

3.5	1. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force. 2. Стеганографические методы защиты информации.		2	Выполнение практически х заданий
-----	---	--	---	----------------------------------

Тема: 3.5 Аппаратное и программное обеспечение защищенных компьютерных систем.

Учебные вопросы:

1. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force.
2. Стеганографические методы защиты информации.

1. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force

Краткие теоретические сведения:

Создание зашифрованных архивов WinRAR

Для защиты информации сравнительно небольшого объема от несанкционированного доступа рекомендуется хранить ее в зашифрованных архивах, созданных с помощью программ-архиваторов «WinRAR» или «WinZIP». При этом архивы позволяют решить сразу несколько вопросов. Заархивировав группу файлов, пользователь получает архив, который представляет собой всего один файл. Такой файл значительно проще передавать по сети либо по электронной почте, чем большое количество отдельных файлов небольшого размера. Кроме этого, при архивации могут использоваться специальные алгоритмы сжатия данных. Это позволяет сэкономить место на жестком диске. При этом, установка пароля на архив гарантирует надежную защиту хранящихся в нем файлов.

Для того, чтобы создать зашифрованный архив с помощью программы «WinRAR», необходимо выделить нужные объекты (файлы и папки) и нажать на один из них правой клавишей мыши. Затем в появившемся контекстном меню выбрать пункт «Добавить в архив...» (рис. 1).

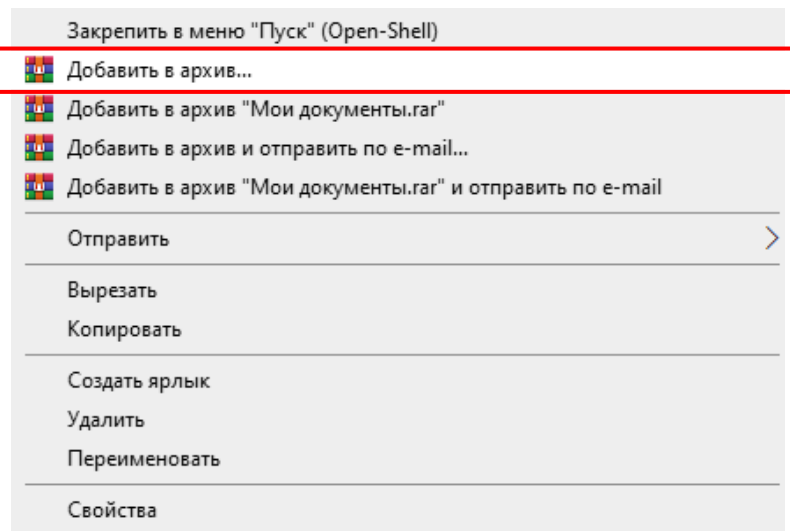


Рис. 1. Контекстное меню. Выбор команды «Добавить в архив».

Откроется диалоговое окно настроек параметров архива (рис. 2). Рассмотрим некоторые, наиболее значимые из них.

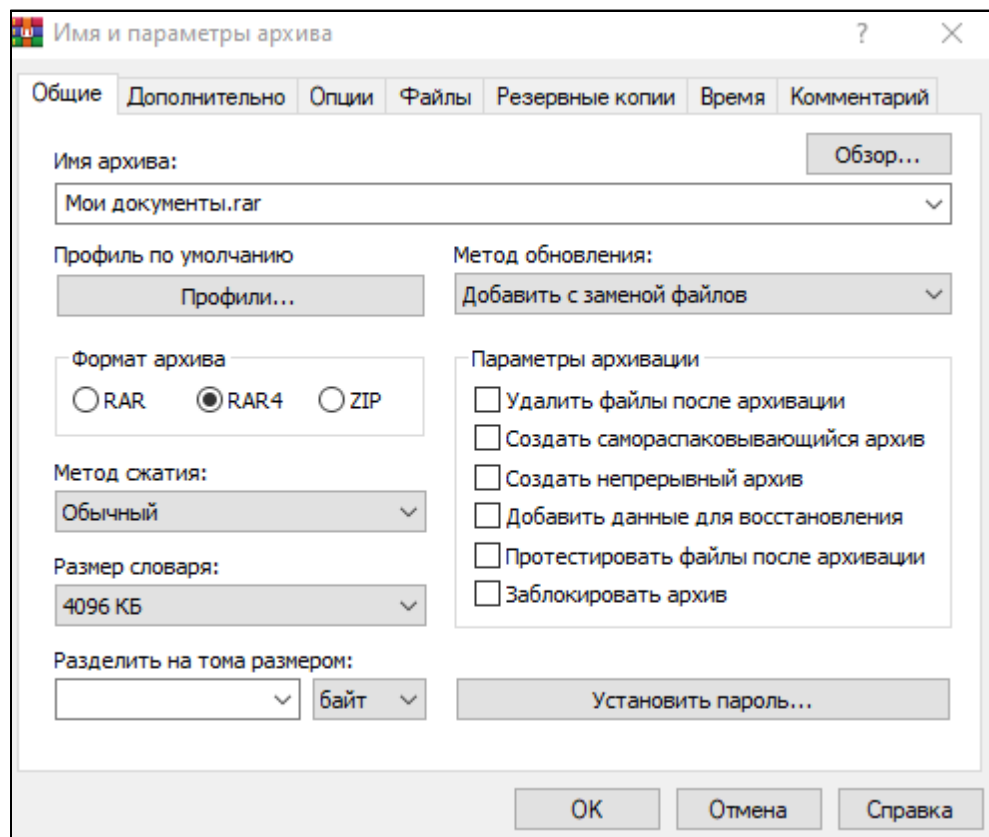


Рис. 2. Главное окно WinRAR

Так, на вкладке «Общие» содержатся следующие основные элементы:

Имя архива. Ввод имени архива (вручную либо с помощью кнопки «Обзор»). Имя может содержать букву диска или полный путь к архиву.

Кнопка «Профили...». Открывает меню, в котором можно создать новый профиль, упорядочить существующие или выбрать один из профилей

архивации (позволяют быстро восстановить ранее сохранённые параметры архивации или указать параметры по умолчанию для данного окна).

Формат архива (RAR, RAR4, ZIP). Выбор формата создаваемого архива. Доступны RAR – новейший формат RAR5, RAR4 – формат, совместимый с WinRAR 4.x, и формат ZIP. В зависимости от выбранного архивного формата некоторые расширенные параметры могут быть недоступны. При обновлении имеющегося архива данный параметр игнорируется, так как в этом случае используется формат обновляемого архива.

Метод сжатия. Выбор одного из методов упаковки: без сжатия, скоростной, быстрый, обычный, хороший и максимальный. Метод «*Без сжатия*» помещает файлы в архив с предельно возможной скоростью, не сжимая их. Остальные методы сжимают данные – чем сильнее, тем медленнее.

Размер словаря. Здесь выбирается размер области памяти, используемый для поиска и сжатия повторяющихся элементов в обрабатываемых данных. Увеличение размера словаря иногда позволяет улучшить сжатие больших файлов, особенно при создании непрерывного архива. Однако, чем больше словарь, тем медленнее архивирование и тем больше памяти требуется.

Разделить на тома размером... Если вы хотите создать многотомный архив, то введите здесь размер тома. В расположенном правее выпадающем списке можно выбрать единицу измерения.

Если вы создаёте многотомный архив на сменных дисках и используете формат RAR, то рекомендуется выбрать пункт «*Автоопределение*», чтобы размер каждого нового тома автоматически подбирался в зависимости от свободного места на диске.

Метод обновления архива. Открывает список следующих параметров:

а) добавить с заменой файлов (действие по умолчанию). Всегда заменять файлы в архиве одноимёнными добавляемыми файлами. Всегда добавлять файлы, которых нет в архиве;

б) добавить с обновлением файлов. Заменять файлы в архиве, только если одноимённый добавляемый файл более новый. Всегда добавлять файлы, которых нет в архиве.

в) обновить существующие файлы. Заменять файлы в архиве, только если одноимённый добавляемый файл более новый. Не добавлять файлы, которых нет в архиве.

г) запрос перед перезаписью. Запрашивать подтверждение перед перезаписью файлов в архиве, имеющих те же имена, что и добавляемые файлы. Всегда добавлять файлы, которых нет в архиве.

д) пропускать существующие файлы. Не заменять файлы в архиве, имеющие те же имена, что и добавляемые файлы. Всегда добавлять файлы, которых нет в архиве.

е) синхронизировать содержимое архива. Заменять файлы в архиве, только если одноимённый добавляемый файл более новый. Всегда добавлять файлы, которых нет в архиве. Удалять из архива те файлы, которых нет среди добавляемых.

Параметры архивации. Группа параметров, реализующая следующие установки:

а) удалить файлы после архивации. После добавления в архив успешно упакованные исходные файлы удаляются.

б) создать самораспаковывающийся архив. Будет создан не обычный архив, а самораспаковывающийся (SFX) в виде EXE-файла, для распаковки которого не требуется никаких других программ.

в) создать непрерывный архив. Использовать режим непрерывного архивирования. Непрерывные (*solid*) архивы, как правило, получаются более компактными, чем обычные.

г) добавить данные для восстановления. В архив будут добавлены данные для восстановления, которые могут помочь восстановить архив в случае его повреждения. В окне «*Дополнительные параметры*» можно указать их размер (по умолчанию – 3% от общего размера архива).

д) протестировать файлы после архивации. После помещения файлов в архив они будут там протестированы, что особенно полезно в сочетании с включённым параметром «*Удалить файлы после архивации*», так как исходные файлы будут удалены с диска только в том случае, если после их добавления в архив он успешно прошёл тестирование.

е) заблокировать архив. Заблокированный архив нельзя изменить с помощью WinRAR, т.е. блокирование важных архивов позволяет избежать их случайной модификации.

Кнопка «*Установить пароль...*». Позволяет установить пароль для шифрования файлов. При нажатии на эту кнопку откроется окно для ввода и подтверждения пароля для создаваемого архива (рис. 3).

Если параметр «*Отображать пароль при вводе*» выключен, то придётся ввести пароль дважды, чтобы гарантировать правильность ввода.

Если включён параметр «*Шифровать имена файлов*», то будет шифроваться не только содержимое файлов, но и другие значимые области архива (имена, размеры, атрибуты, комментарии и другие блоки), что повышает степень защиты информации. У такого архива без указания пароля невозможно даже просмотреть список содержащихся в нём файлов. Этот параметр доступен только для архивов RAR, для архивов ZIP он не поддерживается.

Для сохранения часто используемых паролей и быстрого к ним доступа нажмите на кнопку «*Упорядочить пароли*».

Откроется окно управления паролями (рис. 4), которое содержит список сохранённых пользователем записей о паролях. Обычно в этом списке содержатся метки паролей и маски архивов, но если метка не была задана, вместо неё в колонке *Метка* отображается сам пароль.

Нажмите кнопку *Добавить*, чтобы внести новый пароль в список в позиции ниже курсора. Откроется окно «*Информация о пароле*» (рис. 5), в котором можно указать текст пароля, метку и архивную маску.

Единственное обязательное для заполнения поле – *Текст пароля*. Оно должно содержать сохраняемый пароль.

Поле *Метка пароля* используется для того, чтобы в окне паролей не было видно настоящих паролей. Т.е. вы можете указать здесь метку для пароля и затем вводить не сам пароль, а эту метку всякий раз, когда потребуется указать пароль. WinRAR будет автоматически подменять такую метку паролем. О том, что была введена метка, окно пароля проинформирует вас сообщением «Введена метка пароля» прямо над полем ввода пароля.

Например, вы можете указать *Fhtfl34Shu* как текст пароля, и *home* как его метку, после чего вводить *home* вместо *Fhtfl34Shu*. Эта подстановка работает только в окне пароля.

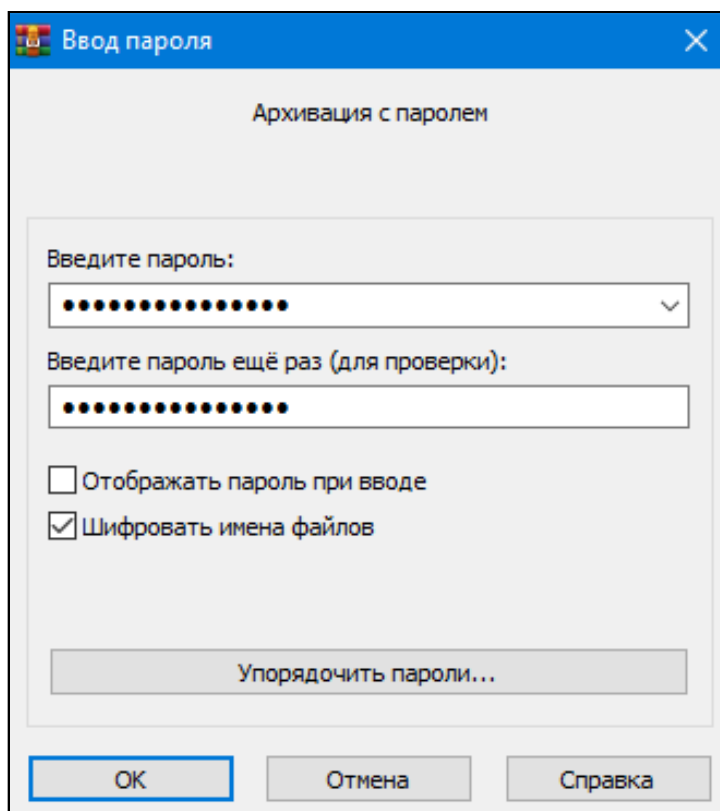


Рис. 3. Диалоговое окно установки пароля к архиву WinRAR

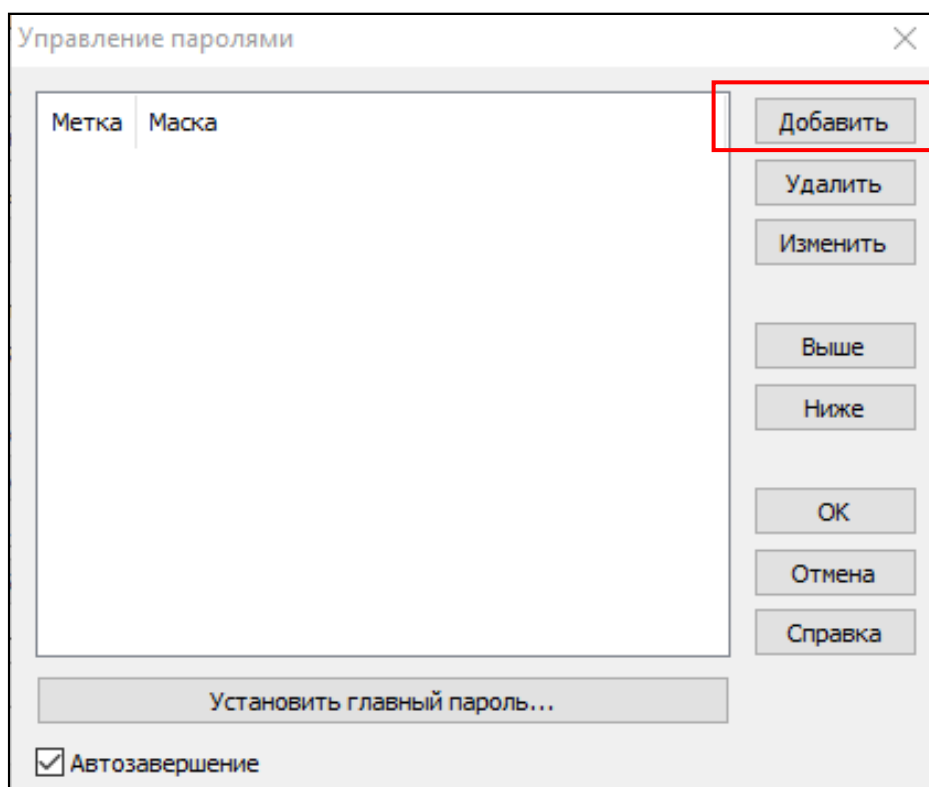


Рис. 4. Окно управления паролями WinRAR

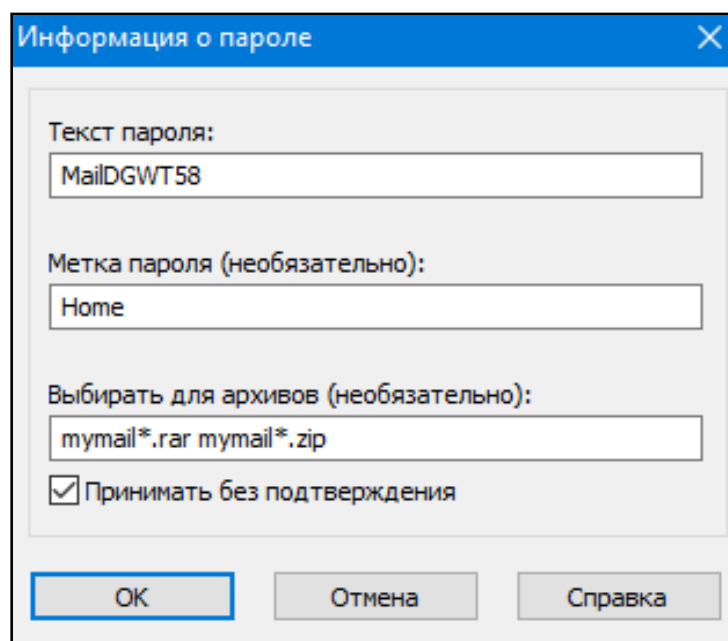


Рис. 5. Окно «Информация о пароле» в WinRAR

Метки паролей должны быть уникальными. Они не должны совпадать ни с одной другой меткой или паролем. В метках не учитывается регистр букв, поэтому *home* и *Home* считаются одной и той же меткой.

Если вы указали и текст пароля, и метку, то в колонке *Метка* в окне «Управление паролями» будет отображаться метка. Если был указан только текст пароля, то в этом списке будет отображаться пароль.

Поле *Выбирать для архивов* может содержать одно или несколько имён или масок архивов (только имена, без пути), разделённых пробелами. Если в имени архива есть пробелы, такое имя должно быть заключено в кавычки. Если имя распаковываемого архива удовлетворяет одной из этих масок, WinRAR автоматически выберет пароль, указанный в поле Текст пароля. Если параметр «Принимать без подтверждения» выключен, этот пароль будет установлен как принимаемый по умолчанию в окне ввода пароля, но у пользователя будет возможность его изменить. Если же параметр «Принимать без подтверждения» включён, пароль будет принят немедленно.

Например, если указать *MailDGWT58* как текст пароля, а в поле *Выбирать для архивов* ввести *my@mail*.rar my@mail*.zip*, то при распаковке архивов *my@mail*.rar* и *my@mail*.zip* будет автоматически выбираться пароль *MailDGWT58*. Этот параметр работает только при распаковке, но не при архивировании.

Примечание: сохранённые пароли хранятся в реестре Windows в виде обычного незашифрованного текста, поэтому их может увидеть любой, у кого есть доступ к компьютеру. Если вам часто приходится использовать пароли, то органайзер паролей может упростить работу с ними, однако при этом нужно тщательно взвесить связанные с этим риски. Если защищаемая паролями информация – особо важная и конфиденциальная, то либо не пользуйтесь органайзером паролей, либо применяйте его только в компьютере, к которому ни у кого нет неавторизованного доступа, либо – установите *главный пароль* (в этом случае записи о паролях будут зашифрованы).

Для установления главного пароля нажмите на кнопку «Установить главный пароль» (рис. 6), введите главный пароль (рис. 7) и затем нажмите «Ok» в окне «Управление паролями». После этого для получения к ним доступа потребуется вводить главный пароль в окне запроса. Будучи введённым, главный пароль остаётся действительным до закрытия WinRAR. Если вы хотите посмотреть, как работает защита, то после задания главного пароля закройте WinRAR и запустите снова. Чтобы удалить шифрование с ранее защищённых записей о паролях, введите пустой пароль.

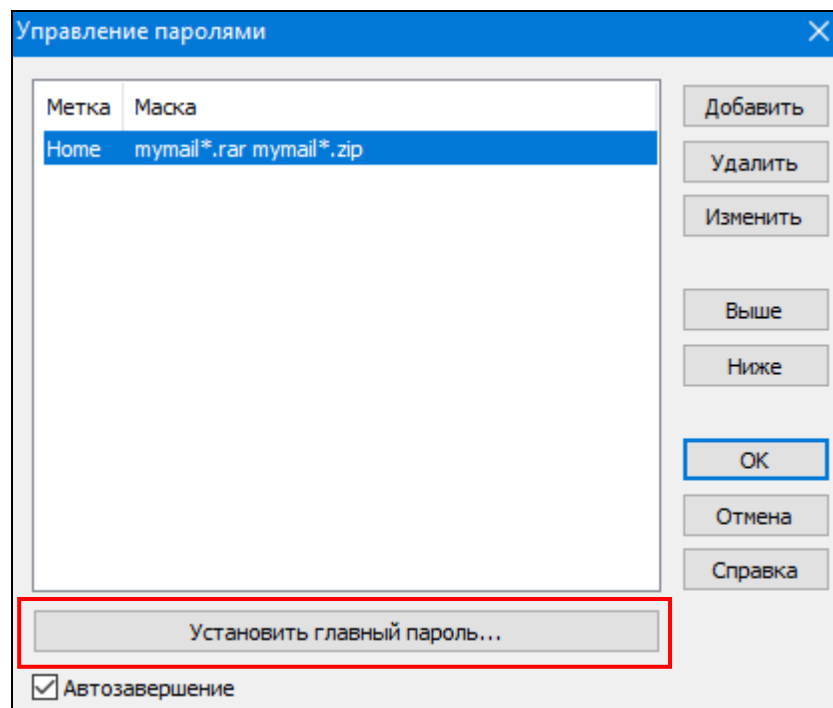


Рис. 6. Окно управления паролями WinRAR

Параметр «Автозавершение» в окне «Управление паролями» позволяет использовать в окне ввода пароля функцию автозавершения паролей. Достаточно ввести только первые буквы пароля или метки пароля, и если эти пароль или метка имеются в списке сохранённых паролей, WinRAR предложит их полный текст. Функция автозавершения работает, только если в окне ввода пароля включён параметр «Отображать пароль при вводе». Если пароли скрыты, автозавершение отключено. Если для сохранённого пароля задана метка, автозавершение будет работать только для метки, но не для текста пароля.

Когда все изменения в списке паролей в окне управления паролями будут выполнены, необходимо нажать кнопку «Ок», чтобы сохранить их.

Сохранённые пароли в окне ввода пароля доступны в выпадающем списке поля *Введите пароль* и как результат действия функции автозавершения.

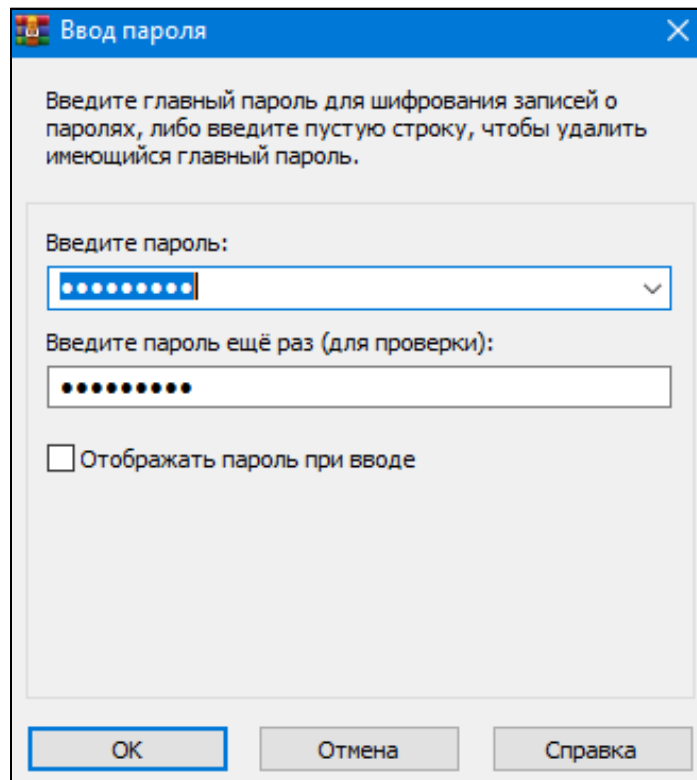


Рис. 7. Окно ввода главного пароля WinRAR

Восстановление пароля методами подбора по словарю и Brute-force.

Подбор пароля по словарю (англ. *dictionary-based attack*) – атака на систему защиты, использующая метод полного перебора предполагаемых паролей, используемых для аутентификации, осуществляемого путём последовательного пересмотра всех слов (паролей в чистом виде или их зашифрованных образов – хэшей) определённого вида и длины **из словаря** с целью последующего взлома системы и получения доступа к защищаемой информации.

Подбор пароля методом *Brute force* (метод «грубой силы») – способ подбора паролей к компьютерной системе, в котором для получения хешированных паролей используются автоматически генерируемые последовательности символов, т. е. **перебираются их всевозможные комбинации** до тех пор, пока пароль не будет подобран. При этом обычно учитывается наименьшая и наибольшая возможная длина пароля.

Рассмотрим указанные методы восстановления пароля на примере зашифрованного архива WinRAR. Для реализации поставленной задачи будем использовать специальную программу определения паролей к архивам «Advanced Archive Password Recovery» (далее – AAPR).

Рабочее окно программы AAPR представлено на рис. 8.

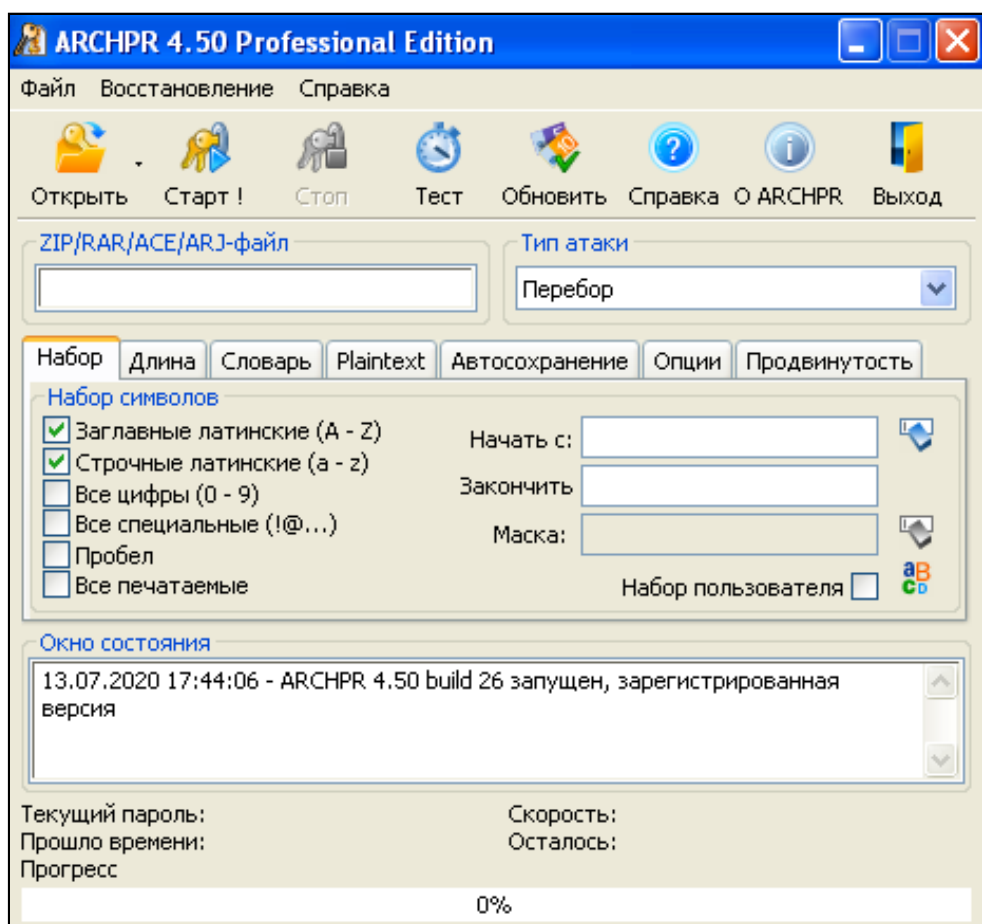


Рис. 8. Главное окно программы для определения паролей к архивам AAPR

Для открытия архива, пароль к которому необходимо подобрать, следует выполнить команду **Файл > Открыть файл**.

Команда **Файл > Открыть проект** открывает сохраненный ранее проект по определению пароля со всеми настройками программы.

На вкладке **Набор** предлагаются опции по выбору символов, которые могут составлять пароль к архиву. По умолчанию предлагаются английские прописные (*Заглавные латинские (A-Z)*) и строчные буквы (*Строчные латинские (a-z)*). Но в паролях могут быть и арабские цифры (*Все цифры (0-9)*), и специальные символы (*Все специальные (!@...)*) (!@#%&*()_+ =<>.,/![]{}~:;`«|»\), и *пробелы*. Поскольку в паролях могут быть не только английские буквы, но и русские, то желательно установить флажок в опцию *Все печатаемые* (в этом случае остальные опции становятся недоступными).

В полях *Начать с..* и *Закончить на..* можно указать начальные или конечные символы пароля, если вы их, конечно, знаете. Если в этих полях были какие-либо символы, то их можно удалить, нажав на кнопку «Очистить начальный пароль» или «Очистить конечный пароль» (пиктограмма обеих кнопок одинаковая (☒)). Если Вы не знаете начальных и/или конечных символов пароля, то в этих полях ничего не заполняйте.

Установка флажка в опции *Набор пользователя* делает недоступным все опции на панели *Набор символов*. Нажатие на кнопку «Определить набор

символов» (🖱️) открывает окно «Определение набора символов» (рис. 10). Вы можете перечислить все символы (буквы, цифры, специальные символы), которые, по Вашему мнению, могут использоваться в пароле. Установка флажка в опцию *OEM-кодировка* предписывает искать символы в соответствии с выбранной кодовой страницей символов национального языка. Кодовая страница национального языка определена в ОС Windows на панели параметров в компоненте «Язык и региональные стандарты».

Вы можете также загрузить уже готовый набор из внешнего файла с расширением *.chr – для этого нажмите кнопку «Загрузить набор» и в открывшемся окне укажите путь к требуемому файлу

После определения пользовательских символов нажмите на кнопку **ОК**.

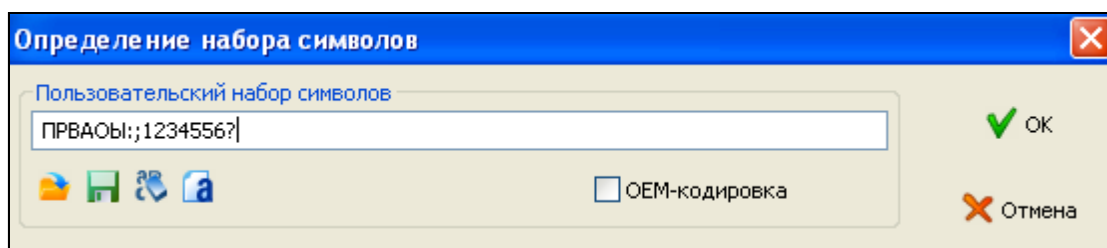


Рис. 9. Настройка пользовательского набора символов

На вкладке **Длина** определяется длина определяемого пароля (рис. 10). Укажите минимальную и максимальную длину пароля архива. Чем больше будет диапазон искомого пароля, тем больше комбинаций должна перебрать программа.

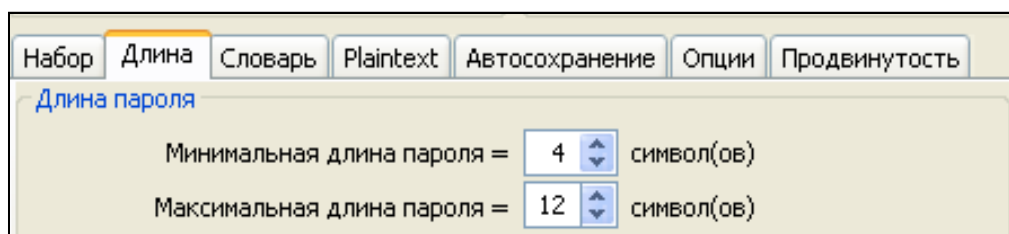


Рис. 10. Настройка параметров для определения пароля

Остальные вкладки программы AAPR нужны в зависимости от выбранного типа атаки.

Список **Тип атаки** доступен из любой вкладки (рис. 11). По умолчанию предлагается наиболее надежный и простой тип атаки: *Перебор (Brute-force)*. Этот тип атаки просто перебирает все варианты выбранных символов в разной комбинации от минимальной до максимальной длины пароля.

Тип атаки *Маска* позволяет определить маску в пароле, если вы знаете хотя бы несколько символов из пароля. Это позволит намного сократить время, необходимое для расшифровки пароля. В данном случае под маской подразумевается набор символов, который программа будет воспринимать как расшифрованную часть пароля и, следовательно, не будет затрачивать на них время и ресурсы.

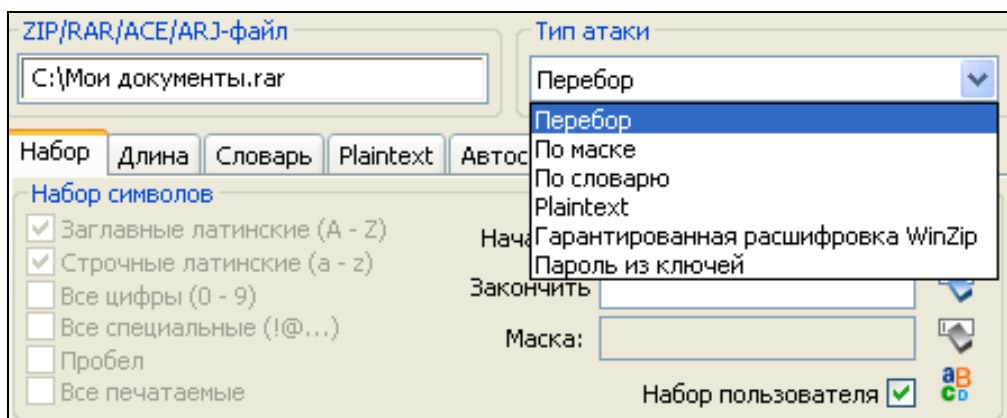


Рис. 11. Выбор типа атаки для определения пароля

Например, вы знаете, что пароль будет содержать 8 символов. При этом пароль начинается с «x», и заканчивается на «99». Другие символы являются строчными или прописными буквами. Известные символы указываются в явном виде, а неизвестные символы указываются в виде вопросительного знака (?). Маска будет выглядеть так: «x?????99».

Символ неизвестного символа маски (?) предлагается по умолчанию. Тем не менее, Вы можете использовать в качестве неизвестного символа любой символ (например, * или #). Для выбора символа перейдите на вкладку программы **Продвинутость**. Символ маски указывается в поле **Символ маски**. Менять символ маски имеет смысл только в том случае, если этот символ действительно имеется в искомом пароле. Например, пароль «*Что делать?*». Здесь вопросительный знак действительно является символом. Если же мы укажем этот символ в маске, то программа будем считать это неизвестным символом.

Тип атаки *По словарю (Dictionary)* предназначен для поиска пароля на основе словаря. Параметры этого типа определяются на вкладке **Словарь** (рис. 12). В поле *Файл словаря* указывается путь к файлу словаря, имеющему расширение *.dic . Чтобы изменить значение данного поля, необходимо нажать расположенную справа кнопку «Выбрать файл словаря» и в открывшемся окне указать требуемый путь.

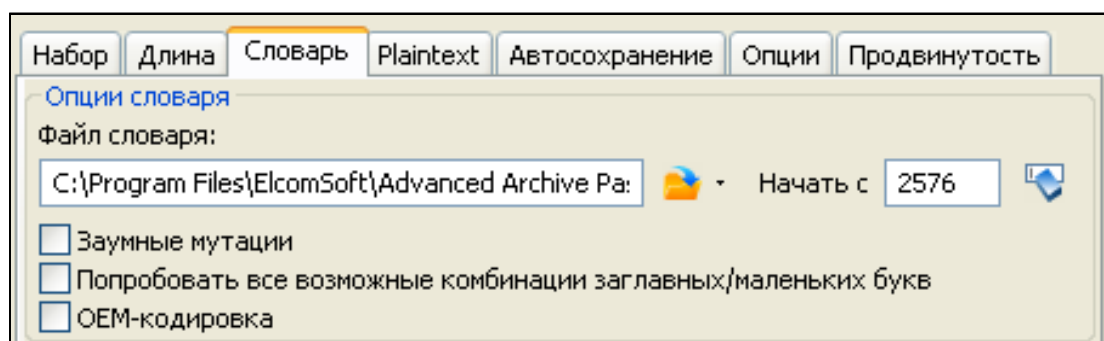


Рис. 12. Настройка параметров определения пароля с помощью атаки «По словарю»

Разработчики данной программы предлагают несколько дополнительных словарей по следующим адресам:

<ftp://sable.ox.ac.uk/pub/wordlists/>

<ftp://ftp.cdrom.com/pub/security/coast/dict/wordlists/>

<ftp://ftp.cdrom.com/pub/security/coast/dict/dictionaries/>

<http://www.elcomsoft.com/prs.html>

Кроме того, вы можете выбрать опции *Заумные мутации* и/или *Попробовать все возможные комбинации заглавных/маленьких букв*, что может действительно помочь в том случае, если вы не уверены в регистре букв пароля.

Например, допустим, что в словаре выбрано следующее слово: *PASSword*. При выборе опции *Попробовать все возможные комбинации заглавных/маленьких букв*, программа просто попробует все возможные комбинации, например: *password*, *passworD*, *passwoRd*, *passwoRD*, *passwOrd*, ..., *PASSWORD*, *PASSWORD*. Тем не менее, проверка всех таких комбинаций занимает много времени: в вышеприведенном примере программа проверит 2^8 слов (то есть, 256) вместо одного. Дополнительно включив опцию *Заумные мутации*, вы можете устранить множество комбинаций фактически возможных. Опция *Заумные комбинации* предлагает 10 комбинаций для каждого слова. Например:

PASSword (как есть);

passWORD (реверс);

password (все в нижнем регистре);

PASSWORD (все в верхнем регистре);

Password (первая в верхнем регистре, остальные в нижнем регистре);

pASSWORD (первая в нижнем регистре, остальные в верхнем регистре);

PaSSWoRD (гласные в верхнем регистре, согласные в нижнем регистре);

pAsswOrd (согласные в верхнем регистре, гласные в нижнем регистре);

PaSsWoRd (с заглавной через одну);

pAsSwOrD (со строчной через одну).

Опция *OEM-кодировка* включается в том случае, если словарь в кодировке ANSI, а архив создан с использованием DOS.

В поле *Начать с..* можно указать букву (или несколько букв) из словаря, с которых нужно начать поиск пароля. Если вы не знаете таких букв, то ничего указывать не нужно. Если в поле имеются буквы от предыдущего поиска, то можете удалить эти символы, нажав на соответствующую кнопку «Очистить» (🗑️).

Метод атаки *Plaintext (Простой текст)* используется в том случае, если в архиве (сам архив должен быть создан WinZip или любым другим архиватором, создающим архивы ZIP), состоящем из нескольких файлов, имеется хотя бы один расшифрованный файл. В этом случае данный метод атаки позволяет расшифровать все остальные файлы архива независимо от сложности пароля.

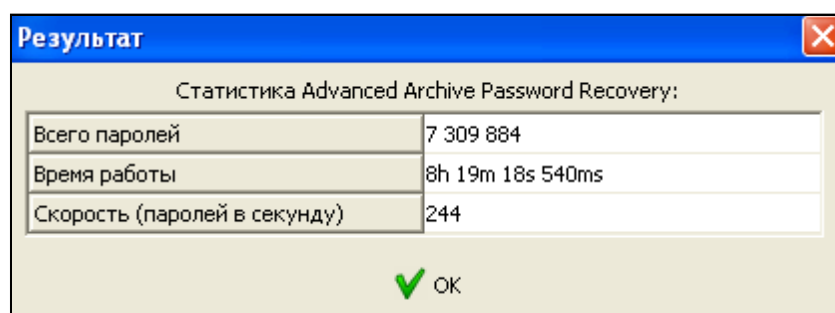
Чтобы выполнять атаку открытого текста, нужно найти не зашифрованный файл, который также существует в защищенном паролем

архиве. Сжать его тем же методом и тем же архиватором ZIP, что и использован в закодированном архиве. После этого нужно запустить данную программу взлома, выбрать закодированный архив, затем выбрать тип Plain-text и сравнить с архивом в незашифрованном файле. После этого программа проверит файлы, и если она найдет схожие фрагменты, то атака будет начата.

Тип атаки *Гарантированная расшифровка WinZip* является наиболее сильной атакой в данной программе. Тем не менее, сам архив должен иметь, по крайней мере, 5 закодированных файлов, защищенных паролем, и должен быть создан WinZip или любым другим архиватором, создающим архивы ZIP. Кроме того, начиная с архивов версии 8.1 и выше, вы не сможете использовать эту атаку. Если архив создан другим архиватором или содержит менее 5 файлов, то программа также выведет сообщение об ошибке.

Тип атаки *Пароль из ключей* восстанавливает пароль в том случае, если имеются ключи шифрования из данной программы. Рекомендуемая минимальная длина пароля – 11 символов.

Кнопка «Тест» (🕒) помогает оценить примерное время, необходимое на поиск пароля, скорость проверки в секунду и число проверок с выбранными параметрами (рис. 13). Это нужно на тот случай, чтобы оценить – сколько же может продлиться процесс поиска и стоит ли его вообще запускать.

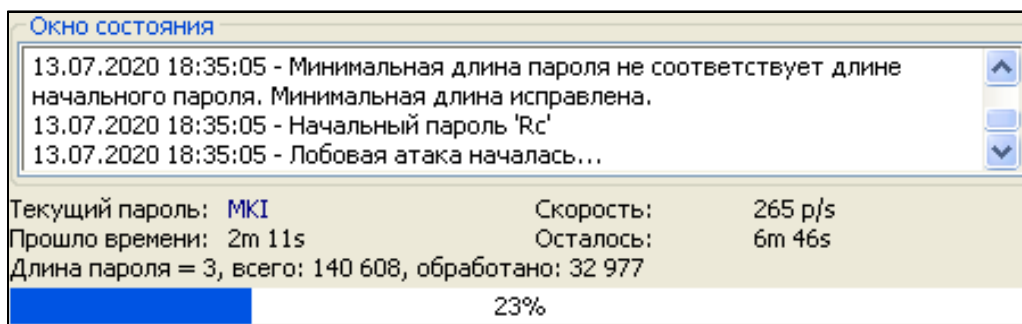


Статистика Advanced Archive Password Recovery:	
Всего паролей	7 309 884
Время работы	8h 19m 18s 540ms
Скорость (паролей в секунду)	244

✔ OK

Рис. 13. Оценка примерного времени, необходимого на определение пароля

Для запуска процесса определения пароля нажмите на кнопку «Старт!». Запустится окно состояния, в котором будет представлена основная текущая информация о процессе извлечения пароля (рис. 14).



Окно состояния		
13.07.2020 18:35:05 - Минимальная длина пароля не соответствует длине начального пароля. Минимальная длина исправлена.		
13.07.2020 18:35:05 - Начальный пароль 'Rc'		
13.07.2020 18:35:05 - Лобовая атака началась...		
Текущий пароль: MKI	Скорость: 265 p/s	
Прошло времени: 2m 11s	Осталось: 6m 46s	
Длина пароля = 3, всего: 140 608, обработано: 32 977		
23%		

Рис. 14. Информация о процессе извлечения пароля

Если пароль будет найден, то он отобразится в специальном окне (рис. 15).

Для остановки процесса анализа предусмотрена кнопка «Стоп». После нажатия на эту кнопку необходимо очистить поле «Начать с..», так как в нем остается последний вариант перебора пароля.

Обратите внимание, что перед анализом (а возможно, что и в ходе него) могут выполняться какие-либо настройки программы. Эти настройки можно сохранить для того, чтобы потом можно было использовать снова. Для этого нужно нажать на кнопку «Сохранить» (📁) и указать имя сохраняемого проекта. Затем этот проект с установками параметров можно открыть кнопкой «Открыть» (📁).

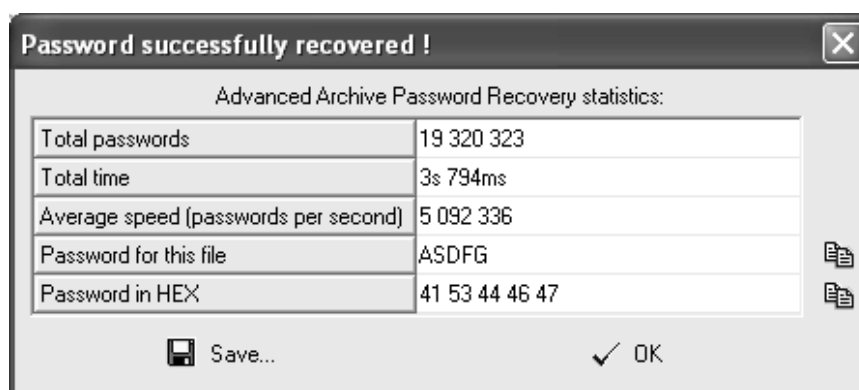


Рис. 15. Информационное окно с результатами работы программы AAPR

Следует отметить, что расшифровка сложных паролей может занимать продолжительное время (например, когда программе придется перебирать большое количество возможных комбинаций).

Проверка сложности (устойчивости ко взлому) пароля. Создание сложного пароля.

Основные требования к паролям, которые позволяют избежать сравнительно быстрого подбора или его взлома с помощью специализированных программ типа AAPR, можно представить в виде следующего набора правил:

минимальная длина пароля должна быть не менее 12 символов;

пароль должен состоять из произвольного (бессмысленного) набора букв (строчных И прописных, английских И русских), а также цифр и специальных символов (!@...) (!@#\$\$%^&*()_+!<>,./?[]{}~:;'«|»\);

пароль, являющийся словарным словом, очень уязвим перед автоматическими программами-взломщиками, которые используют частотные словари для перебора наиболее употребляемых слов (злоумышленник обычно подбирает пароль по словарю, с учётом вероятности слов, начиная с паролей в одно распространённое слово («the», «he» и т.д.), затем комбинация двух распространённых слов, затем одно менее распространённое слово, и т.д. по мере уменьшения вероятности);

пароль, составленный из набора соседних букв, находящихся на клавиатуре, также уязвим, поскольку все популярные комбинации давно включены в базы данных программ подбора паролей;

не рекомендуется использовать в качестве пароля даты, номера телефонов, паспортные данные и иные социально значимые сведения (в том числе и в любых их комбинациях) – именно такие пароли взламываются чаще всего;

пароль должен быть уникальный (нельзя использовать один и тот же пароль на различных аккаунтах, сервисах, ПК, веб-ресурсах, E-mail и т. д.);

пароли необходимо менять с определенной периодичностью, оптимальный срок – от трех до шести месяцев.

Для проверки сложности (устойчивости ко взлому) пароля можно воспользоваться специальным онлайн-сервисом «PASSCHECK» (<https://exploit.in/passcheck/>) (рис. 15). Данный сервис выполняет все необходимые вычисления в браузере и не осуществляет загрузку проверяемых паролей в интернет.

Стойкие пароли являются более безопасными. Расшифровка более сложных паролей занимает больше ресурсов и времени, а в некоторых случаях - невозможна.

Протестируйте устойчивость ваших паролей: Введите ваш пароль.

Пароль:

Устойчивость: **Сильный**

Какой пароль - безопасный?

Безопасным пароль можно считать, если:

- длина: > 15 символов;
- наличие цифр, букв разного регистра и специальных символов;
- уникальность пароля (нельзя использовать один и тот же пароль на аккаунтах, icq, jabber, e-mail и т.д)

Как придумать безопасный пароль?

Используйте [Генератор паролей.](#)

Рис. 15. Онлайн-сервис «PASSCHECK» (<https://exploit.in/passcheck>)

Онлайн-сервис «PASSCHECK» также содержит ссылку на собственный генератор случайных паролей (<https://exploit.in/passgen/>), в котором можно задать необходимые параметры:

- учет заглавных букв;
- учет прописных букв;
- учет цифр;
- учет специальных символов;
- количество символов (длина пароля);
- количество генерируемых паролей.

Нажав на кнопку «Генерировать», пользователь получит искомый список паролей (рис. 16), который можно скопировать в буфер обмена и использовать по назначению.

Password Generator

Заглавные(большие)	<input checked="" type="checkbox"/>
Прописные(маленькие)	<input checked="" type="checkbox"/>
Цифры(1-9)	<input checked="" type="checkbox"/>
Спец. символы	<input checked="" type="checkbox"/>
Кол-во символов	12
Кол-во паролей	6

Список паролей:

```

qUVz.&30224=
St|N+#%oG>ZH
Ltuf~eq9k3q6
p!J(0-u0D5hv
0NZLuix1y)W.
hhEp8V3)k#98

```

Рис. 16. Генератор паролей онлайн-сервиса «PASSCHECK» (<https://exploit.in/passgen/>)

Проверка пароля на предмет возможной компрометации

Существуют сетевые базы данных, включающие сведения об учетных записях (паролях), похищенных в результате взломов различных веб-сайтов. Использование таких баз данных позволяет не только определить факты компрометации (утечки) критически важной информации, но и оценить риск, связанный с тем, что используемый аккаунт попал в зону хакерской атаки.

Одним из таких ресурсов является онлайн-сервис HAVEIBEENPWNERD.COM («Have I Been Pwned») (<https://haveibeenpwned.com/Passwords>), позволяющий выполнить проверку паролей на предмет возможной компрометации (рис. 17). Данный сервис создан известным и уважаемым экспертом по кибербезопасности Троем Хантом и де-факто в последние годы стал отраслевым стандартом для проверки аккаунтов на утечки.

«Have I Been Pwned» использует и регулярно обновляет базу данных, включающую сведения о почти 5 миллиардах учётных записей. База была составлена на основе отсеивания дубликатов из сводной коллекции, включающей 3 миллиарда открытых паролей (в среднем каждый пароль встречается 6 раз). Для каждого пароля имеется счётчик дубликатов, указывающий число разных учётных записей, в которых был зафиксирован данный пароль.

Для проверки паролей онлайн-сервис «Have I Been Pwned» использует два решения (рис. 18, 19).

Первое решение – алгоритм, с помощью которого проверяются пароли на устойчивость ко взлому методом перебора. Этот инструмент позволяет быстро вычислить примерное время, которое потребуется для взлома на усредненной аппаратной конфигурации персонального компьютера. Алгоритм учитывает ускорение процесса перебора с помощью словарей и списки распространенных сочетаний символов. При этом введенный вами пароль никуда не передается и не сохраняется.

Второе решение – сервис «Have I Been Pwned» проверяет, не «засветился» ли введенный пароль в базах утекших аккаунтов.

Вероятность того, что «Have I Been Pwned» используется для тайного сбора чужих паролей, крайне минимальна, поскольку проверяемый пароль не передается для проверки напрямую. Вместо этого используется так называемый хэш пароля SHA-1 – шифрованное значение, по которому можно проверить наличие записи в базе, но нельзя вычислить сам пароль. Соответственно, имеющиеся в базе данных «Have I Been Pwned» сведения также хранятся в виде хэшей SHA-1.

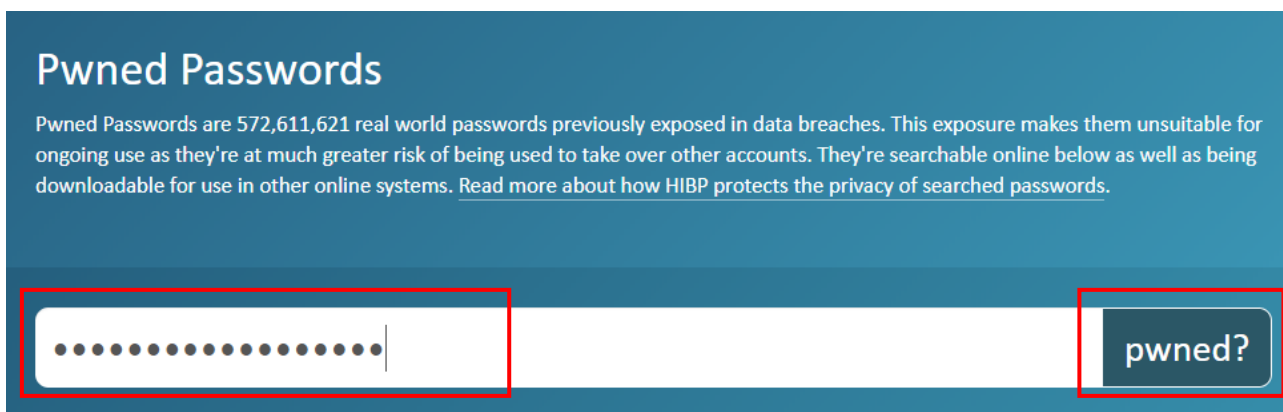


Рис. 17. Онлайн-сервис «Have I Been Pwned» (<https://haveibeenpwned.com/Passwords>)



Рис. 18. Сообщение онлайн-сервиса «Have I Been Pwned» о компрометации пароля



Рис. 19. Сообщение онлайн-сервиса «Have I Been Pwned» об отсутствии сведений о компрометации пароля









Кроме того, на сайте данного онлайн-сервиса можно скачать базу хэшей всех хранящихся паролей (это не пароли в открытом виде, но контрольные

суммы SHA-1, по которым можно однозначно проверить, есть ли пароль в базе) (рис. 25).

Downloading the Pwned Passwords list

The entire set of passwords is downloadable for free below with each password being represented as either a SHA-1 or an NTLM hash to protect the original value (some passwords contain personally identifiable information) followed by a count of how many times that password had been seen in the source data breaches. The list may be integrated into other systems and used to verify whether a password has previously appeared in a data breach after which a system may warn the user or even block the password outright. For suggestions on integration practices, read the [Pwned Passwords launch blog post](#) for more information.

Please download the data via the torrent link if possible! If you can't access torrents (for example, they're blocked by a corporate firewall), use the "Cloudflare" link and they'll kindly cover the bandwidth cost.

	Format	File	Date	Size	SHA-1 hash of 7-Zip file
 	SHA-1	Version 4 (ordered by prevalence)	17 Jan 2019	11.0GB	59741e11e20a3fc4f29ae597972295dcb94cef39
 	SHA-1	Version 4 (ordered by hash)	17 Jan 2019	9.78GB	d81c649cda9cddb398f2b93c629718e14b7f2686
 	NTLM	Version 4 (ordered by prevalence)	17 Jan 2019	8.85GB	2014695d9c4880aac69be031a1cc7c9eee4bcfb9
 	NTLM	Version 4 (ordered by hash)	17 Jan 2019	7.58GB	ee7199ee2a1d8f23dd346d5b1fb2255e1ed8de8a

The bandwidth costs of distributing this content from a hosted service is significant when downloaded extensively. Cloudflare kindly offered to support this initiative by aggressively caching the file at their edge nodes over and beyond what would normally be available. Their support in making this data available to help organisations protect their customers is most appreciated.

Рис. 25. Диалоговое окно настройки параметров архива

Альтернативным средством проверки паролей на устойчивость ко взлому, а также на предмет их возможной компрометации, является онлайн-сервис «Kaspersky Password Checker» (<https://password.kaspersky.com/ru/>) (рис. 20-22).

Наряду с собственным инструментом для оценки уязвимости проверяемого пароля, данный сервис использует базу данных скомпрометированных паролей онлайн-сервиса «Have I Been Pwned» (<https://haveibeenpwned.com/Passwords>)

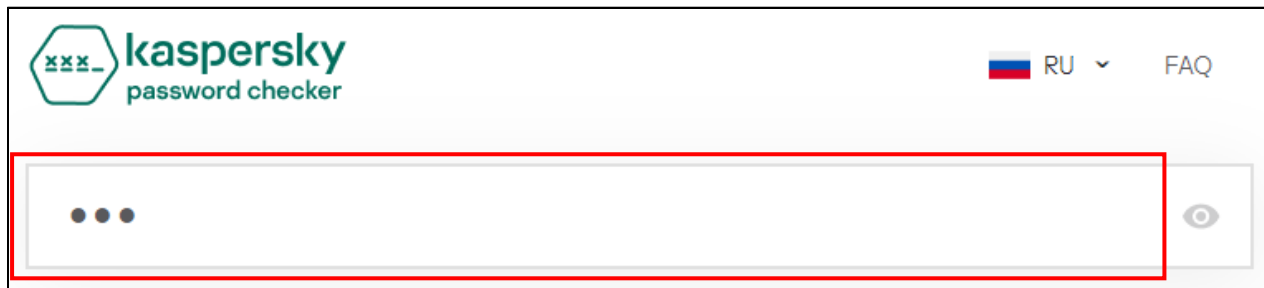


Рис. 20. Онлайн-сервис «Kaspersky Password Checker» (<https://password.kaspersky.com/ru/>)

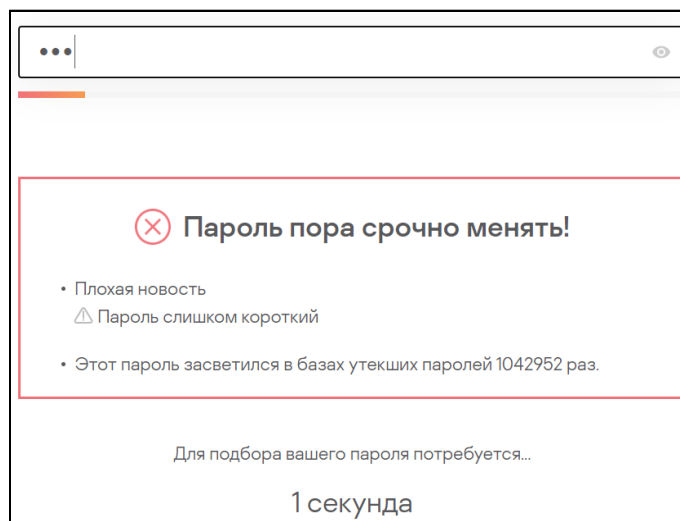


Рис. 21. Сообщение онлайн-сервиса «Kaspersky Password Checker» о компрометации пароля

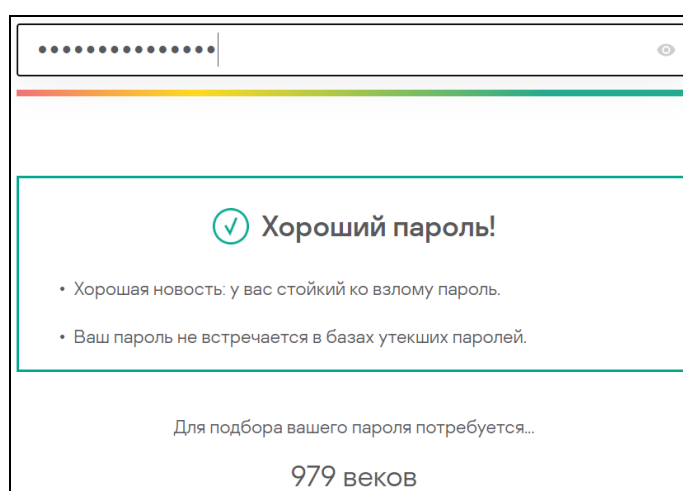


Рис. 22. Сообщение сервиса «Kaspersky Password Checker» об отсутствии сведений о компрометации пароля

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Запустите программу-архиватор WinRAR и выполните следующие настройки программы:

- а) отключите историю архивов, а также в полях ввода;
- б) исключите при разархивации или открытии архивов WinRAR распаковку потенциально опасных файлов, соответствующих следующей маске:

**.exe *.com *.pif *.scr *.bat *.cmd *.lnk;*

- в) включите безвозвратное удаление временных файлов архива, зашифрованного паролем.

2. Создайте **профиль архивации по умолчанию** со следующими настройками:

имя профиля – *Мой профиль*;

формат архива – RAR4;

метод сжатия – быстрый;

метод обновления архива – синхронизировать содержимое архива;

параметры архивации:

а) удалить файлы после архивации;

б) добавить данные для восстановления;

в) заблокировать архив;

г) протестировать файлы после архивации;

режим удаления файлов после архивации – безвозвратное удаление без возможности восстановления (для файлов архива, для которого задан пароль);

файлы, которые не следует архивировать:

файл *c:\temp\info.txt*;

все файлы **.bak* и **.tmp*;

все папки *temp*;

все файлы в папках *temp*;

файлы для добавления в архив без сжатия: архивы RAR и ZIP, а также изображения JPG;

генерировать имя каждого нового архива согласно следующей маске:
My_documents_день.месяц.год/часы.минуты.секунды (например: *My_documents_09.01.2020/10.05.01*);

сохранять предыдущие версии файлов – да;

сохранять время создания и время последнего доступа к архивируемым файлам – да;

параметры пароля на архивы:

текст пароля – *самостоятельно сгенерировать с помощью онлайн-сервиса «PASSCHECK» с учетом рекомендуемых требований безопасности.*

Пароль также следует проверить на сложность (устойчивость ко взлому), а также на предмет возможной компрометации.

метка пароля – *придумать самостоятельно;*

автоматическое использование (установка по умолчанию) и принятие без подтверждения для открытия архивов с именем согласно следующей маске:
My_documents.rar*;

функция автозавершения для метки пароля – *да;*

шифровать имена файлов – *да;*

отображать пароль при вводе – *нет;*

шифрование записей о паролях с помощью главного пароля – *да (пароль придумать самостоятельно с учетом рекомендуемых требований безопасности. Пароль также следует проверить на сложность (устойчивость ко взлому), а также на предмет возможной компрометации).*

Функциональное назначение указанных настроек и параметров опишите в файл-отчете.

3. Создайте несколько папок и файлов произвольного содержания. С помощью программы-архиватора WinRAR заархивируйте их с учетом следующих условий:

имя архива – *Архив 1*;

формат архива – RAR4;
метод сжатия – быстрый;
сохранять время создания и время последнего доступа к архивируемым файлам – да;

параметры пароля на архивы:

текст пароля – словарное или общепринятое английское слово длиной до 5-6 символов либо цифровое значение (например: *qwerty*, *123456*, *love*, *god*, *table*, *admin* и т.п.).

шифровать имена файлов – да;

отображать пароль при вводе – нет.

4. С использованием программы AAPR предварительно оцените время восстановления паролей к архивам *My_documents*.rar* (п. 2 задания) и *Архив 1* с помощью следующих видов атак:

а) *по словарю*;

б) *Brute-force*.

Попытайтесь восстановить пароль к данным архивам, выполнив указанные атаки.

Сравните затраченное время.

Опишите результаты и сформулируйте в файл-отчете вывод.

5*. Самостоятельно установите (из сетевой папки, указанной преподавателем) программу «Advanced Office Password Recovery Pro» (далее – AOPR), предназначенную для подбора паролей к файлам формата MS Word, Excel, Access, Outlook, Money, Visio, PowerPoint, OneNote, OpenDoceumt, iWork и др.

Изучите ее интерфейс, представленные опции и возможности настроек.

6. Создайте несколько файлов формата MS Word, Excel, Access. Часть из них зашифруйте сложным паролем, соответствующим необходимым требованиям безопасности. Оставшиеся файлы – несложным паролем (словарное или общепринятое английское слово длиной до 5-6 символов либо цифровое значение, например: *qwerty*, *123456*, *love*, *god*, *table*, *admin* и т.п.).

7. С использованием программы AOPR предварительно оцените время восстановления паролей к созданным в п. 8 задания файлам с помощью следующих видов атак:

а) *атака перебором (Brute-force)*;

б) *атака по словарю*;

в) *атака по слову*;

г) *атака по маске*;

д) *комбинированная атака*;

е) *гибридная атака*.

Попытайтесь восстановить пароль к зашифрованным файлам. Для этого предварительно настройте и поочередно осуществите вышеуказанные атаки.

* п.п. 7-9 – задание повышенной сложности (возможно выполнение за дополнительную оценку)

Сравните затраченное время.

Опишите результаты и сформулируйте в файл-отчете выводы.

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.

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

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какие программы-архиваторы вы знаете?
2. Какие преимущества дает архивирование файлов и папок?
3. Что обеспечивает шифрование имен файлов при настройке параметров архива?

4. Перечислите основные действия для создания зашифрованного архива с помощью программы-архиватора WinRAR.

5. Какие виды атак на пароль Вы знаете?

6. Как можно противостоять атаке полным перебором?

7. Как длина пароля влияет на вероятность раскрытия пароля?

8. Какие рекомендации по составлению паролей Вы можете дать?

9. Какие программы восстановления паролей вы знаете? Опишите их функциональные возможности.

10. Генераторы случайных паролей: виды, возможности, функционал, примеры использования.

11. Опишите функциональные возможности сервисов проверки сложности (устойчивости ко взлому) паролей. Приведите примеры.

12. Как осуществить проверку пароля на предмет возможной компрометации?

4. Стеганографические методы защиты информации

Краткие теоретические сведения:

Существует множество компьютерных программ, которые защищают конфиденциальные данные путем шифрования. Но в большинстве случаев выявления самого факта наличия конфиденциальной информации (даже зашифрованной) уже является своего рода утечкой информации. Очевидно, что самым надежным способом защиты конфиденциальных данных является сокрытие их факта наличия. Такую возможность предоставляет стеганография.

Стеганография – это метод сокрытия определенного сообщения в другом таким образом, при котором невозможно увидеть присутствие или смысл скрытого сообщения. В современных условиях – это цифровая стратегия

сокрытия файла в мультимедийном формате, например: картинка, звуковой файл (wav, mp3), обычный текстовый документ или даже видеофайл.

Как и большинство специализированных программных утилит по безопасности, стеганография может использоваться для сохранения ценной информации, например, в целях защиты данных от возможного саботажа, кражи или несанкционированного просмотра.

Одной из программ, предназначенных для стеганографического сокрытия данных, является бесплатный программный продукт «BDV DataHider». При помощи этой программы пользователь может, например, поместить скрываемые файлы в исполняемый файл какого-нибудь приложения, в графический или звуковой файл или скрыть целый диск. При этом на работе файлов, в которые помещены скрытые данные, это никак не отразится. Путем создания невидимого «контейнера» в файлах произвольного формата или на дисках с файловой системой NTFS, FAT или FAT32 (в том числе на съемных) он позволяет скрывать данные одним из трех способов:

- упаковка данных в графическом файле,
- сокрытие данных в файл любого формата,
- создание «секретного» носителя информации.

Скрытые данные становятся абсолютно невидимы. При этом, в любое время пользователь может извлечь из файла или диска скрытую информацию с помощью той же программы (путем ввода пароля).

Алгоритм работы с программой «BDV DataHider» состоит из следующей последовательности действий:

1. Запустите исполняемый файл программы «BDV DataHider». На экране отобразится диалоговое окно мастера создания стеганографического контейнера (рис. 1).

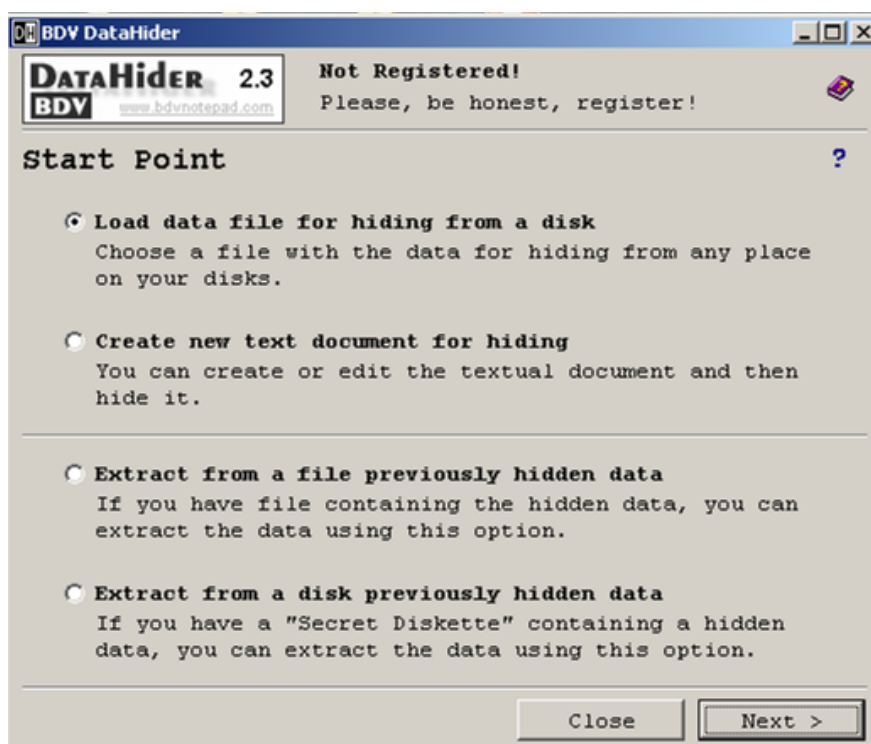


Рис. 1. Диалоговое окно мастера создания стеганографического контейнера с помощью программы «BDV DataHider» (начало работы)

На данном шаге мастера вы можете выбрать один из четырех вариантов:

1) Load data file for hiding from a disk.

С помощью этой опции вы можете загрузить файл с конфиденциальными данными для сокрытия. После нажатия кнопки «Далее» появится окно «Открыть».

2) Create new text document for hiding.

Вы можете создать и отредактировать текстовый документ, а затем скрыть его.

3) Extract from a file.

Эта опция используется для извлечения конфиденциальной информации, скрытой в файле.

4) Extract from a disk.

Если у вас имеется съемный носитель информации (USB-Flash, HDD и пр.), созданный с помощью этой программы, используйте эту опцию для извлечения конфиденциальной информации, скрытой на нем.

Вы можете переходить к следующему шагу или вернуться к предыдущей с помощью кнопок «Далее» и «Назад», расположенную в нижней части окна.

2. Создайте стеганографический контейнер в графическом файле и поместите в него текстовый документ. Для этого в вышеуказанном окне выберите пункт «Load data file for hiding from a disk», нажмите на кнопку «Next» и укажите месторасположение текстового файла, который будет внедряться в графический файл (рис. 2).

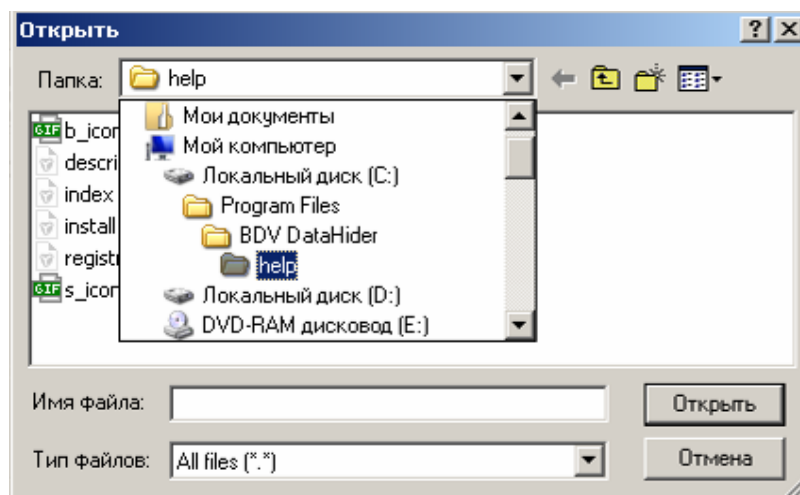


Рис. 2. Выбор месторасположения текстового файла, который будет внедряться в графический файл с помощью программы «BDV DataHider».

После этого появится диалоговое окно для ввода и подтверждения пароля (рис. 3).

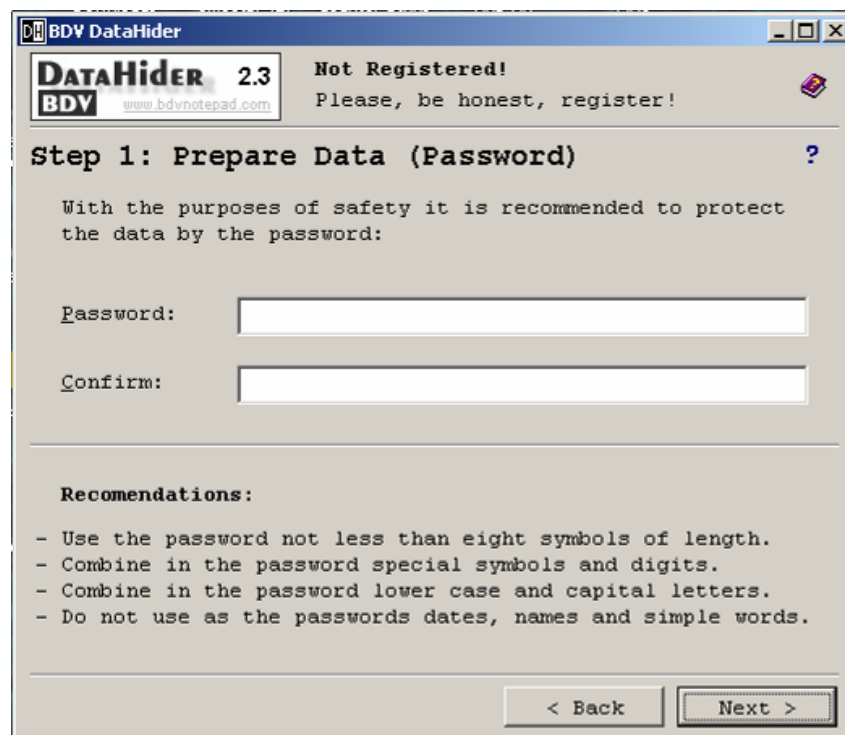


Рис. 3. Диалоговое окно для ввода и подтверждения пароля (шаг 1)

3. Введите пароль в поле «Пароль» и введите его еще раз в поле «Подтверждение». Для продолжения нажмите на кнопку «Next».

После этого появится диалоговое окно выбора метода стеганографического сжатия (рис. 4).

У вас есть возможность выбрать один из трех методов сокрытия данных:

1) Hide the data in a bitmap (сокрытие данных в растровом файле).

Это самый надежный способ сокрытия конфиденциальной информации. Данные будут упакованы в растровый файл и будут абсолютно незаметны для постороннего пользователя.

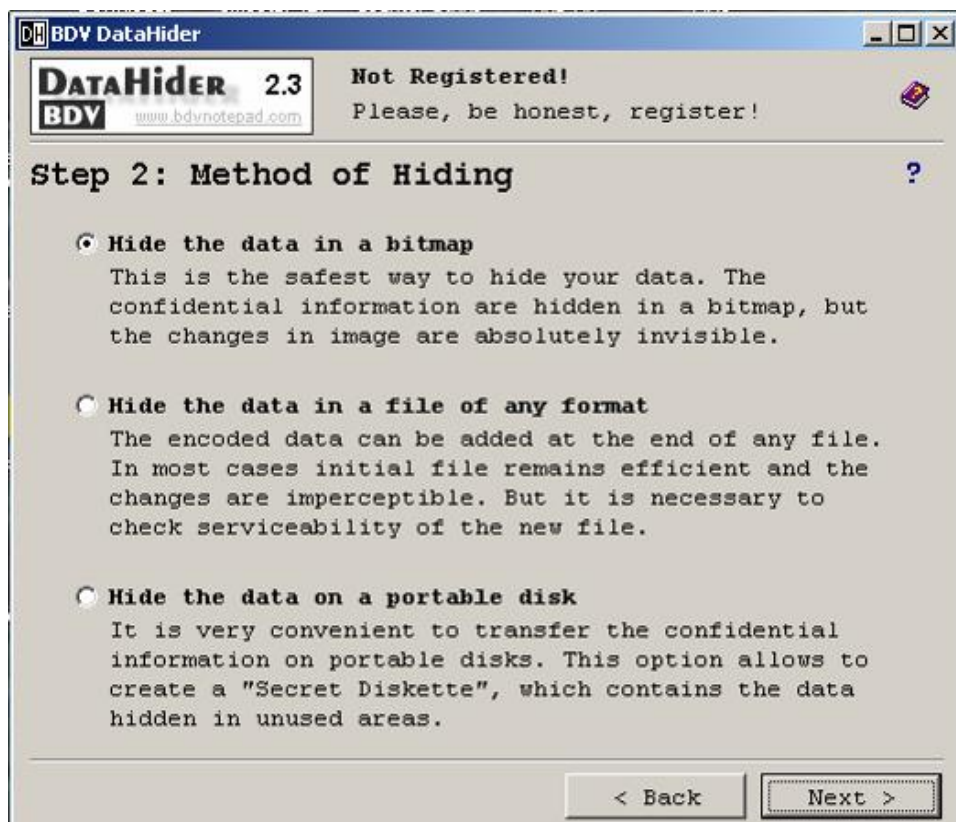


Рис. 4. Диалоговое окно выбора метода сокрытия информации в стеганографическом контейнере (шаг 2)

После нажатия кнопки «Далее» появится окно «Открыть изображение», где вы можете выбрать графический файл, в котором необходимо создать стеганографический контейнер.

2) Hide the data in a file of any format (сокрытие данных в файл любого формата).

Для выбора данного метода сокрытия данных выберите файл любого формата в диалоговом окне «Открыть». Данные будут зашифрованы и внедрены в этот файл. После выбора файла появится окно для сохранения созданного файла. Рекомендуемые форматы файлов: *.DOC, *.JPG, *.EXE, *.EMF, *.SWF. Не рекомендуется : *.TXT, *.HTM *.

3) Hide the data on a portable disk (сокрытие данных на съемном диске).

Эта опция служит для создания скрытых носителей информации. Информация записывается на свободное место носителя и становится «невидимой». Восстановить их можно только с помощью этой программы.

4. Выберите пункт «Hide the data in a bitmap» (сокрытие данных в растровом файле) и нажмите кнопку «Next». После этого появится диалоговое окно настройки растрового изображения, в который будет внедрен стеганографический контейнер (рис. 5):

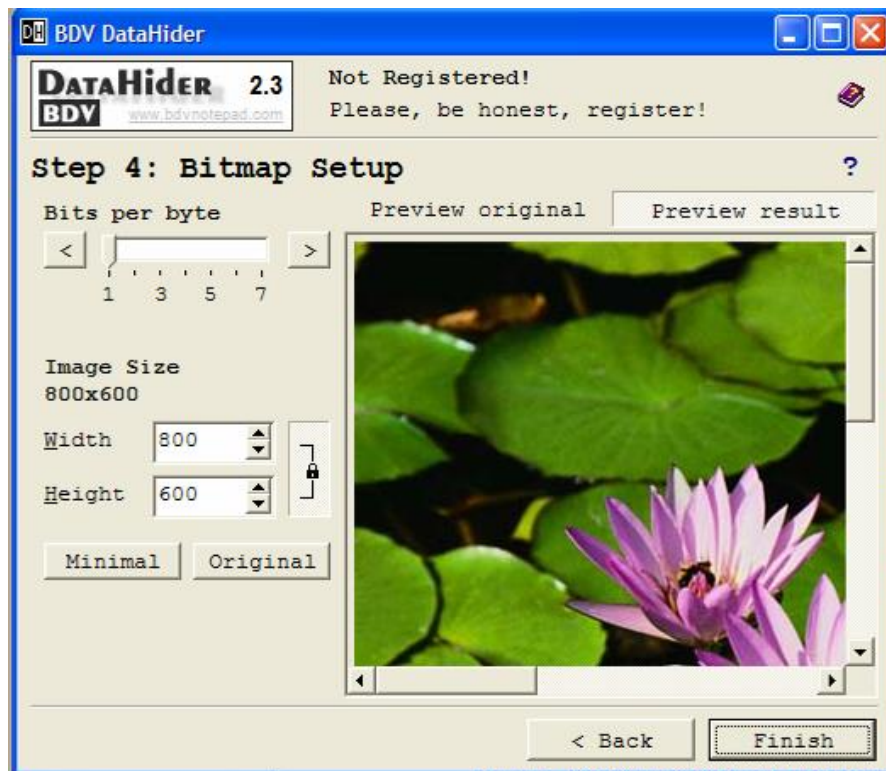


Рис. 5. Диалоговое окно настройки растрового изображения (шаг 4)

Рассмотрим более подробно настройки параметров данного изображения.

1) Bits per Byte. Эта опция служит для изменения глубины кодирования изображения. Чем больше эта величина, тем более заметны искажения графического изображения, но размер созданного файла может быть меньше.

2) Image Size. Параметры «Ширина» и «Высота» данной опции позволяют задать ширину и высоту созданного растрового изображения.

Кнопка «Минимальный» устанавливает минимально возможный размер созданного растрового изображения. Кнопка «Оригинал» устанавливает начальный размер.

Вы можете выбрать просмотр исходного или созданного растрового изображения, используя кнопки «Предварительный просмотр оригинала» или «Предварительный просмотр результата».

После нажатия на кнопку «Готово» появится окно «Сохранить» для сохранения созданного растрового изображения с внедренным в него контейнером.

5. На следующей странице мастера (рис. 6) сообщается об успешном окончании операции. Если вы хотите отправить файл результатов по электронной почте, нажмите кнопку «Отправить».

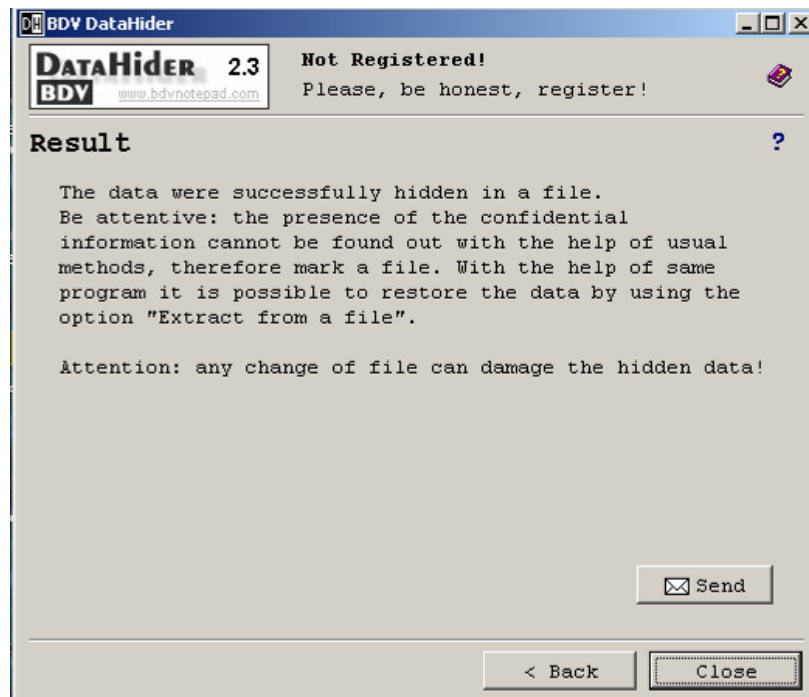


Рис. 6. Информационное окно программы с сообщением об успешном окончании операции.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. С помощью программы BDV DataHider создайте текстовое сообщение произвольного содержания и внедрите его в графический файл «Водяные лилии», находящийся в папке, указанной преподавателем.

2. В текстовом редакторе MS Word создайте два документа произвольного содержания. С помощью программы BDV DataHider первый документ внедрите:

- а) в графический файл «Голубые холмы»;
- б) во второй документ MS Word.

3. Воспользуйтесь функцией «Hide the data on a portable disk» (скрытие данных на съемном диске) программы BDV DataHider и осуществите создание защищенного съемного носителя информации (при его наличии).

4. Продемонстрируйте работу и файл-отчет преподавателю.

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

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

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое стеганография? Для чего она применяется?
2. Какие алгоритмы шифрования использует программа «BDV DataHider»?
3. Перечислите основные действия для создания стеганографического контейнера с помощью программы «BDV DataHider».