер-пароль базы, пока она открыта» **(Сервис > Параметры > Безопасность)**.

4. Включить опцию «Всегда выходить вместо блокирования программы» **(Сервис > Параметры > Безопасность)**.

5. В системном реестре Windows создать раздел *HKLM\Software\Microsoft\Windows\Windows Error Reporting\LocalDumps\KeePass.exe* и в нем параметр *DumpCount* типа *DWORD* со значением = 0. Это отключит создание в каталоге *%LOCALAPPDATA%\CrashDumps* дампа памяти «KeePass'a» при его аварийном завершении.

Для выполнения данной задачи откройте редактор реестра Windows **(Win+R > *regedit* > Enter)** (рис. 17).

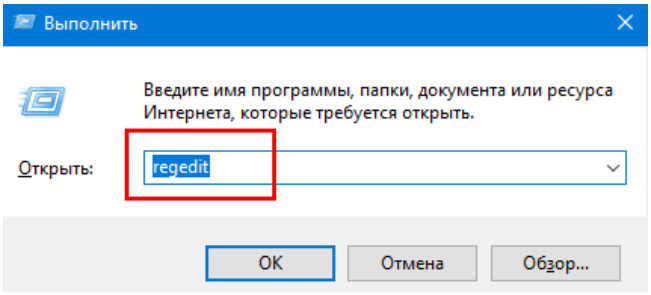


Рис. 17. Запуск редактора реестра Windows

В окне редактора реестра откройте раздел *HKLM\Software\Microsoft\Windows\Windows Error Reporting* (рис. 18).

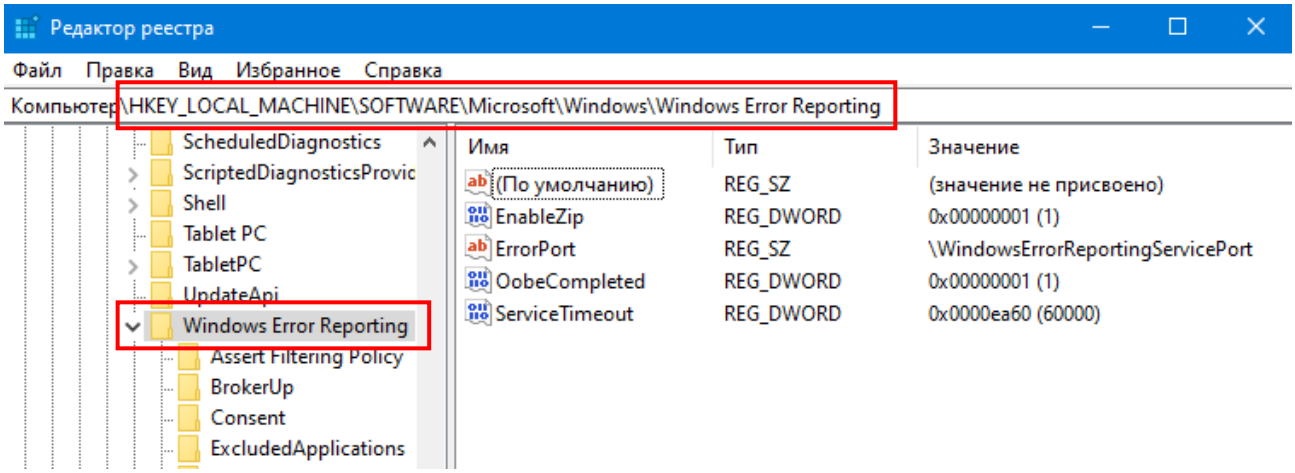


Рис. 18. Редактор реестра Windows

В разделе *Windows Error Reporting* создайте новый раздел *LocalDumps*, а в нем – подраздел *KeePass.exe* (рис. 19).

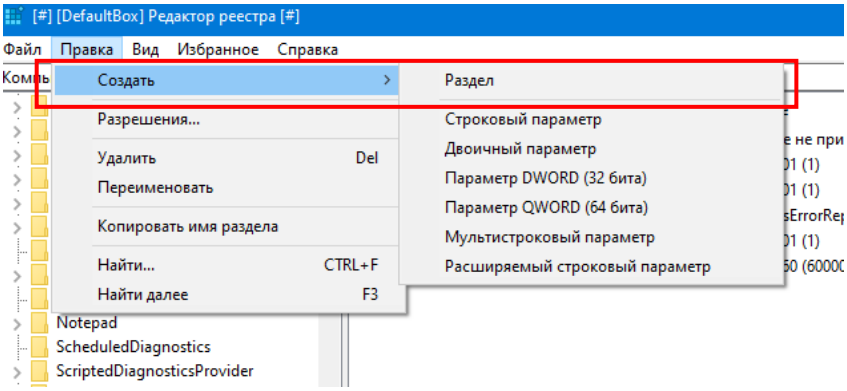


Рис. 19. Создание раздела в реестре Windows

В подразделе *KeePass.exe* создайте параметр *DumpCount* типа *DWORD (32 бита)* (рис. 20). Данному параметру будет присвоено значение по умолчанию = 0 (рис. 21).

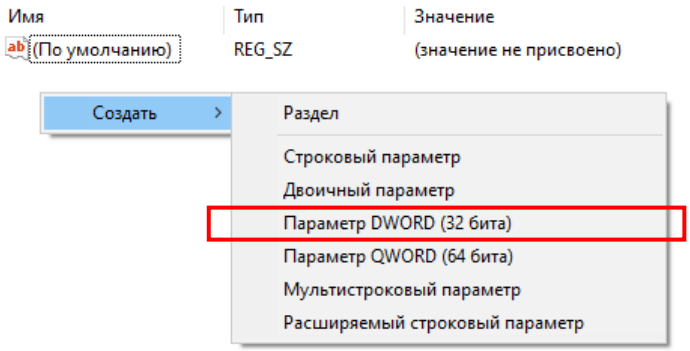


Рис. 20. Создание параметра в разделе реестра Windows

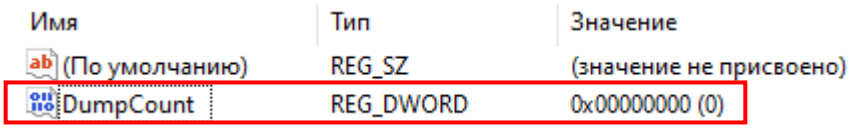


Рис. 21. Значение параметра в разделе реестра Windows

6. В качестве Ключевого файла рекомендуется выбирать файл с большим количеством случайных данных, который ни при каких обстоятельствах не должен быть изменен (иначе вы не сможете открыть базу).

7. Не стоит хранить Ключевой файл в одной папке с «KeePass» или базой паролей. Лучше выбрать файл, который будет одним из многих схожих файлов, находящихся в другой папке и желательно на съемном носителе. Проследите, чтобы имя, расширение, размер и дата файла совпадала с остальными файлами в этой папке.

8. Отключить хранение пути к Ключевому файлу, а также хранение истории. Для этого следует выполнить команду **Сервис** > **Настройки** > **Дополнительно** и отключить параметр «Запоминать источники ключа». А затем во вкладке «Внешний вид» установить для параметра «Запоминать недавно использованные файлы» значение = 0.

9. Отключить сохранение истории недавно использованных документов в Windows.

Настройка основных параметров безопасности программы «KeePass» доступна с помощью команды **Сервис > Параметры**. Набор необходимых параметров безопасности представлен на вкладке «Безопасность» (рис. 22).

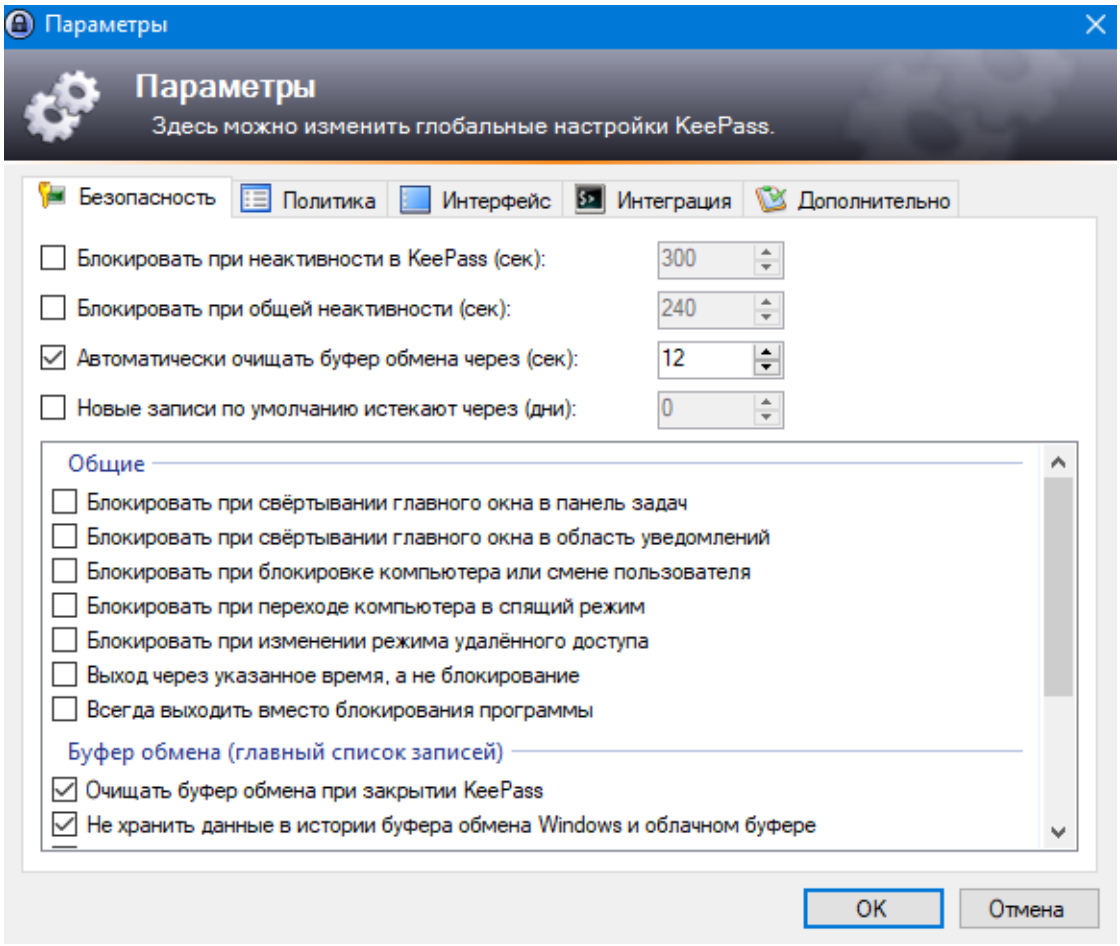


Рис. 22. Настройка параметров в программе «KeePass»

Пользователь может настроить блокировку программы после некоторого периода бездействия, при сворачивании окна, при блокировке рабочего стола или при переходе компьютера в спящий режим. По умолчанию, «KeePass» стирает все данные, скопированные в буфер обмена по истечении 12 секунд. Пользователь может настроить это время или выбрать очистку буфера обмена при выходе.

Чтобы вредоносные программы-кейлоггеры не смогли перехватить ввод мастер-пароля, в разделе «Безопасность» включена опция «Вводить основной пароль в защищенном режиме». На вкладке «Дополнительно» включена опция «Запоминать и автоматически открывать последнюю базу данных при запуске», как по умолчанию; но в то же время отключены опции «Запоминать источники ключа» и «Запоминать рабочие папки», поскольку расположение ключевого файла является приватной информацией.

Набор дополнительных опций позволяет также настраивать и другие параметры программы – от способа идентификации веб-сайтов для заполнения данных до метода отмены сессии автонабора при изменении целевого окна.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.7»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Скопируйте с официального сайта программу «KeePass», установите ее в свою рабочую папку и русифицируйте.
3. Удостоверьтесь в подлинности основных файлов программы «KeePass».
4. Создайте базу данных паролей «KeePass», защитите ее составным мастер-ключом (пароль и ключевой файл, созданный средствами программы). Базу данных сохраните под именем *Курсант.kdbx* в папке *..\KeePass-2.45*.

Сформулируйте рекомендации по выбору и использованию ключевого файла. и укажите их в файл-отчете.

5. Выполните следующие настройки программы «KeePass»:

5.1. Активизируйте:

а) автоматическое очищение буфера обмена через 5 сек;

б) автоматический запуск «KeePass» только с правами администратора;

5.2. Включите опции:

а) «Помнить зашифрованный мастер-пароль базы, пока она открыта»;

б) «Всегда выходить вместо блокирования программы»;

в) «Вводить основной пароль в защищенном режиме».

5.3. Отключите опции хранения пути к ключевому файлу, а также хранение соответствующей истории;

5.4. Выполните защиту файлов «KeePass'a» (включая конфигурацию и базу) от изменений;

5.5. В системном реестре Windows создайте раздел *HKLM\Software\Microsoft\Windows\Windows Error Reporting\LocalDumps\KeePass.exe* и в нем параметр *DumpCount* типа *DWORD* со значением = 0;

5.6. Отключите сохранение истории недавно использованных документов в Windows.

Опишите в файл-отчете функциональное назначение указанных настроек.

6. Создайте группу записей *Пароли > Общие > Учебные*. Укажите срок действия для паролей в этой группе: *[сегодня+10 дней]*.

7. С использованием программы «KeePass»:

7.1. Создайте текстовый документ произвольного содержания *Документ1.doc* и защитите его паролем.

7.2. Заархивируйте несколько файлов произвольного содержания и создайте защищенный паролем архив WinRAR под именем *Архив1.rar*;

Для указанных объектов в программе «KeePass» настройте автонабор и автозапуск*.

Указанные объекты сохраните в своей рабочей папке.

8. Продемонстрируйте работу и файл-отчет преподавателю.

9. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, в том числе зашифрованные; установите первоначальные настройки использованного программного обеспечения.

13. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

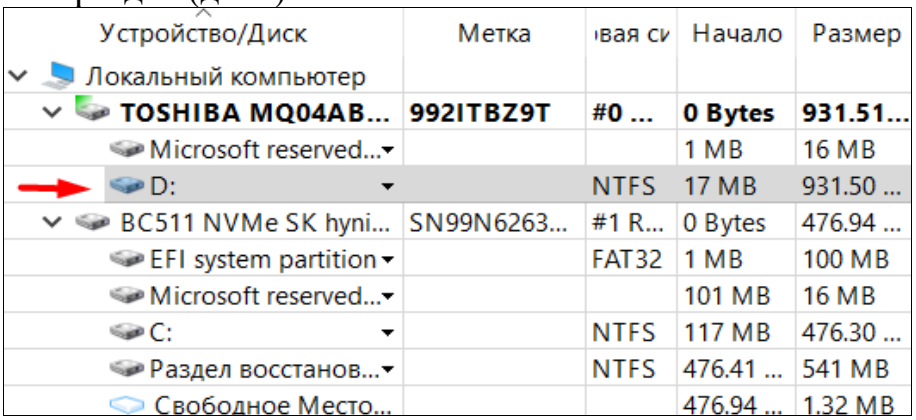
1. Какие элементы защиты может включать составной мастер-ключ программы «KeePass»? Опишите их преимущества и недостатки.
2. Почему не рекомендуется включать в состав мастер-ключа учетную запись Windows? Приведите примеры.
3. Сформулируйте основные рекомендации к выбору пароля и ключевого файла.
4. Как удостовериться в подлинности основных файлов программы «KeePass»?
5. Перечислите последовательность действий по созданию в программе «KeePass» записи о паролях.
6. В чем состоят преимущества функции «Автонабор»? Назовите основную задачу безопасности данных, решаемую с ее помощью.
7. Опишите алгоритм действий по использованию программы «KeePass» с защищенными ресурсами (документ, архив, криптоконтейнер, веб-сайт).
8. Охарактеризуйте известные вам критические уязвимости программы «KeePass». Какие настройки программы «KeePass» следует выполнить в целях их нейтрализации (минимизации)?

* *Задание повышенной сложности (возможно выполнение за дополнительную оценку)*

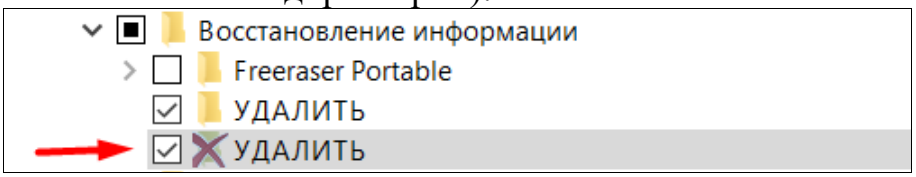
2. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения. Порядок удаления информации программными способами без возможности ее восстановления.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ № 2:

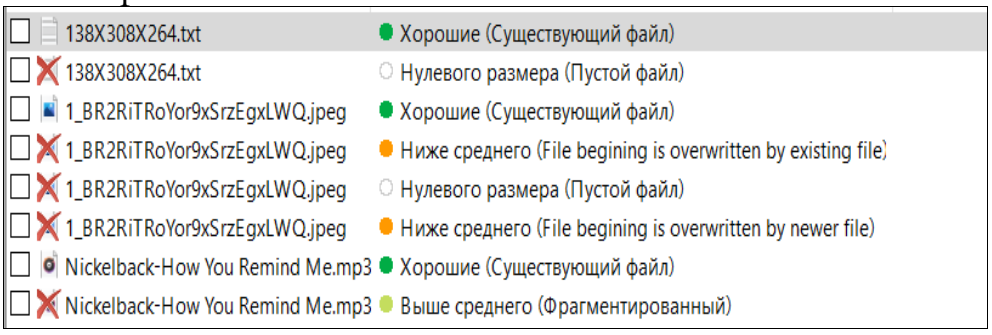
1. Из директории указанной преподавателем, скопируйте папку «Восстановление информации» на диск «D» Вашего ПК;
2. Установите программу R-Studio, находящуюся внутри указанной директории, после чего установите рускоязычный интерфейс (В меню навигации выберите пункт «Help», где во вкладе «Language interface» выберите русский язык).
3. Из директории «Восстановление инрформации» удалите директорию под названием «УДАЛИТЬ» (Комбинация клавиш правый Shift + Delete).
4. Откройте программное обеспечение R-Studio, где двойным кликом мыши откройте раздел (диск) «D».



В появившемся списке найдите удаленную ранее директорию и восстановите её (Отличительной чертой удаленных файлов является наличие красного крестика на иконке директории).



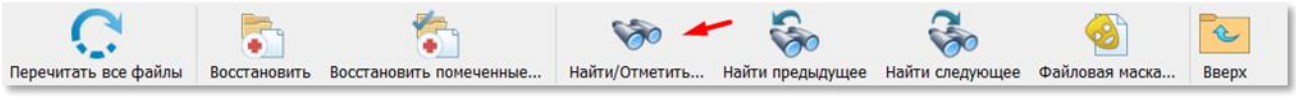
При выделении необходимой директории справа в окне появится информация о файлах в указанной директории с отражением шансов на восстановление файлов.



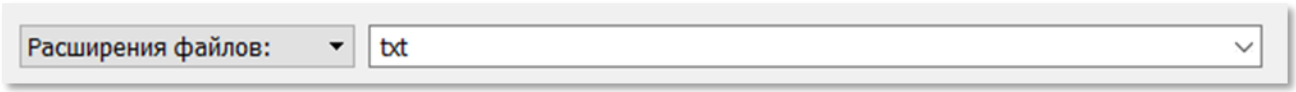
5. Проверьте работоспособность восстановленныйх файлов (изображения открываются, текстовые файлы открываются с содержимым, аудиозапись проигрывается).

6. **Опциональное восстановление.**

На панели навигации выберите пункт «Найти/Отметить».



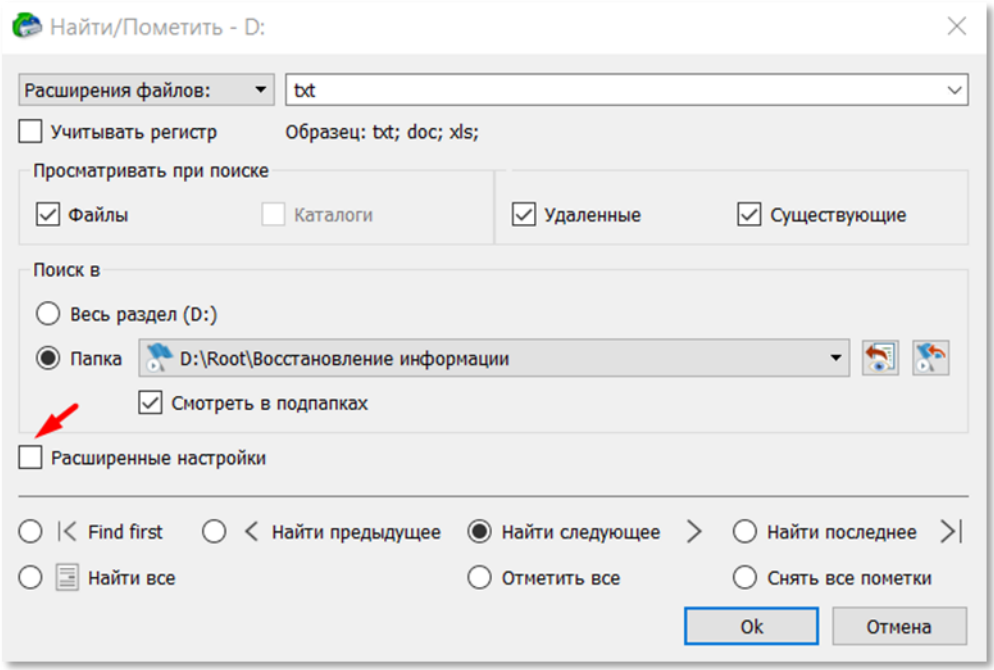
Далее во вкладке «Все файлы и папки», в выпадающем списке выберите пункт «Расширения файлов», после чего справа от выпадающего списка в поле для ввода данных введите наименование расширения «txt», после чего нажмите кнопку «Ок» и найдите файлы с искомым расширением.



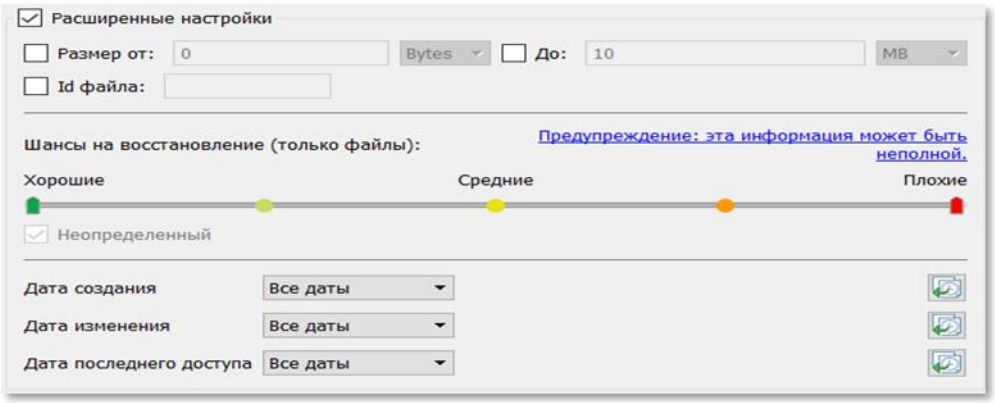
7. **Поиск с расширенными настройками.**

На панели навигации выберите пункт «Найти/Отметить».

В открышемся окне поставьте галочку напротив пункта «Расширенные настройки»



В появившемся меню Вы можете увидеть параметры расширенных настроек восстановления информации.



ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ № 3

1. Из директории «Восстановление информации» установите программу «Freeraser».
2. После установки на рабочем столе появится иконка с корзиной. ПКМ по иконке «Select file to destroy» и выберите файлы для удаления, находящиеся в директории «УДАЛИТЬ 2».
3. Посредством программного обеспечения «R-Studio» попробуйте восстановить информацию из директории «УДАЛИТЬ 2» и проверьте работоспособность информации.

Установите программное обеспечение CCleaner. После установки откройте программу и перейдите во вкладку «Инструменты», где выберите пункт «Стирание дисков». Ознакомьтесь с интерфейсом данного инструмента и режимами удаления информации. (Стирать диск не требуется, данный материал представлен в качестве информирования).

3. Проверка и удаление следов активности пользователя в системе.

ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО 3 ВОПРОСУ:

1. Откройте программу CCleaner, где откройте вкладку «Очистка» и ознакомьтесь с интерфейсом данного инструмента.
2. Посредством вкладки «Windows» предоставляется возможным очистить:

историю браузеров Microsoft Edge и Internet Explorer, а также сопутствующие файлы, образующиеся в ходе осуществления веб-серфинга;

историю работы с проводником ОС;

систему ОС от информации, образующейся в ходе работы с ней.

3. Посредством вкладки «Приложения» предоставляется возможным очистить ОС от информации, образующейся в ходе работы к с предустановленным ПО, так и стороннем.
4. Очистите ОС посредством двух режимов и сопоставьте результате, выделив для себя предпочтительный вариант очистки.