НАРОДНАЯ УКРАИНСКАЯ АКАДЕМИЯ

В. А. Кирвас

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. АРХИВАТОРЫ И АНТИВИРУСЫ

Учебное пособие

Издательство НУА

НАРОДНАЯ УКРАИНСКАЯ АКАДЕМИЯ

В. А. Кирвас

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. АРХИВАТОРЫ И АНТИВИРУСЫ

Учебное пособие для студентов первого курса
высших учебных заведений

Харьков
Издательство НУА
2012

УДК 004.492 + 004.627 (075.8)
ББК 32.973.26-018.2 я73-1
К43

Утверждено на заседании кафедры
информационных технологий и математики
Народной украинской академии.
Протокол № 8 от 6.02.2012

Рецензент д-р техн. наук, проф. *Е. И. Бобыр*, Новокаховский политехнический институт.

Наведено загальні властивості й принципи архівації файлів, розглянута робота з найбільш популярними ліцензійними архіваторами WinZip та WinRAR, а також із безкоштовними програмами 7-Zip й IZArc. Розглянуто комп'ютерні віруси, методи захисту від них і робота з одним із кращих антивірусів – програмним продуктом Касперського. Наведено основні правила антивірусної безпеки. Містить словник основних термінів і список рекомендованої літератури.

Призначено для самостійної роботи студентів.

Кирвас, Виктор Андреевич.

К43 Информационная безопасность. Архиваторы и антивирусы: учебное пособие для студентов 1 курса вузов / В. А. Кирвас ; Нар. укр. акад., [каф. информ. технологий и математики]. – Харьков : Изд-во НУА, 2012. – 108 с.

Приведены общие свойства и принципы архивации файлов, рассмотрена работа с наиболее популярными лицензионными архиваторами WinZip и WinRAR, а также с бесплатными программами 7-Zip и IZArc. Рассмотрены компьютерные вирусы, методы защиты от них и работа с одним из лучших антивирусов – программным продуктом Касперского. Приведены основные правила антивирусной безопасности. Содержит словарь основных терминов и список рекомендуемой литературы.

Предназначено для самостоятельной работы студентов.

УДК 004.492 + 004.627 (075.8)
ББК 32.973.26-018.2 я73-1

ВВЕДЕНИЕ

Данные, содержащиеся в компьютере, зачастую являются более дорогими, чем сам компьютер. В случаях потери информации, когда невозможно восстановить эти данные, это может привести (и часто приводит) к большим личным ущербам или даже к полному краху отдельных компаний, потерявших свои данные. Обезопасить на 100% свой компьютер не может никто. Даже опытный пользователь постоянно подвержен угрозам со стороны других, более опытных хакеров. Но совершать элементарные простейшие действия и следовать простым логическим правилам информационной безопасности может и должен каждый пользователь.

Пользователям персонального компьютера (ПК) приходится защищаться от традиционных вирусов и «троянских» приложений, от сетевых атак, кражи личной информации, жуликов в социальных сетях и даже фальшивых антивирусов. Киберзлоумышленники все активнее используют популярные поисковые системы для перенаправления пользователей на страницы, которые специально разработаны для распространения вредоносного программного обеспечения (ПО). Для заражения пользователя обычно достаточно одного «клика» по гиперссылке или сообщению электронной почты, поэтому антивирусная проверка почтового и Интернет-трафика является одной из главных задач обеспечения информационной безопасности.

Студентами Харьковского гуманитарного университета «Народная украинская академия» в первом семестре в рамках дисциплины «Информатика» изучается тема «Информационная безопасность. Архиваторы. Антивирусные программы». В данном пособии приведены принципы, правила, советы, утилиты и сервисы по информационной безопасности ПК, рассмотрена работа с одним из лучших антивирусов – программным продуктом Касперского. Эти данные должны оказать помощь студентам в изучении указанной темы, а рассмотренные вопросы помогут всем пользователям в решении проблем компьютерной безопасности, помогут защитить ПК и сохранить нужную информацию, удалить вирусы и вылечить компьютер.

Другая проблема заключается в том, что хранение и передача информации все чаще осуществляется в цифровом виде. Сегодня происходит лавинообразное увеличение объемов данных, которые нужно хранить и передавать. Наиболее дешевым вариантом защиты данных от разрушения и утери в процессе их хранения и передачи, а также в результате различных аварийных ситуаций является архивирование. В пособии рассмотрена работа с наиболее популярными лицензионными архиваторами WinZip и WinRAR, а также с бесплатными программами 7-Zip и IZArc.

При разработке данного пособия были использованы материалы сайтов: win-rar.ru, kaspersky.ru, antivibest.ru, ru-best.ru, biblprog.org.ua, kocby.ru и др., а также справки программ Kaspersky Internet Security 2012, 7-Zip, IZArc, WinZip, WinRAR.

ГЛАВА 1. АРХИВАТОРЫ

При интенсивной работе с данными на компьютере возникают две проблемы. Первая – непрерывный рост объема информации, который необходимо хранить на диске, и рост количества данных, которые отправляются по электронной почте или переносятся с одного компьютера на другой (исчисляются гигабайтами и даже терабайтами). Вторая – возможность порчи или потери информации на магнитном диске, обусловленная его физическим разрушением, случайным уничтожением объектов или наличием какого-либо компьютерного вируса. Причины потери данных, согласно статистике, собранной профильными компаниями, распределяются так: 40% – неисправности и сбои оборудования; 29% – ошибки пользователя; 13% – ошибки программного обеспечения (ОС, утилиты, прикладные программы); 9% – преднамеренный ущерб данным (кража, повреждение и т.п.); 6% – воздействие вирусов и другого вредоносного ПО; 3% – внешние воздействия (стихийные бедствия, пожары и т.п.).

Первую проблему можно решать увеличением емкости и количества носителей информации (учитывая их удешевление) или же уплотнением, упаковкой данных на этих дисках. Решение второй проблемы обеспечивается механизмом резервного копирования, например, с помощью программы, встроенной в операционную систему. В этом случае также может помочь сжатие, архивация данных. В общем, зачем нужны архиваторы?

- для сжатия и архивирования файлов;
- для сжатия приложений к электронным письмам;
- для защиты файлов и вложений паролем;
- для блокировки файлов;
- для разделения файлов на несколько частей;
- для создания самораспаковывающихся архивов;
- для создания резервных копий;
- для защиты файлов от повреждений.

Несмотря на то, что со временем места на дисках стало значительно больше, а скорости в Интернете возросли многократно, архиваторы по-прежнему остаются одними из самых используемых программ в арсенале любого пользователя компьютера. На сегодня архиватор – пожалуй, самая распространенная программа после операционной системы и браузера.

1.1. Общие сведения об архивации файлов

Сжатие – это специальный метод кодирования данных с целью уменьшения их размера. Точнее, сжатие информации — это процесс преобразования информации, хранящейся в файле, к виду, при котором уменьшается избыточность в ее представлении и, соответственно, требуется меньший объем памяти

для хранения. Это позволяет экономить дисковое пространство, расходы на передачу данных и, самое главное, рабочее и личное время.

Сжиматься могут как один, так и несколько файлов, которые в сжатом виде помещаются в так называемый *архивный файл* или *архив*.

Архивный файл или *архив* — это специальным образом организованный файл, содержащий в себе один или несколько файлов в сжатом или несжатом и/или зашифрованном виде и служебную информацию об именах файлов, дате и времени их создания или модификации, размерах и т.п.

Имена файлов архивов обычно заканчиваются расширением *.zip, .rar, .lzh, .arj, .arc, .tar* и др. в зависимости от типа архиватора, в котором они были созданы.

Целями упаковки файлов обычно являются:

- обеспечение более компактного размещения информации на диске;
- сокращение времени и соответственно стоимости передачи информации по каналам связи в компьютерных сетях.

Кроме того, упаковка в один архивный файл группы файлов:

- существенно упрощает их перенос с одного компьютера на другой;
- сокращает время копирования файлов на диски;
- позволяет защитить информацию от несанкционированного доступа;
- способствует защите от заражения компьютерными вирусами.

Принято различать *архивацию* и *упаковку* (или *компрессию, сжатие*) данных. В первом случае речь идет о слиянии нескольких файлов и даже каталогов в единый файл – архив, во втором – о сокращении объема исходных файлов путем устранения избыточности. Как правило, современные программные архиваторы обеспечивают также сжатие данных, являясь еще и упаковщиками. Поэтому далее будем придерживаться следующих определений.

Архивация (упаковка) — помещение (загрузка) исходных файлов в архивный файл в сжатом или несжатом виде.
Разархивация (распаковка) — процесс восстановления файлов из архива точно в таком виде, какой они имели до загрузки в архив.

При распаковке файлы извлекаются из архива и помещаются на диск или в оперативную память.

Программы, осуществляющие упаковку и распаковку файлов, называются *программами-архиваторами*.

Программы-архиваторы не входят в комплект поставки ОС Windows и на конкретном компьютере могут отсутствовать!

Принцип работы архиваторов основан на поиске в файлах избыточной информации и последующем её кодировании, чтобы получить минимальный

объем хранимых данных. В настоящее время известно множество различных алгоритмов сжатия информации. Однако для пользователя, в принципе, не столь важно, какой алгоритм функционирует внутри программы-архиватора. Важнее интегральное качество системы сжатия. Например, в список задач архиваторов может входить не только сжатие/распаковка файлов, но и сохранение дерева файловой системы, атрибутов и имен файлов, шифровка данных архива, архивация с паролем и т.д.

Степень сжатия файлов характеризуется коэффициентом *Кс*, определяемым как отношение объема сжатого файла *Vc* к объему исходного файла, *Vo*, выраженное в процентах:

$$K_c = \frac{V_c}{V_o} 100\%.$$

Степень сжатия зависит от используемой программы, метода сжатия и типа исходного файла. Наиболее хорошо сжимаются файлы графических образов, текстовые файлы и файлы данных, для которых степень сжатия может достигать 5–40%, меньше сжимаются файлы исполняемых программ и загрузочных модулей – 60–90%. Почти не сжимаются архивные файлы.

Большие по объему архивные файлы могут быть разбиты на несколько частей. Такие архивы называются *многотомными*, а их составные части – *томами*. Создавая архив из нескольких частей, можно копировать и хранить его части на нескольких носителях (дисках, флешках и пр.).

Сегодня архиватор чаще всего используется для упорядочивания файлов, для хранения или пересылки. Речь идет о том, что, например, при отправке пакета однотипных документов по электронной почте гораздо лучше заархивировать их в единый файл архива, чем прикреплять каждый из них в качестве отдельного вложения. Помимо этого существует достаточно большое количество медиаформатов, которые трудно подвергаются сжатию, – это фотографии в форматах JPG, музыка в MP3, видеофильмы в AVI и так далее. Архиватор в этом случае выступает в роли приложения, которое позволяет «разрезать» или единый файл, или коллекцию однотипных файлов на части – тома архивов с целью преодоления, например, лимита на одиночную загрузку на файлообменниках или на почтовых серверах.

Чтобы не зависеть при распаковке данных от наличия соответствующей программы-архиватора, можно создать так называемый *самораспаковывающийся* архивный файл.

Самораспаковывающийся архивный файл – это загрузочный, исполняемый модуль, который способен к самостоятельной разархивации находящихся в нем файлов без использования программы-архиватора.

Самораспаковывающийся архив получил название *SFX-архив* (англ. SelF-eXtracting). Архивы такого типа обычно создаются в форме EXE-файла. Они чуть больше обычных, но для их распаковки не требуются дополнительные программы.

Наиболее популярными программами-архиваторами в настоящее время являются *WinZip* и *WinRAR*. «Родным» архивным форматом первого из них является формат ZIP, второго – RAR, несмотря на то, что каждый из них поддерживает работу еще с десятками других архивных форматов. Ниже описаны преимущества каждого из них.

Архивы ZIP

Основное преимущество формата ZIP – его распространенность и популярность. Так, большинство архивов в Интернете имеют формат ZIP. Кроме того, например, *WinZip 14 Pro* поддерживает распространенные в Интернете форматы сжатия: RAR, 7Z, BZ2, LHA / LZH, CAB, IMG, ISO, TAR, GZIP, GZ, TAZ, TGZ, TZ, Z, UU, UUE, XXE, B64, MIM, BHX, HQX. Другое преимущество ZIP – скорость. Архивы ZIP обычно создаются быстрее архивов RAR.

Архивы RAR

WinRAR может создавать архивы форматов как RAR, так и ZIP, а архиватор WinZip формат RAR не создает. Формат RAR в большинстве случаев обеспечивает существенно лучшее сжатие, чем ZIP. WinRAR, кроме обычного режима сжатия, имеет режим *solid*, в котором создается специальный архив с повышенной степенью сжатия и особой структурой организации (*непрерывный архив*). Непрерывный архив – это специальный метод архивирования файлов, при котором данные упаковываются в виде непрерывного потока. Метод позволяет существенно увеличить коэффициент сжатия, если в архив помещается большое количество небольших файлов и одинакового формата.

Другая важная возможность RAR – поддержка *многотомных архивов*. Они намного удобнее и проще в использовании, чем так называемые «разделенные по дискам» (span disks) архивы ZIP. Настоящие многотомные архивы с изменением размера тома можно создавать только в формате RAR.

Кроме того, у формата RAR есть несколько важных возможностей, отсутствующих у ZIP, например добавление информации для восстановления, которое позволяет восстановить физически поврежденный файл, и осуществить блокировку важных архивов для предотвращения их случайной модификации.

Формат RAR позволяет обрабатывать файлы практически неограниченного размера (до 8589934591 Гб), а максимальный размер одного файла в архиве ZIP ограничен 2 Гб.

Более подробно сравнение архивов RAR и ZIP приведено в приложении.

1.2. Основные особенности архиватора WinRAR

Многофункциональный интегрированный архиватор WinRAR является одним из самых популярных архиваторов, предоставленным в

настоящее время в распоряжение пользователей. Это мощный инструмент сжатия данных с огромным количеством дополнительных интегрированных функций.

Название программы образовано от слов WIN (Windows) и RAR (Roshal ARchive). Автором программы является Евгений Рошал (Roshal). WinRAR обладает интуитивным интерфейсом, что делает работу в нем очень простой и комфортной.

Существует несколько версий RAR для разных операционных систем, в частности, RAR для Windows, Linux, FreeBSD, DOS, OS/2, Mac OS X. WinRAR – это 32-разрядная версия архиватора RAR для Windows, мощного средства создания архивов и управления ими.

Основные свойства WinRAR:

- возможность работы в двух режимах — полноэкранного интерактивного интерфейса (WinRAR.exe) и обычного интерфейса командной строки (Rar.exe);
- поддержка других типов архивов. Кроме полной поддержки архивов RAR и ZIP, в WinRAR реализована поддержка основных операций для архивов форматов 7Z, ACE, ARJ, BZ2, CAB, GZ, ISO, JAR, LZH, TAR, UUE, Z, созданных с помощью других программ архивирования. К ним относятся: извлечение файлов, а также просмотр содержимого архива, комментариев и информации об архиве. Для работы с этими архивами не нужны никакие дополнительные программы;
- использование высокоэффективного метода сжатия solid (непрерывный архив) для получения высокой степени сжатия (на 10–50% выше, чем обычно);
- возможность создания самораспаковывающихся и многотомных архивов;
- защита архивов паролем;
- оболочка с поддержкой технологии «перетащить и оставить» (drag & drop).

Сервисные функции RAR:

- шифрование с паролем (WinRAR идеален для передачи конфиденциальных данных по Интернету и другим незащищённым каналам. 128-битная криптографическая защита и электронные подписи архивов не дадут злоумышленникам ни единого шанса узнать ваши секреты);
- добавление файловых и архивных комментариев;
- возможность частичного или полного восстановления поврежденных архивов;
- защита архива от изменений;
- поддержка технологии медиасжатия;
- возможность добавления в архив информации о создателе архива, времени и дате последних изменений, внесенных в архив.

WinRAR прекрасно подходит для сжатия мультимедийных файлов. Программа автоматически распознаёт формат файла и выбирает оптимальный метод упаковки. Преимущества RAR особенно заметны при архивировании исполняемых модулей (.EXE), объектных файлов (.OBJ), больших текстовых файлов и т.д.

Основные режимы работы архиватора WinRAR

Оболочка WinRAR имеет два основных режима: *режим управления файлами* и *режим управления архивами*.

В режиме управления файлами в окне WinRAR показывается список файлов и папок в текущей папке (рис. 1.1). Можно выделить эти файлы и папки, как обычно в Windows, с помощью мыши или клавиатуры, и произвести с выделенными файлами различные операции, например, заархивировать их или удалить. В этом режиме также можно протестировать группу архивов и извлечь из них файлы.

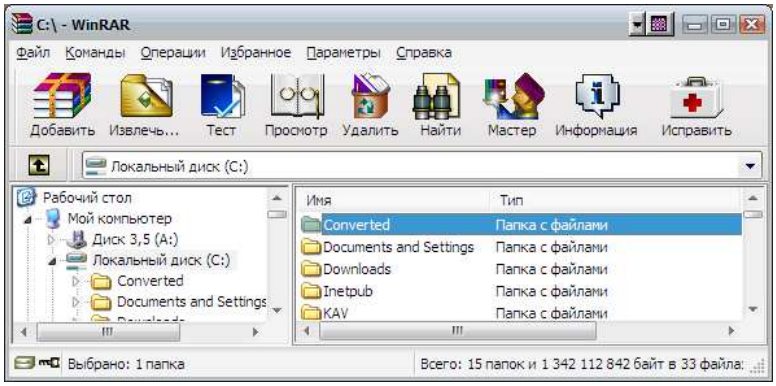


Рис. 1.1. Окно WinRAR в режиме управления файлами

В *режиме управления архивами* в окне WinRAR отображается список файлов и папок в открытом архиве (рис. 1.2).

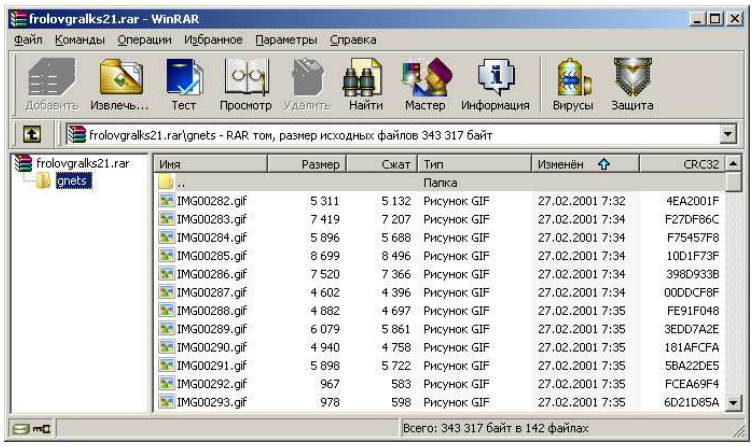


Рис. 1.2. Окно WinRAR в режиме управления архивами

Здесь также можно выделить файлы и папки и выполнить с ними различные действия, специфичные для архива, например, распаковать, протестировать или прокомментировать.

Для входа в *режим управления файлами* надо запустить WinRAR двойным щелчком на его значке. Для входа в *режим управления архивами* необходимо запустить WinRAR в *режиме управления файлами*, поместить курсор на выбранный архив и нажать **Enter** (это же можно сделать, выбрав в меню **Файл** пункт **Открыть архив** или дважды щелкнув мышью на имени архива). Кроме того, вход в *режим управления архивами* происходит в оболочке Windows (в *Проводнике* или на *Рабочем столе*) при двойном щелчке мышью по пиктограмме архива или при нажатии клавиши **Enter**.

Архивация файлов в оболочке WinRAR

Порядок действий при архивации данных таков.

1. Запустить *WinRAR* в *режиме управления файлами*, для этого дважды щелкнуть мышью или нажать **Enter** на значке **WinRAR** либо **Пуск** – **Все Программы** – **WinRAR** – пункт **WinRAR**.
2. Перейти в папку, в которой находятся файлы, предназначенные для архивации.
3. Выделить файлы и папки, которые необходимо заархивировать. Это можно сделать клавишами управления курсором или левой кнопкой мыши при нажатой клавише Shift (как в *Проводнике* и других программах Windows). Выделять файлы в окне WinRAR можно также клавишами **Пробел** или **Ins**. Клавиши **+** и **–** на цифровой клавиатуре позволяют выделять и снимать выделение с группы файлов с помощью шаблонов.
4. Щелкнуть на кнопке 

Добавить (это же можно сделать, нажав **Alt+A** или выбрав команду **Добавить файлы в архив** из меню **Команды**).

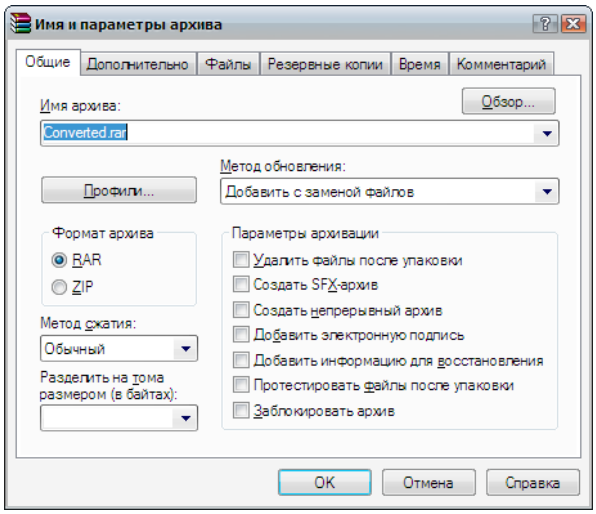


Рис. 1.3. Диалоговое окно указания имени и параметров архива

5. В появившемся диалоговом окне (рис. 1.3) ввести имя архива или просто подтвердить имя, предложенное по умолчанию.
6. Выбрать формат нового архива (**RAR** или **ZIP**), метод сжатия (рис. 1.4), размер тома и прочие параметры архивации. Для создания самораспаковывающегося архива следует установить флажок *Создать SFX-архив*.
7. Щелкнуть на кнопке **Ok** для создания архива.

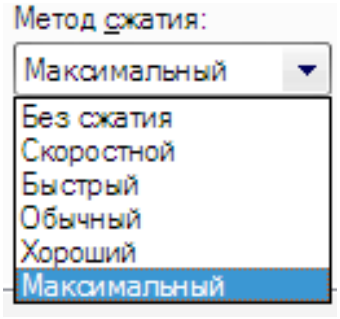


Рис. 1.4. Методы сжатия архивов RAR

Поддерживаются шесть методов сжатия. *Максимальный* метод обеспечивает наиболее высокую степень сжатия, но с наименьшей скоростью. Напротив, *Скоростной* сжимает плохо, но очень быстро. Метод *Без сжатия* просто помещает файлы в архив без их упаковки. Если создается ежедневная резервная копия данных, то, как правило, лучше использовать метод *Обычный*.

Размер словаря (вкладка ***Дополнительные параметры сжатия***) может принимать значения 64, 128, 256, 512, 1024 и 4096 Кб. Чем больше размер словаря, тем лучше, но медленнее сжатие, т.е. здесь все аналогично выбору метода упаковки. В общем случае лучше установить размер словаря 4096 Кб и управлять соотношением размер/скорость, изменяя метод сжатия. Опытный пользователь может задать специальные параметры для сжатия текста, графических или аудиофайлов.

Для создания *многотомного архива* надо ввести размер тома.

Том — это фрагмент архива, состоящего из нескольких частей. Обычно тома используются для сохранения большого архива на нескольких сменных носителях.

Можно выбрать размер тома из списка предустановленных: 1,44 Мб (для дискет формата 3,5"), 700 Мб (для CD), 4,4 Гб (для DVD) и 98 Мб (для ZIP100) или указать самостоятельно. Если архивируются данные сразу на сменные диски, то лучше выбрать пункт *Автоопределение* – в этом случае WinRAR будет подбирать размер каждого нового тома так, чтобы максимально заполнить соответствующий диск.

По умолчанию тома RAR получают имена вида «имя_тома.partNNN.rar», где NNN — номер тома.

Созданные многотомные архивы не допускают изменения, т.е. в них нельзя добавлять, обновлять или удалять файлы.

Для распаковки томов необходимо начинать извлечение с первого тома. Если тома находятся на несменном носителе (например, на жёстком диске), то сначала нужно переписать все тома в одну папку.

Тома также могут быть *непрерывными* и *самораспаковывающимися*. Первый самораспаковывающийся том имеет другое (т.е. не .rar) расширение, например, для SFX-томов DOS это будет **.exe.**

Архивирование файлов в окнах Мой компьютер и Проводник

При установке программы WinRAR на ПК программа интегрируется в оболочку операционной системы (хотя пользователь может в процессе установки отменить эту возможность). В результате архивировать файлы становится значительно удобнее, даже не запуская саму программу-архиватор.

Если WinRAR при инсталляции на компьютер не был интегрирован в оболочку ОС, это можно сделать и позже – вызвав командой *Параметры / Установки* диалоговое окно *Параметры* и на вкладке *Интеграция* установив флажок *Встроить WinRAR в оболочку ОС.*

Для архивации в окне *Проводник* или *Мой компьютер*:

- выделить файлы, которые надо заархивировать;
- нажать правую кнопку мыши на выделенных файлах и в контекстном меню выбрать команду **Добавить в архив**...;
- в появившемся диалоговом окне (см. рис. 1.3) ввести имя архива или просто подтвердить имя, предложенное по умолчанию. Здесь же можно выбрать прочие параметры архивации;
- щелкнуть на кнопке **Ok** для создания архива. Архив будет создан в той же папке, где находятся выделенные файлы.

Чтобы добавить файлы в предложенный архив без дополнительных запросов, нужно воспользоваться командой **Добавить в архив "имя архива.rar"**. В этом случае будут применены параметры архивации из профиля архивации по умолчанию.

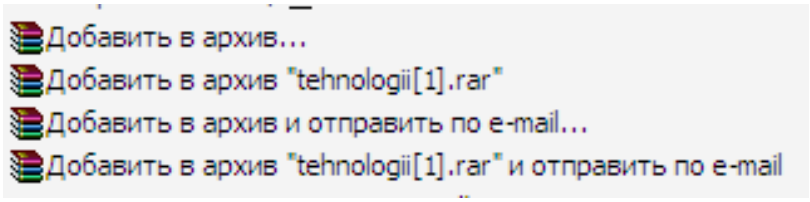


Рис. 1.5. Фрагмент контекстного меню файлов и папок Проводника

Если требуется добавить файлы в уже существующий архив, самым простым способом будет перетащить их пиктограммы на значок существующего архива.

Разархивирование файлов

Извлечение файлов в программах *Проводник* и *Мой компьютер*

Самый простой способ разархивации файлов – выбрать из контекстного меню архива (рис. 1.6) команду *Извлечь файлы*, после чего ввести в появившемся диалоговом окне имя папки, в которую их надо извлечь, и нажать кнопку *Ok*.

Можно также выбрать в контекстном меню команду *Извлечь в <имя папки>*, чтобы распаковать файлы в предложенную папку без каких-либо дополнительных запросов.

Также весьма удобным методом является перетаскивание одного или нескольких архивов правой кнопкой мыши в папку назначения и выбор из появившегося меню команды *Извлечь в <имя папки>* (рис. 1.7).

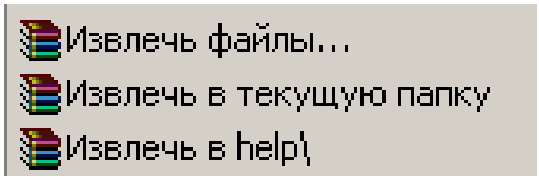


Рис. 1.6. Фрагмент контекстного меню архивного файла

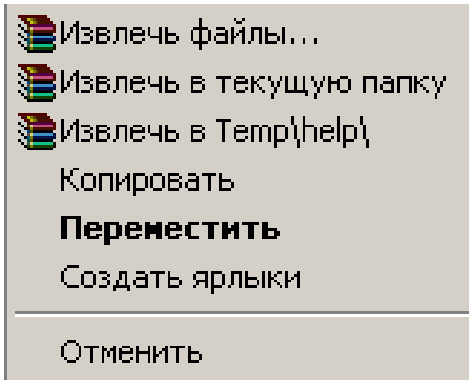


Рис. 1.7. Контекстное меню перетаскивания архивного файла

Извлечение файлов в оболочке WinRAR

1. Открыть архив в WinRAR. Это можно одним из следующих способов:
   - дважды щелкнуть мышью или нажать **Enter** на файле архива в оболочке Windows;
   - дважды щелкнуть мышью или нажать **Enter** на файле архива в окне WinRAR;
   - перетащить архив на значок или окно WinRAR (перед тем как это сделать, убедитесь, что в окне WinRAR не открыт другой архив, иначе перетаскиваемый архив будет добавлен в открытый).
2. Выделить файлы и папки, которые необходимо извлечь.

3. Щелкнуть на кнопке 

Извлечь на панели инструментов окна WinRAR (это же можно сделать, нажав **Alt+E** или выбрав пункт **Извлечь в указанную папку** в меню **Команды**).

Во время извлечения отображается окно со статистикой. Если нужно прервать извлечение, щелкните на кнопке **Отмена**. Можно минимизировать окно WinRAR в системный трей на панели задач, нажав кнопку **Фоновый**.

Удаление файлов из архива

Эта команда доступна как в *режиме управления файлами*, так и в *режиме управления архивами*.

Чтобы удалить из архивного файла часть информации (файлы либо папки), надо открыть его в *режиме управления архивами* в окне WinRAR, выделить требуемые файлы и нажать клавишу **Delete**. Можно использовать также пункт *Удалить файлы* меню **Команды**, кнопку панели инструментов 

Удалить, клавиши **Alt+D** или **Del**. Выделенные файлы и папки будут удалены окончательно, отменить удаление будет невозможно, поэтому нужно делать это осторожно.

Удаление в окне WinRAR файлов или папок в *режиме управления файлами* (в файловой оболочке, а не из архивного файла) осуществляется, как обычно в Windows, через *Корзину* – случайно удаленные данные можно будет восстановить.

Полностью удалять файлы, не помещая их в *Корзину*, можно и в *режиме управления файлами*. Для этого вместо клавиши **Del** можно использовать комбинацию клавиш **Shift+Del**.

Дополнительные возможности

Непрерывный архив – это архив RAR, упакованный специальным способом, при котором все сжимаемые файлы рассматриваются как один последовательный поток данных. Непрерывная архивация поддерживается только в формате RAR, для формата ZIP такого типа архива не существует. Метод сжатия для архивов RAR – обычный или непрерывный – выбирает пользователь в диалоговом окне (рис. 1.3).

Непрерывная архивация значительно увеличивает степень сжатия, особенно при добавлении значительного количества небольших похожих файлов. Однако следует учитывать некоторые недостатки непрерывной архивации:

- обновление непрерывных архивов происходит медленнее, чем обычных;
- зашифрованные непрерывные архивы невозможно изменять;
- для извлечения одного файла из непрерывного архива необходимо проанализировать все предыдущие заархивированные файлы, поэтому извлечение отдельных файлов из середины непрерывного архива происходит медленнее, чем извлечение из обычного архива;
- если в непрерывном архиве какой-либо файл окажется поврежденным, то не удастся извлечь и все файлы, следующие после него. Поэтому при сохранении непрерывного архива на ненадежном носителе рекомендуется добавлять информацию для восстановления.

Непрерывные архивы лучше использовать в тех случаях, когда: архив редко обновляется; нет необходимости часто извлекать из архива один или несколько файлов; степень сжатия важнее скорости сжатия.

Самораспаковывающийся архив

Созданный ранее архивный файл можно преобразовать в самораспаковывающийся. Для этого предназначена команда **Преобразовать архив в SFX** в меню **Операции** и кнопка  **SFX** на панели инструментов.

Самораспаковывающиеся SFX-архивы удобны в тех случаях, когда нужно передать кому-то архив, но вы не уверены, что у адресата есть соответствующий архиватор для его распаковки.

SFX-архивы, как и любые другие исполнимые файлы, обычно имеют расширение **.exe**.

Защита архива от несанкционированного доступа

Чтобы зашифровать файлы, необходимо указать ***пароль***. Установка пароля может быть произведена до начала архивации с помощью команды **Установить пароль по умолчанию** в меню **Файл** или щелчком мыши на маленьком значке ключа  в левом нижнем углу окна WinRAR. Когда пароль по умолчанию задан, значок ключа меняет свой цвет с желтого на красный. Кроме того, если начинать архивацию с использованием пароля, заголовок диалога ввода имени и параметров архива дважды мигнет.

Не надо забывать удалять введенный пароль после того, как он становится ненужным, иначе можно случайно запаковать какие-либо файлы с паролем, абсолютно не намереваясь этого делать. Для удаления пароля нужно ввести пустую строку в диалоге ввода пароля или закрыть WinRAR и снова его запустить.

Можно ввести пароль в процессе архивации файлов – для этого в диалоговом окне **Имя и параметры архива** (рис. 1.3) надо перейти на вкладку **Дополнительно** и нажать кнопку **Установить пароль**.

Если пароль введен непосредственно в диалоговом окне, то не нужно отменять его самостоятельно – пароль будет действителен только в течение одной архивации, по окончании которой сбросится автоматически.

Шифрование имен файлов

В отличие от ZIP, формат RAR позволяет шифровать не только данные файлов, но и другие важные области архива: имена файлов, размеры, атрибуты, комментарии и другие блоки. Для использования этой функции нужно включить параметр *Шифровать имена файлов* в диалоговом окне задания пароля. Зашифрованный в таком режиме архив нельзя без пароля не только распаковать, но даже просмотреть список находящихся в нём файлов.

При извлечении зашифрованных файлов можно ввести пароль заранее, хотя это и необязательно. Если пароль не был введен перед началом извлечения и WinRAR обнаружил зашифрованный файл, он спросит пароль у пользователя.

1.3. Основные особенности архиватора WinZIP

Многим пользователям программа WinZip служит для открытия Zip-файлов, обычно загруженных из Интернета или полученных во вложении электронного сообщения, а также, как обычно, для создания Zip-файлов в целях ускорения отправки сообщений и экономии места на диске.

Для запуска программы WinZip служит команда меню Пуск / Все программы / WinZip / WinZip. Можно открыть окно программы (рис. 1.8) и двойным щелчком по любому Zip-файлу.

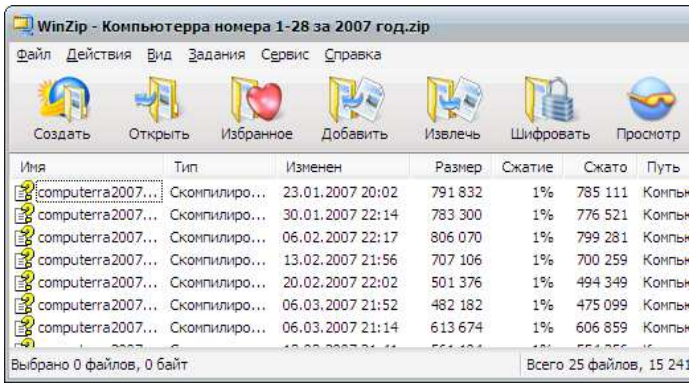


Рис. 1.8. Фрагмент основного окна WinZip

Архиватор WinZip имеет два интерфейса: *мастер* и *классический*.

Интерфейс мастера предназначен скорее для новичков; чтобы открыть программу в этом режиме, надо нажать кнопку **Мастер** на панели инструментов. Появится диалоговое окно с вопросом **Что вы хотите сделать?** Просто надо выбрать пункт **Создать новый Zip-файл** и нажать кнопку **Далее**. Мастер WinZip поможет выполнить всю процедуру.

Пользователи, хорошо знакомые с операциями с Zip-файлами, могут выбрать классический интерфейс WinZip. В этом интерфейсе доступно множество дополнительных возможностей, которых нет в интерфейсе мастера WinZip.

Создание нового архива

Последовательность действий для архивирования файлов такова. Сначала необходимо выбрать в меню **Файл** команду **Создать архив** или щелкнуть по кнопке 

Создать на панели инструментов.

В появившемся диалоговом окне **Создание архива** нужно набрать название создаваемого архива (*но не названия архивируемых файлов*) и нажать **ОК**. В результате будет создан новый *пустой архив*.

Архив можно создать непосредственно на *Рабочем столе*, в окнах *Мой компьютер* или *Проводник*. Для этого надо щелкнуть в свободном месте *Рабочего стола* или окон правой кнопкой мыши и выбрать из контекстного меню команду **Файл WinZip**. На *Рабочем столе* или в активной папке окон *Мой компьютер* или *Проводник* появится пустой файл-архив с именем **Файл WinZip.zip** (затем файл можно переименовать).

Добавление файлов в архив

Для выбора и добавления в архив файлов необходимо:

- выбрать команду **Добавить** в меню **Действия** или щёлкнуть по кнопке **Добавить** на панели инструментов главного окна архиватора;
- в раскрывшемся диалоговом окне *Добавить* (рис. 1.9) выбрать папку, из которой надо взять файлы для архивирования;
- выбрать нужные файлы (можно выделить сразу несколько файлов с помощью клавиш Ctrl (для несмежных файлов) и Shift (для смежных), установить степень сжатия и нажать кнопку **Добавить**. Выбранные файлы будут помещены в архив.

Обычно после создания архива в него сразу же добавляют файлы, поэтому, чтобы диалоговое окно **Добавить** открылось автоматически, убедитесь, что в **Сервис / Параметры / Расширения Проводника** выбран флажок **Добавить в...**.

Всего в поле **Действие** предлагается четыре варианта добавления файлов в архив:

Добавить (и заменить) файлы – WinZip копирует указанные файлы в архив, оставляя их в своей папке (т.е. получается две копии для каждого файла – исходная и упакованная).

Обновить существующие файлы – обновляет уже имеющиеся в архиве файлы на их более новые варианты (сравниваются время и даты создания файлов).

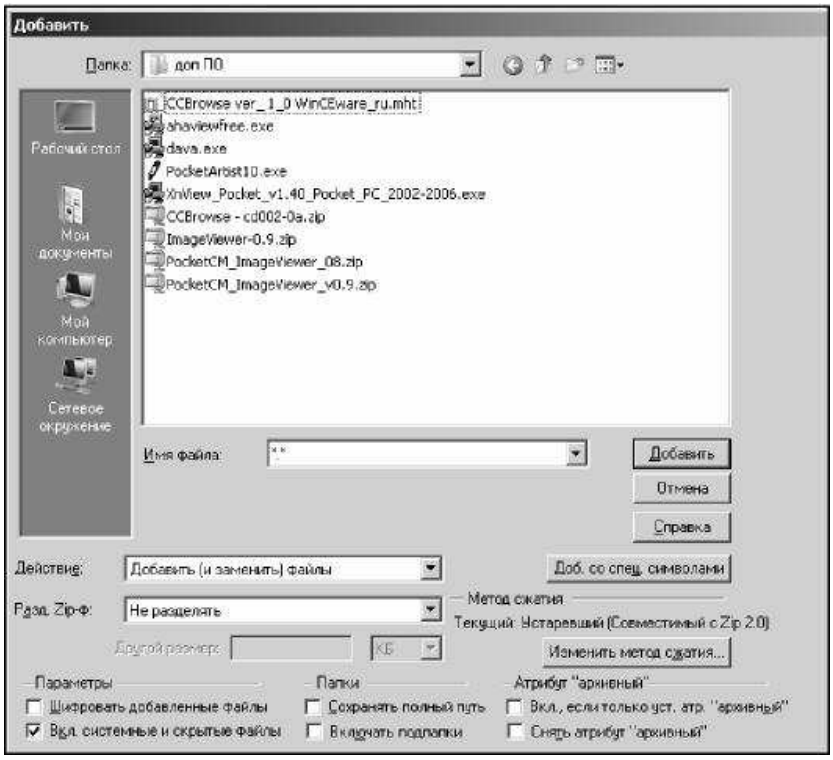


Рис. 1.9. Окно добавления файлов в архив

Переместить (и заменить) файлы – работает аналогично первому пункту, но после добавления файлов в архив их исходные копии удаляются с диска.

Обновить (и добавить) файлы – выполняет те же действия, что и предыдущий пункт, но при этом добавляет в архив файлы, которых раннее не было в этом архиве.

Другие способы добавления файлов в архив:

- перетащить их мышкой из *Моего компьютера* или *Проводника* в окно *WinZip*;

- перетащить их на значок файла-архива Файл WinZip или использовать контекстное меню в окнах *Мой компьютер* или *Проводник*.

Архивация файлов в окнах Мой компьютер и Проводник

Программа WinZIP может быть интегрирована в оболочку Windows, что обычно и происходит при установке по умолчанию. В противном случае можно добавить возможности интеграции, выбрав в окне программы пункт меню *Сер-*

вис / Параметры. На вкладке *Расширения Проводника* надо отметить флажками названия команд, которые будут добавлены в контекстное меню файлов в Проводнике.

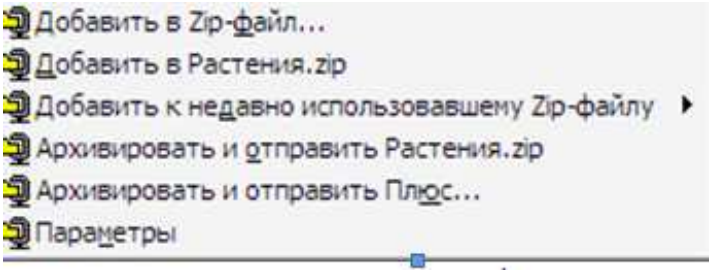


Рис. 1.10. Фрагмент контекстного меню файлов и папок Проводника при архивировании программой WinZIP

Архивация файлов непосредственно из *Проводника* или *Моего компьютера* значительно упрощает весь процесс. Для этого надо всего лишь выделить файлы и (или) папки для архивирования и выбрать в их контекстном меню (рис. 1.10) нужную команду.

Открытие существующего архива

Первый способ

Дважды щелкнуть по названию архива в *Моем компьютере* или *Проводнике*.

Второй способ

1. Выбрать в меню **Файл** команду **Окрыть архив** или нажать на панели инструментов главного окна архиватора кнопку 

Открыть. При этом активизируется стандартное диалоговое окно **Открытие архива**.
2. Выбрать в этом диалоговом окне нужный архив и папку.
3. Нажать кнопку **OK**.

Третий способ

1. Щелкнуть по архиву в *Моем компьютере* или *Проводнике*.
2. Удерживая кнопку мыши, передвинуть (перетащить) указатель мыши в окно WinZip.
3. Отпустить кнопку мыши. При этом выбранный архив откроется.

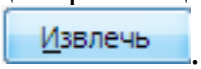
Извлечение файлов из открытого архива

Когда извлекается файл, WinZip распаковывает его и помещает в выбранную папку. Можно восстанавливать целые папки, сохраняя структуру подпапок.

Чтобы вывести на экран диалоговое окно **Извлечь**, нажмите кнопку **Извлечь** на панели инструментов или выберите команду **Извлечь** в меню **Действия**.

WinZip извлечет файлы из архива в папку, указанную в поле **Извлечь в:**.

Задать название папки можно любым способом:

- выбрать папку и устройство в дереве папок;
- напечатать имя папки в поле **Извлечь в**:...;
- раскрыть список **Извлечь в:** и выбрать папку из тех, в которые файлы извлекались ранее;
- нажать кнопку  и создать новую папку. После выбора папки для размещения извлекаемых из архива файлов щёлкните по кнопке 

.

Значительно более простой способ извлечения файлов – из окна *Проводника* или *Моего компьютера*, не запуская самой программы WinZip. Достаточно в контекстном меню Zip-архива (рис. 1.11) выбрать нужную команду.

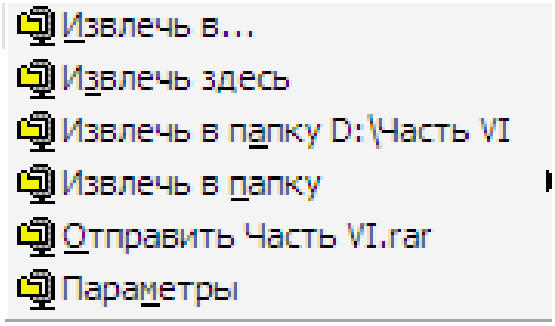


Рис. 1.11. Контекстное меню Zip-архива в Проводнике

Удаление файлов из архива

Проще всего удалить файлы из архива, выделив в окне WinZip ненужные более файлы, а затем выбрав команду **Удалить** в меню **Действия**. Эту операцию отменить нельзя.

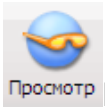
Просмотр файла без извлечения из архива

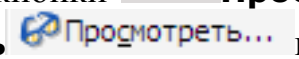
Просмотреть файлы в архиве можно несколькими способами.

Большинство файлов можно просмотреть, дважды щелкнув по названию в основном окне WinZip.

Если это исполняемый файл (имеет, например, расширение **exe**, **com**, **bat** или **PIF**), WinZip запустит его. Другие файлы откроются в соответствую-

щем приложении. Например, файлы с расширением **.txt** откроются в приложении *Блокнот*, с расширением **.doc** – в окне *Word*.

Другой способ – при помощи кнопки 

Просмотр на панели инструментов или команды **Просмотреть** 

из меню **Действия**.

В этом случае вызывается диалоговое окно **Просмотр**, которое также дает возможность просмотреть выбранные файлы.

Создание самораспаковывающегося архива

Самораспаковывающийся Zip-файл – это исполнимая программа (**EXE-файл**), которая содержит одновременно и Zip-архив, и программу для извлечения его содержимого. Пользователь запускает (выполняет) такой файл, как обычную программу.

Создание самораспаковывающегося архива состоит из двух этапов:

1. Создание обычного архива (файла с расширением **.zip**) или открытие ранее созданного в окне архиватора.
2. Создание самораспаковывающегося архива (файла с расширением **.exe**) с помощью программы **WinZip Self-Extractor Personal Edition**. Для этого необходимо в окне программы WinZip открыть ранее созданный Zip-архив и выбрать в меню **Действия** команду *Сделать .EXE файл*. В открывшемся окне (рис. 1.12) указать папку и название для создаваемого exe-файла и нажать кнопку *ОК*.

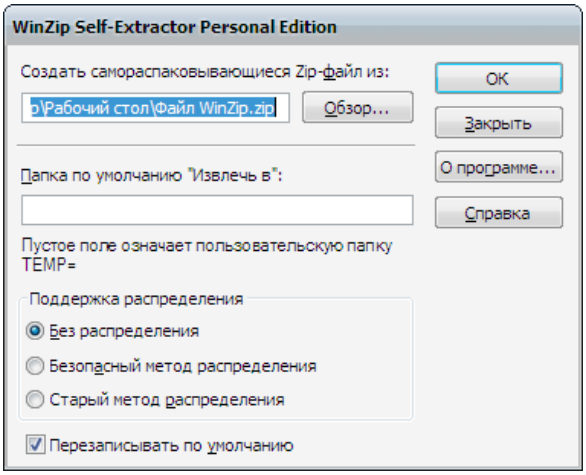


Рис. 1.12. Окно программы **WinZip Self-Extractor Personal Edition**

Самораспаковывающийся архив можно создать и вне окна программы WinZip. Для этого в окне *Мой компьютер* или *Проводник* в контекстном меню Zip-архива (или группе таких файлов) надо выбрать команду *Создать саморас-*

паковывающийся архив (*.Exe*). Самораспаковывающийся Zip-файл, имеющий значок 

, будет создан в текущей папке.

Создание многотомных архивов

WinZip позволяет создавать многотомные архивы. Это полезно, если файлы не должны превышать определенный размер или не умещаются на один диск.

Для этого надо сначала создать Zip-архив, а затем разделить его. Для разделения надо открыть Zip-архив в окне программы и в меню **Действия** выбрать команду *Разделить*. В диалоговом окне следует задать имя будущего разделенного архива, папку его размещения, размер тома (рис. 1.13) и нажать **ОК**.

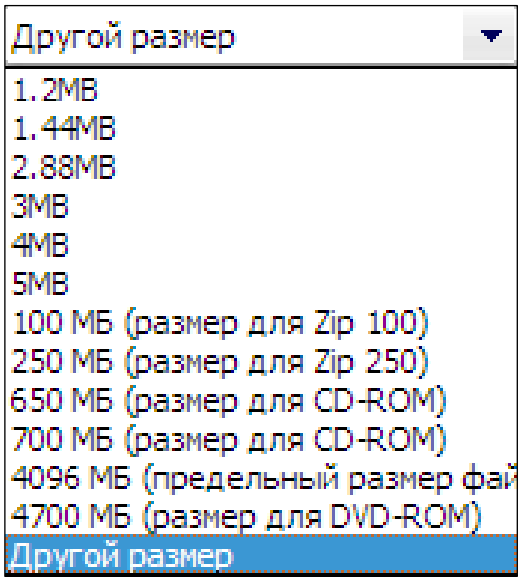


Рис. 1.13. Перечень вариантов размеров тома Zip-архива

В списке *Размер тома* можно выбрать не только один из заранее определенных размеров, но и опцию *Другой размер* и задать размер, отличающийся от стандартных.

Файлы многотомного архива будут иметь расширения .z01, z02 и т. д.

Из архива, занимающего несколько томов, нельзя ни удалить, ни добавить в него файлы.

В заключение надо отметить, что отсутствие в операционной системе Windows встроенных функций для работы с упакованными архивами обусловило появление огромного множества программ-архиваторов. Однако все со-

временные архиваторы обеспечивают практически одинаковое качество сжатия. Поэтому основная «борьба» развернулась за лучшее время сжатия и ковки, а также дополнительные возможности, облегчающие работу пользователя с архивом. Одни из наилучших результатов показывают программы WinZip и WinRAR. Сегодня они являются у нас самыми популярными архиваторами. Кроме платных (лицензионных) архиваторов, существуют и бесплатные архивирующие программы.

1.4. Бесплатные архиваторы

Бесплатные архиваторы далеко не всегда уступают платным. На сегодняшний день современные бесплатные программы-архиваторы с успехом могут заменить, а по некоторым функциям даже лучше выполнить работу, чем платные. Список бесплатных архиваторов довольно большой: 7-Zip, IZArc, PeaZip, TUGZip, Universal Extractor, FreeArc, jZip, KGB Archiver, SimplyZip, ZipItFree, ZipGenius, Fast Serial Archiver, RarMonkey, QuickZip, Gzip, vuZip, FilZip и др. Некоторые бесплатные программы обладают большими возможностями при работе с операционными системами и уже успели хорошо себя зарекомендовать. Большинство из них характеризуется высокой степенью сжатия данных, работой с большим количеством форматов (зачастую больше двадцати), возможностью легко и быстро извлекать сразу несколько файлов. Поэтому некоторые из них могут быть достойной заменой коммерческим архиваторам. Из большого выбора бесплатных архиваторов можно выделить самые популярные: 7-Zip, IZArc, TUGZip, PeaZip, FreeArc и Universal Extractor.

Лидером среди «альтернативных» архиваторов несколько лет является 7-Zip. По степени сжатия он является лучшим не только среди бесплатных программ, но и подавляющего большинства коммерческих продуктов. 7-Zip работает со всеми популярными форматами архивов, поддерживает шифрование, умеет создавать самораспаковывающиеся архивы и обладает многими другими удобными функциями.

К недостаткам 7-Zip относят малое количество поддерживаемых форматов. Поэтому, если нужен более гибкий бесплатный архиватор, можно присмотреться к IZArc. Это приложение умеет открывать около 50 типов архивов, включая многие редкие. Также он может архивировать и сохранять файлы в 12 различных форматах и обрабатывать многотомные ZIP-архивы.

Рядом с IZArc можно поставить и другой мультиформатный архиватор — TUGZip. Хотя количество поддерживаемых им форматов значительно меньше, чем у предыдущего, TUGZip имеет некоторые специальные возможности, например восстановление поврежденных архивов ZIP и SQX.

Другой небольшой бесплатный архиватор PeaZip, как и IZArc, поддерживает множество форматов архивов, включая ACE, ARJ, CAB, DMG, ISO, LHA, RAR и UDF. PeaZip работает как с 32, так и с 64-битными версиями Windows.

Программа FreeArc – современный и мощный архиватор общего назначения, созданный для операционных систем Linux и Windows. Отличительной особенностью программы является широкий выбор методов сжатия, благодаря которым FreeArc признан утилитой с высокой степенью сжатия файлов и отличной производительностью. Архиватор FreeArc работает в несколько раз быстрее (от 2 до 5) других упаковщиков, которые показывают ту же степень сжатия (например: ccm, 7-zip, rar, uharc-mz, pkzip). При этом программа характеризуется широким спектром алгоритмов сжатия мультимедийных данных. Утилита использует 11 различных алгоритмов и фильтров, к примеру, мощный бесплатный архиватор 7-Zip использует всего четыре, а известная программа архивирования данных WinRAR – только семь.

И наконец, Universal Extractor – это программа для любителей минимализма, которую нельзя назвать настоящим архиватором, сжимать файлы он не умеет. Зато он является наилучшим распаковщиком. Огромное количество поддерживаемых форматов делает его лучшим в этом секторе. Если часто приходится распаковывать экзотические форматы, то Universal Extractor может стать хорошим дополнением к одному из «полноценных» архиваторов.

Ниже рассмотрена работа с наиболее популярными бесплатными архиваторами 7-Zip и IZArc.

Архиватор 7-Zip

Программа 7-Zip (разработчик Игорь Павлов) является одним из самых молодых и популярных бесплатных архиваторов с возможностью высокого сжатия файлов. Архиватор успешно функционирует на большинстве версий ОС Windows. Программа имеет понятный простой интерфейс (рис. 1.14) и полное интегрирование с операционной системой. Рекомендуется для использования как в офисе, так и дома.

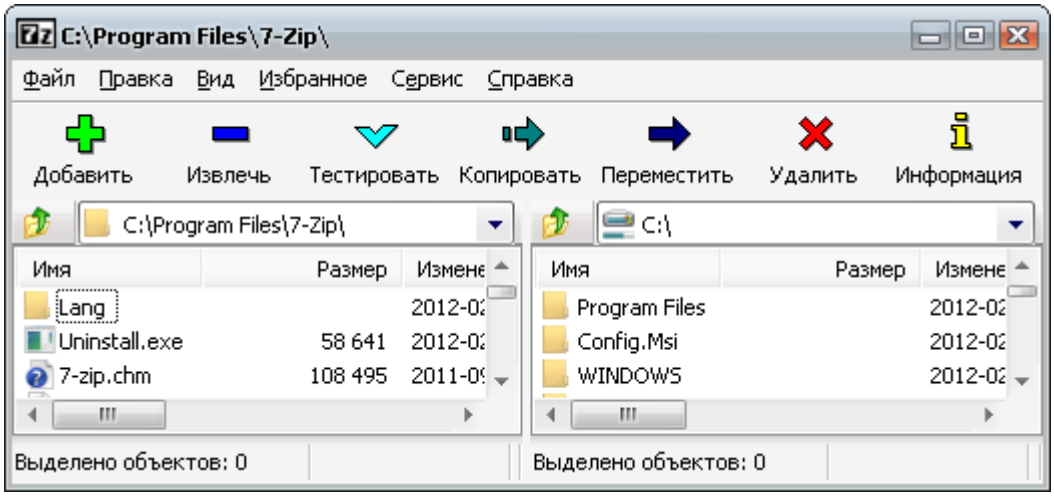


Рис. 1.14. Окно архиватора 7-Zip

Особенность программы

По степени сжатия 7-Zip является несомненным лидером среди подобных бесплатных и платных программных продуктов. Поддерживает несколько новых улучшенных алгоритмов сжатия, в программе содержится много точных и гибких настроек, для неопытных пользователей существуют готовые предустановки. Кроме того, программа имеет следующие возможности:

- Поддерживает различные форматы: 7z, MSI, RPM, ZIP, TAR, CPIO, CAB, Z, ARJ, WIM, CHM, DEB, NSIS, BZIP2, LZH, RAR, GZIP, ISO и RPM на уровне просмотра содержимого и распаковки.
- Высокое качество и степень сжатия файлов.
- Возможность создания самораспаковывающихся архивов.
- Интеграция в систему Windows, поддержка 32-х и 64-битных систем.
- Внутренний мощный двухоконный файловый менеджер.
- Встроенная в архиватор утилита для тестирования производительности.
- Имеется поддержка работы с помощью командной строки. При установке 7-Zip встраивается в контекстное меню ОС Windows для более удобной распаковки и создания архивов.
- Мультиязычный графический интерфейс (в том числе поддержка русского языка).
- Поддержка плагинов от программы FAR Manager (позволяет поддерживать работу без каких-либо внешних архиваторов).
- Наличие открытого исходного кода.
- Поддержка кодировки Юникод для имён файлов.
- Имеется возможность шифрования архивов (поддерживается 256-бит AES шифрование).
- Помимо шифрования, возможно установить персональный пароль для защиты секретной информации.
- Поддержка плагина для программы Total Commander.
- Поддержка многопоточного сжатия.

7-Zip является замечательной альтернативой широко известному WinRAR. 7-Zip имеет много преимуществ перед платными программами-архиваторами в быстроте и качественной упаковке файлов. Многочисленные тестирования доказывают, что данный архиватор является одним из лидеров по степени сжатия файлов (обеспечивает сжатие на 2–10% лучше, чем PKZip и WinZip), что, несомненно, заслуживает внимания.

Архиватор, будучи хорошо интегрирован с ОС Windows, позволяет создавать новый архив, извлекать файлы из существующего, а также производить другие стандартные операции. Интерфейс программы разработан таким образом, что слева находится так называемая панель папок, где отображена информация о каталогах, содержащихся в архиве, а справа можно изучить содержимое архива, а также открыть или удалить файлы из него. Архиватор поддерживает около 70 различных языков, в том числе и русский.

Удобным и функциональным приложением к архиватору является встроенный файловый менеджер архиватора (рис. 1.14) – это не полноценная программа, а лишь приложение к существующей. Двухпанельный интерфейс менеджера позволяет осуществлять основные операции с файлами: протестировать архив на целостность, получить информацию о заданном файле, а также разбить файлы на части заданного размера. Также, за счет подключения дополнительных модулей, можно увеличить функциональность программы, которая позволяет работать файловому менеджеру с архивами как с обычными папками.

Что касается упаковки файлов, то архиватор поддерживает не только формат 7z, но и другие наиболее распространенные форматы.

Отдельно следует отметить опцию *бенчмарк*, которая встроена в программу 7-Zip. Ее можно использовать для определения времени, которое понадобится системе для выполнения поставленного задания. Чтобы вызвать опцию, достаточно лишь выполнить команду *Сервис – Тестирование производительности*. Опция предлагает два основных теста: компрессия LZMA и декомпрессия с применением того же алгоритма. Также посредством бенчмарк можно оценить производительность компьютера (MIPS – миллион команд в секунду). Оценка производительности и скорость компрессии напрямую зависят от характеристик системы – латентности оперативной памяти. Ускорить процесс сжатия можно, включив опцию «Многопоточность», в этом случае компрессия будет проходить в два потока. Однако опцию невозможно использовать при распаковке архива ввиду того, что «Многопоточность» не оказывает влияние на скорость извлечения файлов и оценку производительности системы.

Работа с архиватором 7-Zip

Открытие архива

Для открытия архива можно дважды щелкнуть по файлу или в контекстном меню файла (рис. 1.15) указать на 7-Zip и выбрать команду *Открыть архив*.

Извлечение файлов из архива

Чтобы извлечь все файлы из архива, нужно в контекстном меню файла (рис. 1.15) или в меню *Файл* указать на *7-Zip* и затем выбрать команду *Распаковать* (можно просто нажать кнопку *Извлечь* (рис. 1.14) на панели инструментов). Появится диалоговое окно *Извлечь* (рис. 1.16). В поле *Распаковать в...* необходимо ввести имя папки вывода или, нажав кнопку «**…**», воспользоваться окном *Обзор папок* для выбора папки, в которую будут распакованы файлы, и нажать *ОК*. В этом же окне в поле *Пути* можно определить режим извлечения: извлекать файлы с полными именами пути или без путей папки, а в поле *Перезапись* следует определить режим замены для файлов, которые уже представлены на диске: *С подтверждением* – перед перезаписью существующих файлов

выдается запрос, *Без подтверждения* – существующие файлы перезаписываются без подсказки, *Пропускать* – пропускается извлечение существующих файлов, *Переименовать автом.* – извлекаемые файлы переименовываются, если файл с таким именем уже существует. Например, файл document.txt будет переименован в document_1.txt., *Переим. автом. существ.* – существующий файл переименовывается, если файл с таким именем уже существует. Здесь же можно ввести пароль для зашифрованных архивов и в конце нажать кнопку *ОК* для извлечения файлов архива.

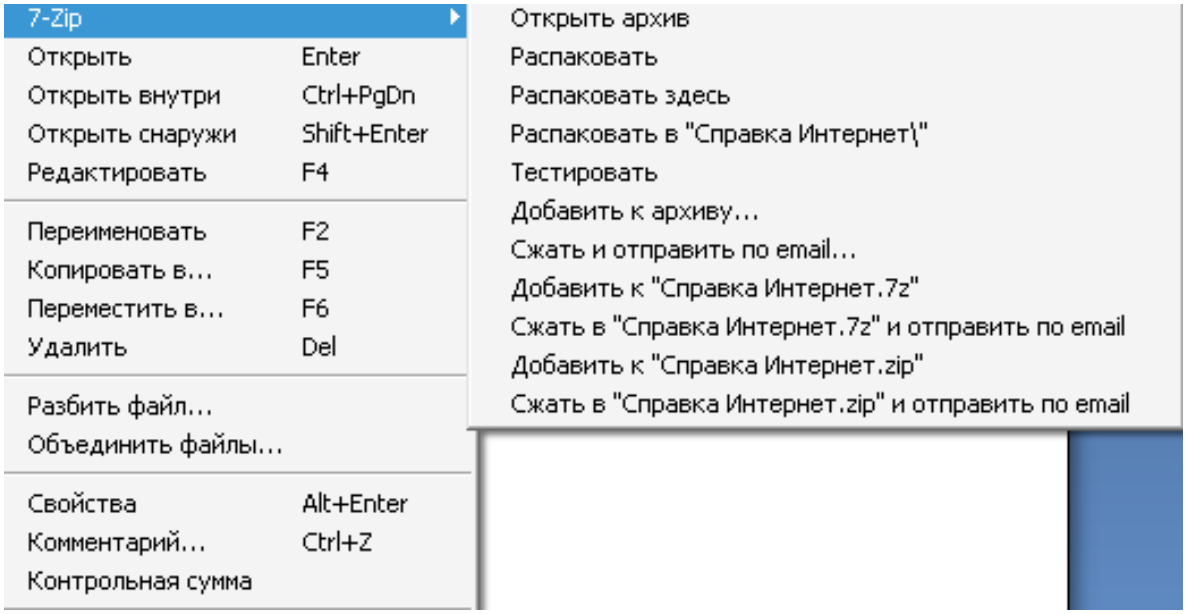


Рис. 1.15. Контекстное меню архивного файла 7-Zip

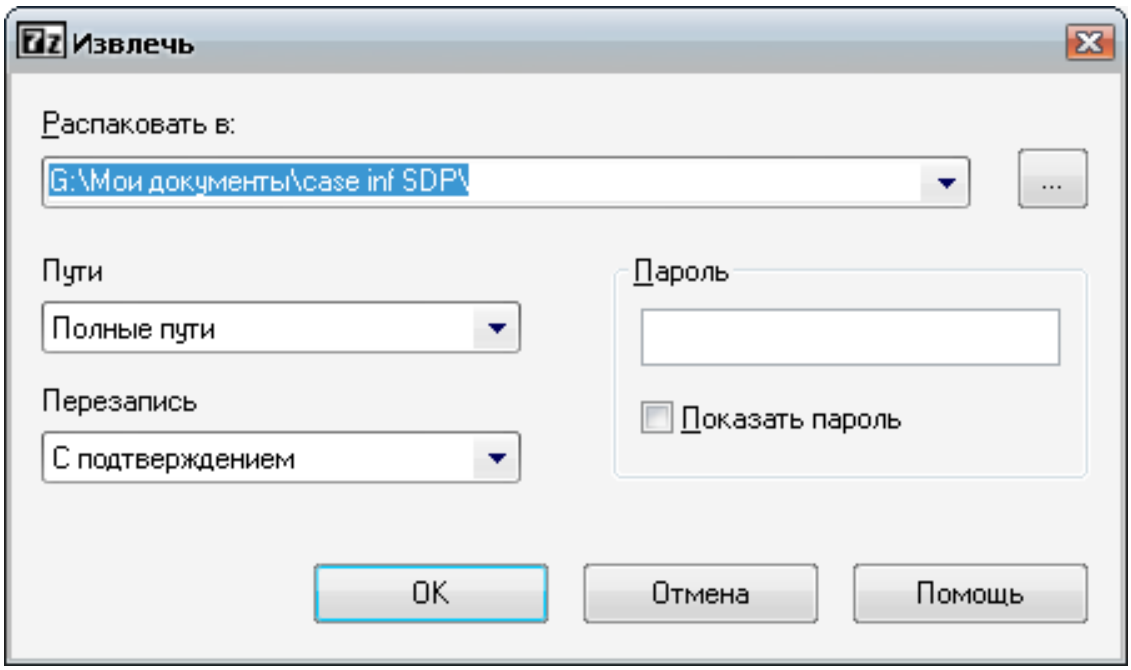


Рис. 1.16. Диалоговое окно *Извлечь* архиватора 7-Zip

Чтобы извлечь определенные файлы из архива, надо открыть архив в *7-Zip*, выбрать пункты для извлечения и выполнить в контекстном меню (рис. 1.15) или в меню *Файл* команду *Копировать в...* (можно просто нажать кнопку *Копировать* (рис. 1.14) на панели инструментов). Появится диалоговое окно *Копировать*. В поле *Копировать в...* необходимо ввести имя папки вывода или, нажав кнопку «**...**», воспользоваться окном *Обзор папок* для выбора папки, в которую будут распакованы файлы, и нажать *ОК*.

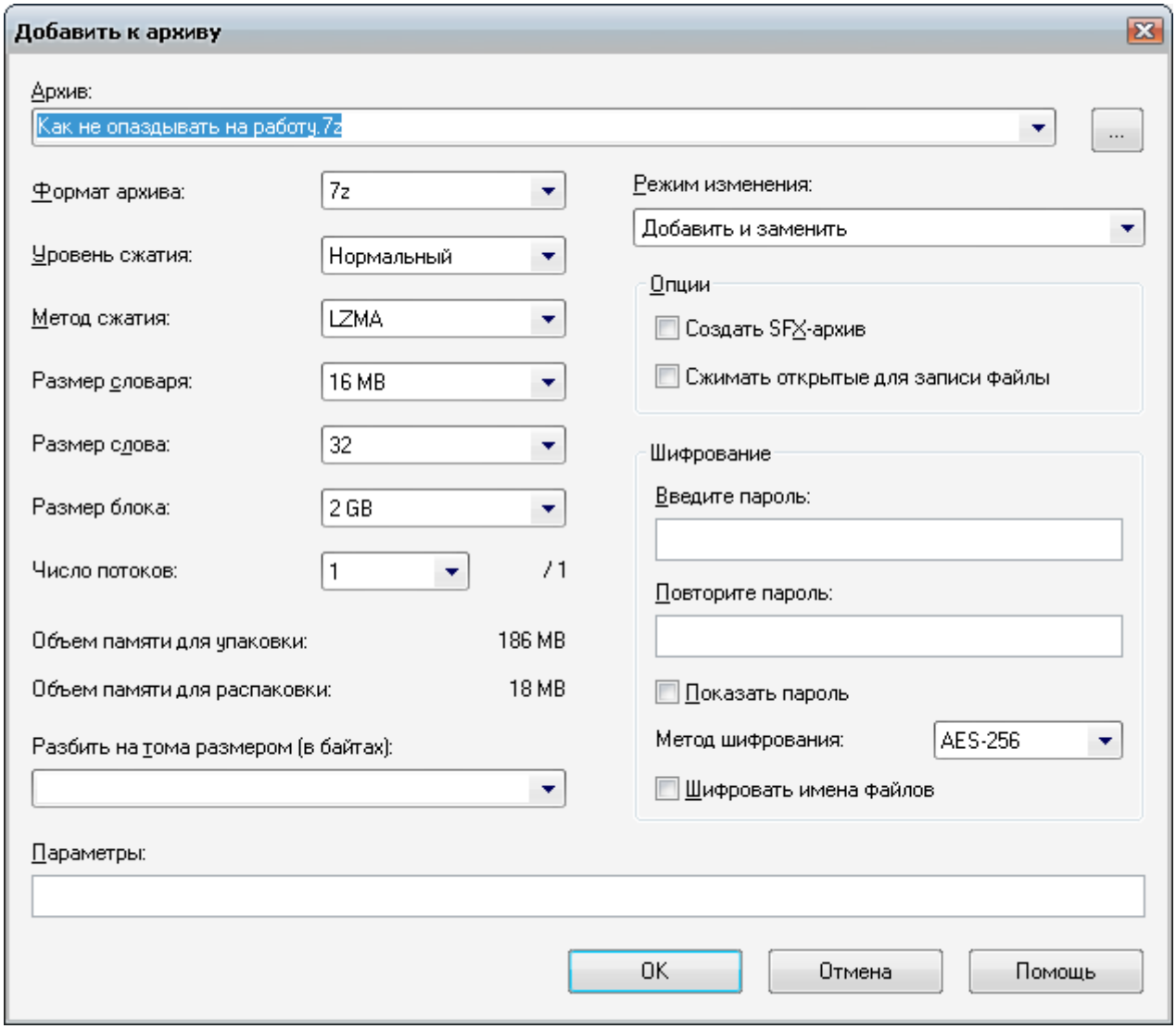


Рис. 1.17. Контекстное диалоговое окно *Добавить к архиву*

Создание и обновление файлов в архиве

Для того, чтобы создать или обновить файл архива, следует в Проводнике ОС или в главном окне 7-Zip в контекстном меню (рис. 1.15) файла (ов) или папки (ок), которую надо сжать, указать на *7-Zip*, и затем выбрать команду *Добавить к архиву*... Появится диалоговое окно *Добавить к архиву* (рис. 1.17), которое позволяет определять опции для создания или обновления архива.

Поле *Архив* обеспечивает место для ввода имени архива. Чтобы определить местонахождение архива, можно щелкнуть кнопкой «**...**», чтобы открыть диалоговое окно *Пролистать*. В поле *Формат архива* нужно определить формат создаваемого архива.

В этом же окне выбирается уровень сжатия. Есть 6 уровней сжатия: *Без сжатия, Скоростной, Быстрый, Нормальный, Максимальный* и *Ультра*. Для каждого формата архива может задать свои собственные методы сжатия.

Далее можно задать *размер словаря* для метода сжатия. Обычно больший размер словаря повышает степень сжатия. Но сжатие может быть медленнее, и это может потребовать большего количества памяти.

Размер слова определяет длину слов, которые будут использоваться, чтобы найти идентичные последовательности байтов для сжатия.

Размер блока определяет размер solid блока. Можно также отключить solid-режим. В solid-режиме все файлы будут сжаты как непрерывные блоки данных. Обычно сжатие в solid-архив улучшает степень сжатия. Эту опцию можно использовать только для 7z архивов. Обновление solid .7z архивов может быть медленным, так как может потребоваться некоторое пересжатие.

Число потоков определяет число потоков для сжатия. Большое число потоков может увеличить скорость сжатия на многопроцессорных системах.

Архиватор 7-Zip позволяет создавать многотомные архивы. Поле *Разбить на тома размером (в байтах)* определяет размеры томов в байтах, килобайтах, Мегабайтах или Гигабайтах по схеме: {Size}[b | k | m | g].

Если определить только {Size}, 7-zip обработает это как байты. Можно определить несколько значений. Например: 10k 15k 2m. В таком случае первый том будет 10 кб, второй будет 15 кб, а все остальные будут по 2 Мб.

В этом же окне (рис. 1.17) в поле *Режим изменения* можно определить режим обновления архива: *Добавить и заменить* – добавляет все указанные файлы в архив, *Обновить и добавить* – обновляет старые файлы в архиве и добавляет новые файлы в архив, *Обновить* – обновляет определенные файлы в архиве, которые старее чем выбранные файлы на диске, *Синхронизировать* – заменяет определенные файлы, только если добавляемые файлы более новые. Всегда добавляет те файлы, которые отсутствуют в архиве. Удаляет из архива те файлы, которые отсутствуют на диске.

Для 7z архивов можно создать *самораспаковывающийся архив*, установив соответствующий флажок (рис. 1.17) *Создать SFX-архив*.

Можно также установить опцию сжатия файлов, открытых для записи другим приложением.

В группе *Шифрование* вводится пароль, а также можно установить опцию *Показать пароль* и выбрать метод шифрования (для 7z формата это может быть только AES-256, а для ZIP формата можно выбрать ZipCrypto или AES-256). Чтобы получить архив, совместимый с большинством ZIP архиваторов, лучше использовать ZipCrypto.

В этой же группе можно включить опцию шифрования заголовка архива, включая шифрование имен файлов.

Тестирование архива

Чтобы проверить архив на целостность и отсутствие ошибок, надо в контекстном меню файла архива (рис. 1.15) указать на *7-Zip* и затем выбрать команду *Тестировать* (либо просто нажать кнопку *Тестировать* (рис. 1.14) на панели инструментов).

Архиватор IZArc

Архиватор IZArc (разработчик Иван Захарьев) распространяется бесплатно, но по полноте предлагаемых функций он легко может соперничать с коммерческими продуктами аналогичного назначения. Это надежная, удобная и очень популярная программа для полноценной работы с различными типами данных. Программа работает под управлением ОС Windows 2000/ XP/Vista/7. Архиватор отличается простым и вместе с тем удобным и функциональным интерфейсом (рис. 1.18), он не перегружен мелочами и прочими деталями, которые могут помешать отлаженной и быстрой работе с данными, файлами и приложениями. IZArc поддерживает множество языков, в том числе и русский.

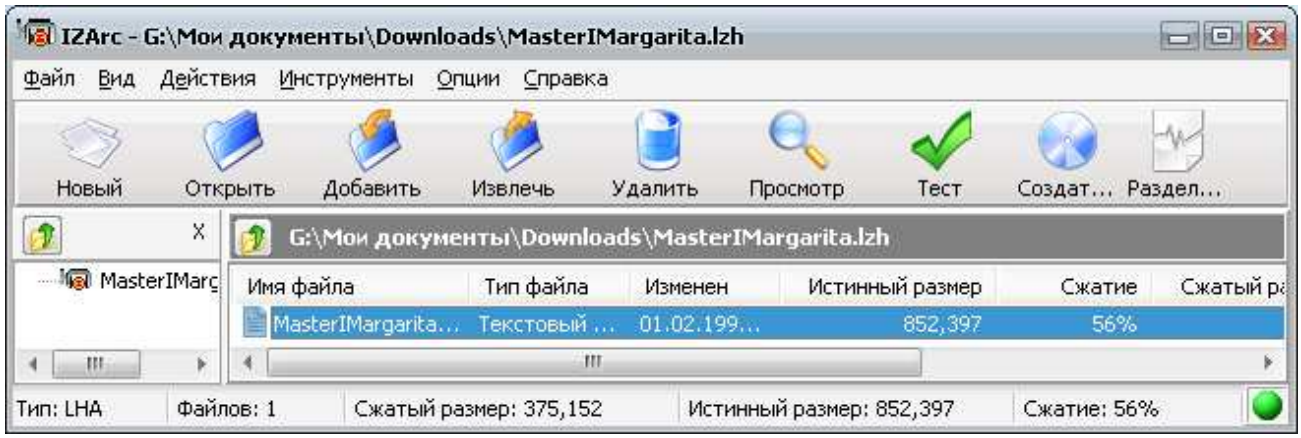


Рис. 1.18. Основное окно архиватора IZArc

Основные возможности и особенности архиватора

IZArc имеет все необходимые функции для работы с архивами: предусмотрено создание новых архивов, просмотр, распаковка и пополнение существующих, доступ к отдельным файлам внутри архива для просмотра и удаления. Реализовано создание самораспаковывающихся и многотомных архивов. Полностью поддерживается технология перетаскивания мышкой (Drag & Drop). Кроме того, можно проверять и восстанавливать поврежденные архивы в формате ZIP, вести поиск внутри архивов, защищать архивы при помощи пароля и отправлять их по электронной почте. Будучи полностью интегрированной с ан-

тивирусными программами и в контекстное меню Windows, программа поддерживает возможность встраивания различных команд в меню Проводника, благодаря чему архиватор очень удобен для работы с различными типами данных.

Архиватор IZArc поддерживает (в том числе читает, распаковывает, конвертирует, исправляет и т.д.) самые разнообразные форматы архивов, такие как: 7-ZIP, A, ACE, ARC, ARJ, B64, BH, BZ2, BZA, CAB, CDI, CPIO, DEB, ENC, GCA, GZ, GZA, HA, JAR, LHA, LIB, LZH, MBF, MIM, PAK, PK3, RAR, RPM, TAR, TAZ, TBZ, TGZ, TZ, UUE, WAR, XXE, YZ1, Z, ZIP, ZOO. Более того, архиватор может конвертировать архивы из одного формата в другой. Помимо этого, IZArc может читать и конвертировать основные форматы образов дисков (CD/DVD), таких как: ISO, BIN, MDF, NRG, IMG, C_2D, PDI, CDI, а также перекодировать их.

Для безопасной работы и сохранности данных архиватор IZArc поддерживает режим автоматической проверки данных на вирусы и шпионские программы. Также программа характеризуется возможностью зашифровать данные архива с применением мощного алгоритма, тем самым преобразовывая открытую информацию в закрытую.

Работа с архиватором IZArc

Открытие архива

Выполнение многих операций начинается в основном окне IZArc (рис. 1.18). Его можно открыть через меню Пуск, щелкнув по значку 

. Оно появляется также автоматически после двойного щелчка по архивному файлу в программах Проводник или Мой компьютер. Настраиваемая панель инструментов обеспечивает быстрый доступ к наиболее часто используемым действиям. В основном окне IZArc показывается список с именами и размерами всех файлов открытого архива. Этот список можно прокручивать и сортировать по любому полю.

Для открытия архива можно просто перетащить архивный файл на значок IZArc, а также, щелкнув по значку *Открыть* в основном окне IZArc или в меню *Файл* (рис. 1.19), выбрать команду *Открыть архив* и далее использовать открывающееся диалоговое окно *Открыть существующий архив*. В этом окне следует выбрать нужный архив и нажать кнопку OK.

Извлечение файлов из архива

При извлечении файла IZArc распаковывает его и помещает в выбранную папку. Можно восстанавливать целые папки, сохраняя структуру вложенных папок. Чтобы вывести на экран диалоговое окно *Извлечь файлы* (рис. 1.20), надо в основном окне архиватора нажать кнопку *Извлечь* на панели инструментов (рис. 1.18) или выбрать в меню *Действие* (рис. 1.21) команду *Извлечь*....

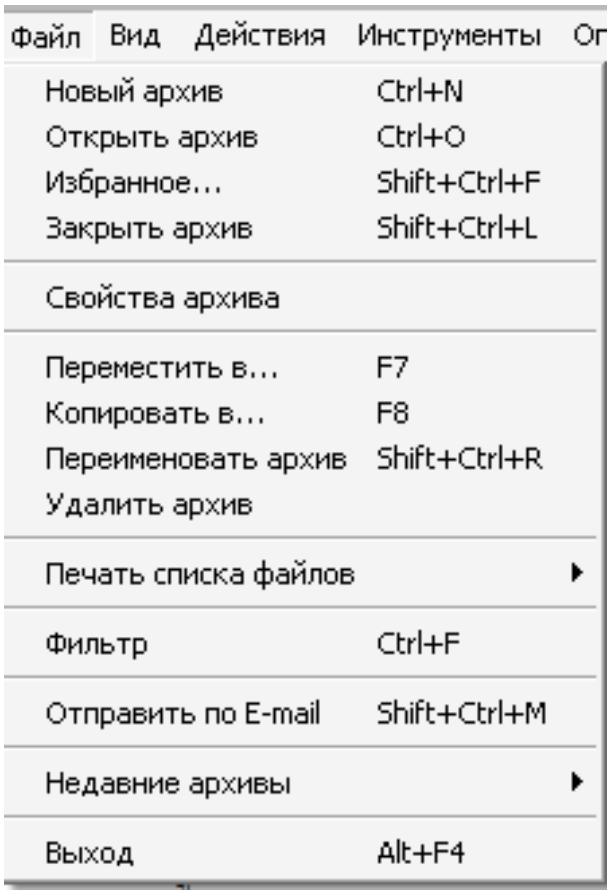


Рис. 1.19. Меню *Файл* основного окна архиватора IZArc

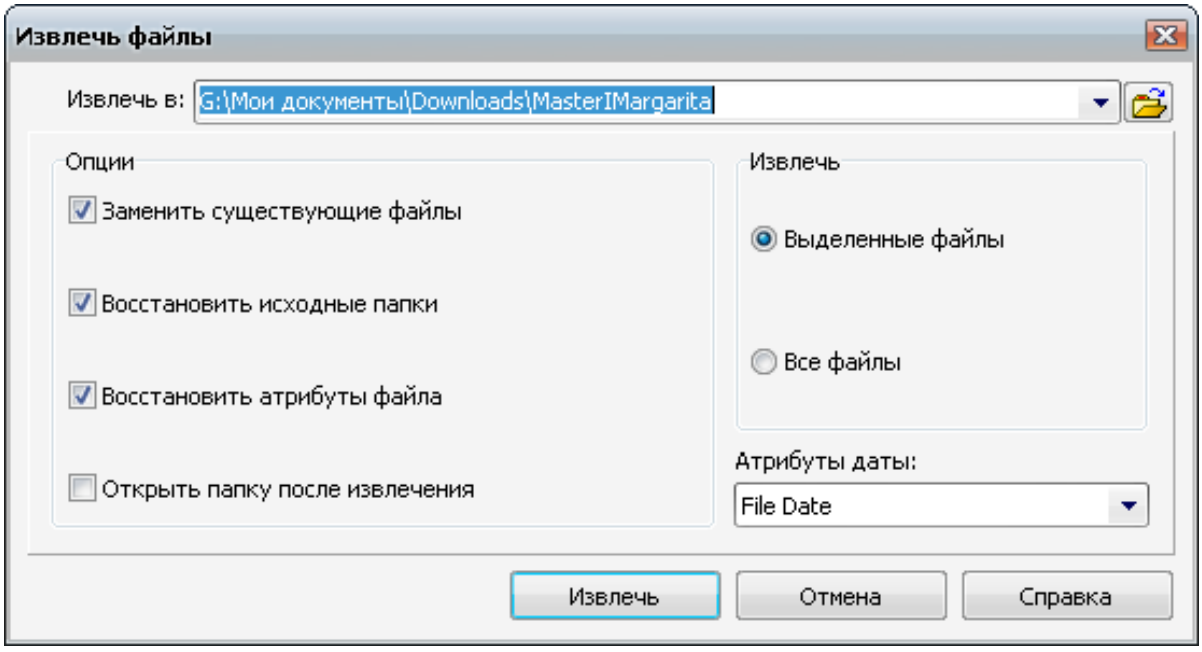


Рис. 1.20. Диалоговое окно *Извлечь файлы* архиватора IZArc

Еще проще – в контекстном меню архивного файла (рис. 1.22) указать на IZArc и выбрать одну из команд: *Извлечь в…* либо *Извлечь в текущую папку* или *Извлечь в* .\ имя архива. Другой способ извлечения файлов – перетаскивание файлов из окна IZArc прямо на рабочий стол или в любую папку в Проводнике Windows либо в другом файловом менеджере.

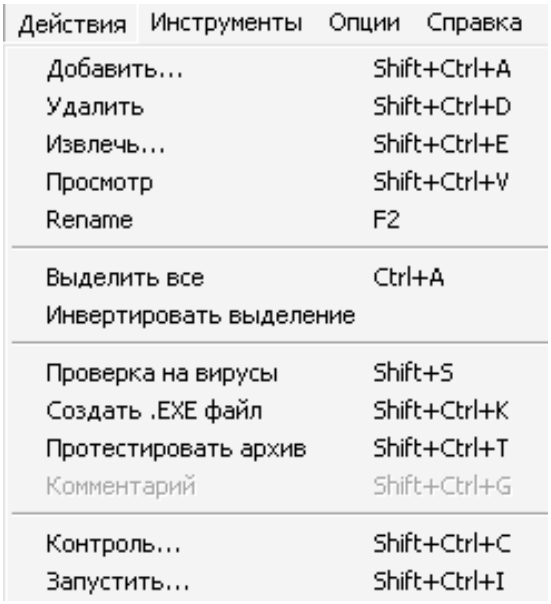


Рис. 1.21. Меню *Действие* основного окна архиватора IZArc

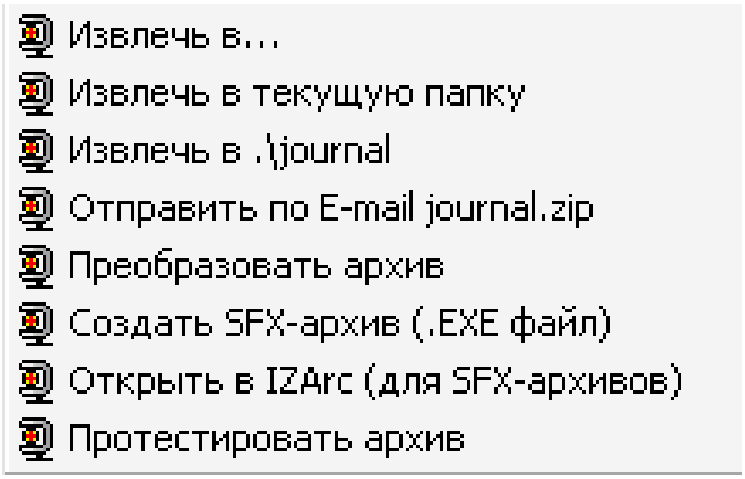


Рис. 1.22. Контекстное меню архивного файла IZArc

IZArc извлечет файлы из архива в папку, указанную в поле *Извлечь в:* (рис. 1.20). В это поле можно оставить предлагаемую папку, имя которой совпадает с именем архива, или ввести другое имя папки вывода. Другой способ – нажав кнопку справа от указанного поля, можно воспользоваться открывающимся окном *Обзор папок* для выбора папки, в которую будут распакованы

файлы, и затем нажать *ОК*. При этом в окне *Обзор папок*, нажав на кнопку *Создать папку*, можно создать новую папку.

Следует заметить, что в диалоговом окне *Извлечь файлы* (рис. 1.20), в группе *Извлечь*, можно выбрать способ распаковки: *Все файлы* или только *Выделенные файлы* в основном окне IZArc. В другой группе нужно указать *Опции*: *Заменить существующие файлы*, *Восстановить исходные папки*, *Восстановить атрибуты файла* и *Открыть папку после извлечения*. В этом же окне при необходимости задаются *Атрибуты даты*.

Создание нового архива и добавление файлов в архив

Для создания нового архива можно использовать любой из перечисленных способов: выбрать *Новый архив* в меню *Файл* (рис. 1.19), щелкнуть по кнопке *Новый* на панели инструментов (рис. 1.18) или нажать кнопки *Ctrl+N*.

Откроется диалоговое окно *Создать новый архив* (рис. 1.23), которое работает так же, как обычные диалоговые окна в Windows.

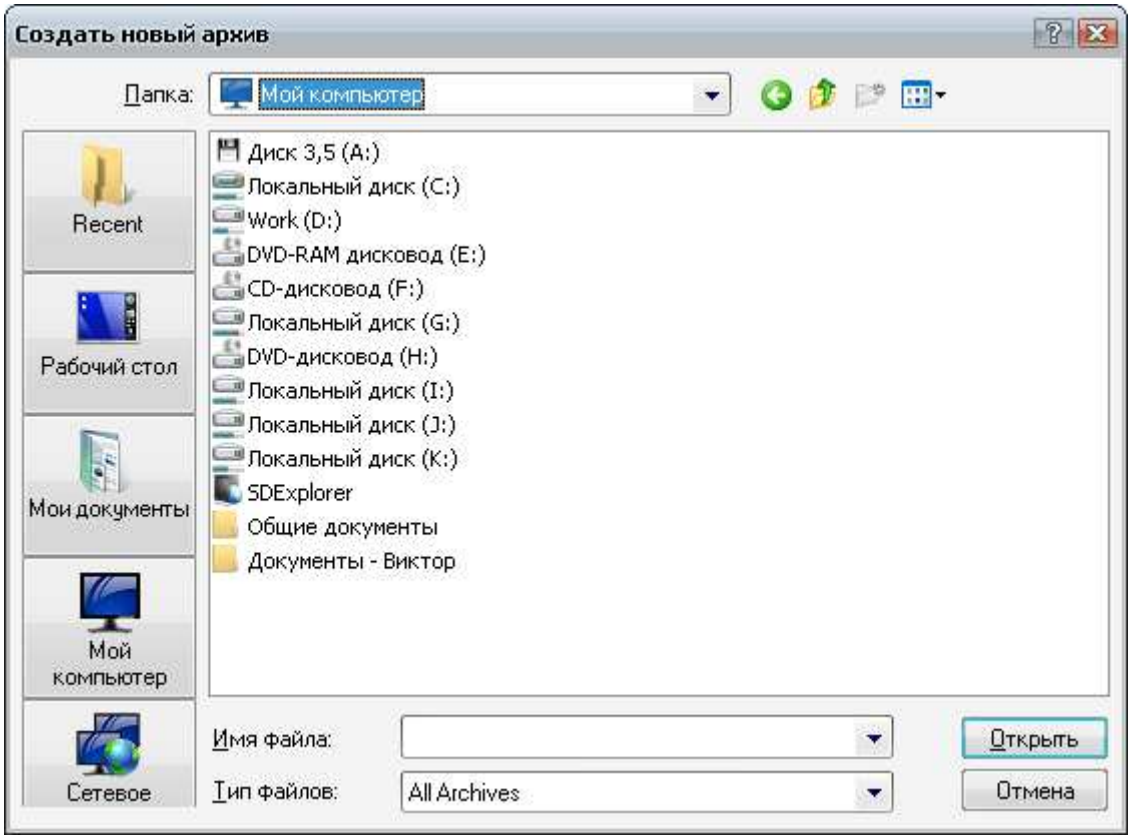


Рис. 1.23. Диалоговое окно *Создать новый архив*

Здесь нужно выбрать диск и папку, куда будет создан архив, либо создать новую папку, затем набрать название создаваемого архива *Имя файла* (но не названия архивируемых файлов) и нажать кнопку *Открыть*. Чтобы легче было выбрать название, которого еще не существует, видны имена уже имеющихся в папке архивов. Если выбрать имя существующего архива, IZArc спросит, хоти-

те ли вы перезаписать его. Обычно после создания архива в него сразу же добавляют файлы, поэтому автоматически откроется диалоговое окно *Добавить файлы в архив* (рис. 1.24), где нужно на вкладке *Selection* выбрать все файлы и папки для добавления в новый архив. В этом же диалоговом окне (рис. 1.25) на вкладке *Опции (Options)* можно выбрать *степень сжатия* (максимальный, обычный, быстрый или очень быстрый), выбрать *тип архивации*, выбрать *Действие*: *Добавить* и можно установить пароль на архив, выбрав предварительно *тип шифрования*.

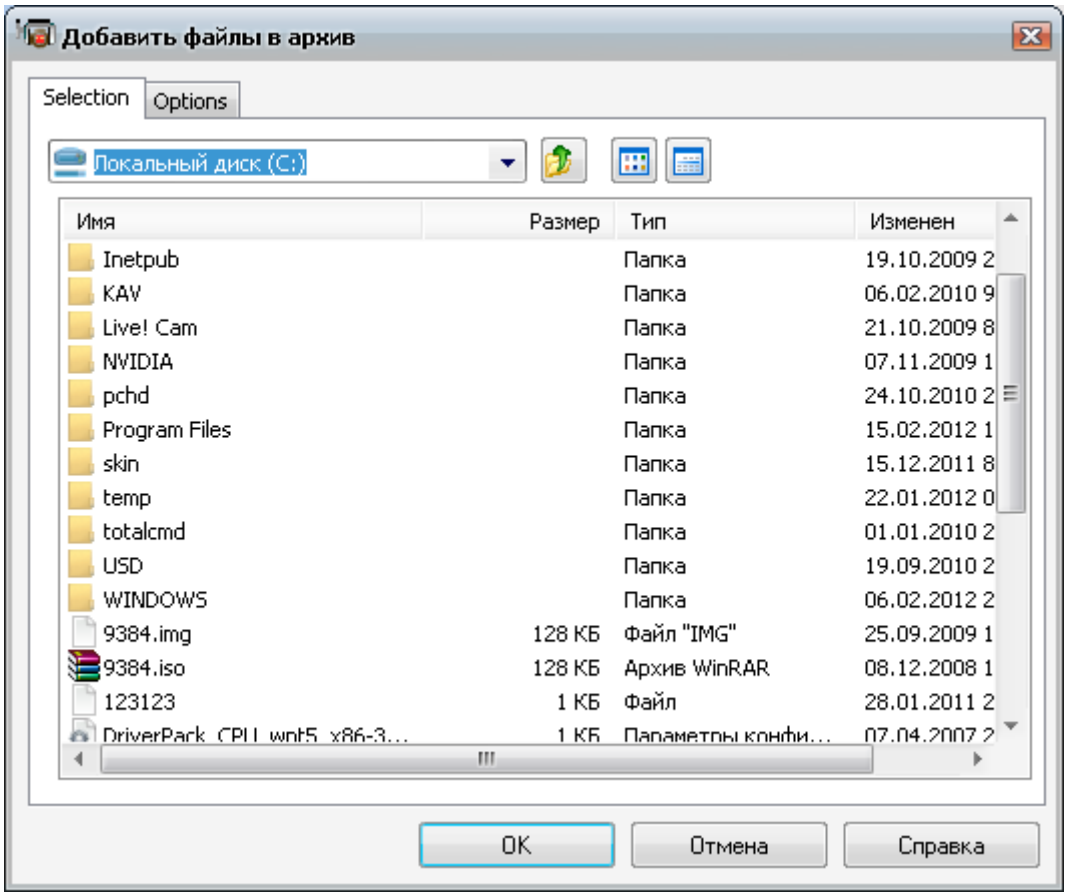


Рис. 1.24. Диалоговое окно *Добавить файлы в архив* (вкладка *Selection*)

После нажатия на кнопку ОК начинается процедура сжатия. Если нужно отменить процесс добавления, можно просто нажать на красный свет в правом нижнем углу приложения.

Чтобы добавить файлы в существующий архив, нужно выбрать *Добавить* в меню *Действие* (рис. 1.21) или нажать на кнопку *Добавить* на панели инструментов основного окна архиватора (рис. 1.18). В открывшемся окне (рис. 1.25), на вкладке *Опции (Options)* в поле *Действие* предлагается три варианта добавления файлов в архив:

- *Добавить* – IZArc копирует указанные файлы в архив, оставляя их в своей папке (т.е. получаются две копии для каждого файла – исходная и упакованная).
- *Обновить* – IZArc обновляет уже имеющиеся в архиве файлы на их более новые варианты (сравниваются время и даты создания файлов).
- *Переместить* – IZArc работает аналогично *Добавить*, но после добавления файлов в архив их исходные копии удаляются с диска.

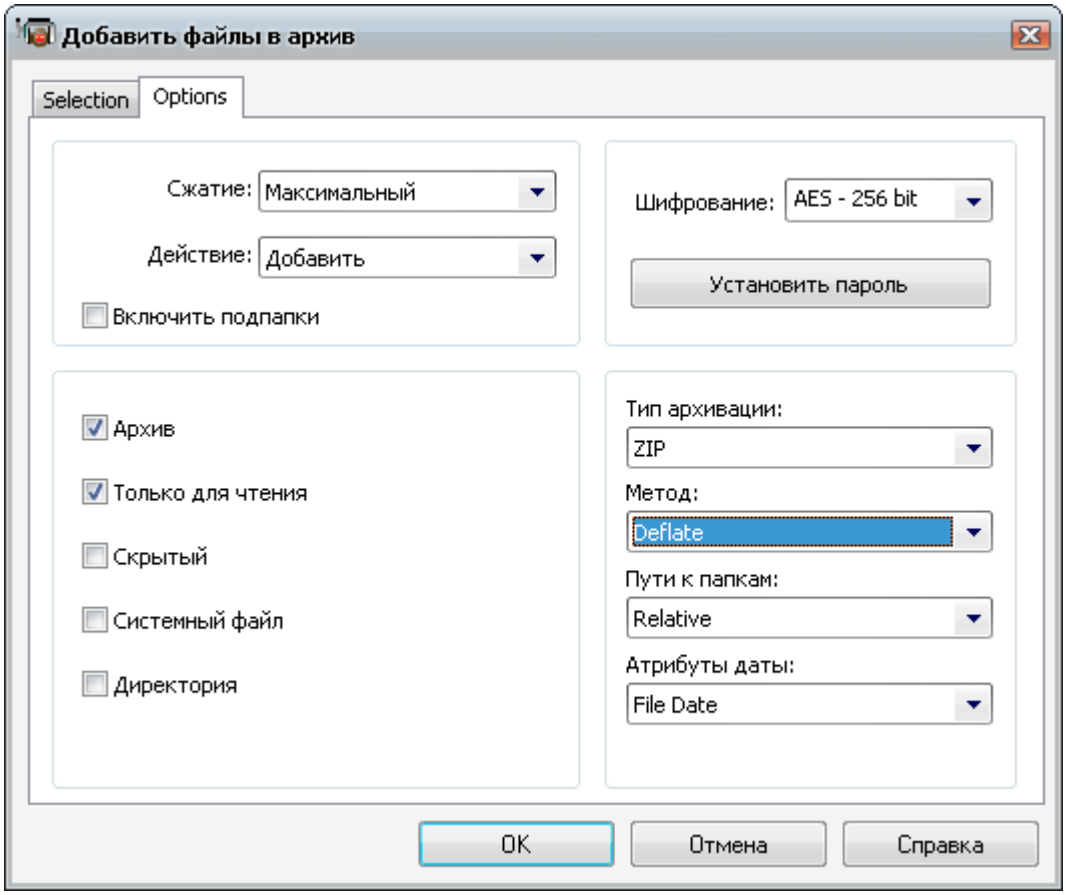


Рис. 1.25. Вкладка *Options* окна *Добавить файлы в архив*

В поле *Метод* можно определить алгоритм сжатия. Поле *Пути к папкам* позволяет выбрать способ хранения информации о пути к файлам.

Другой способ добавления файлов в архив – в окно любого открытого в IZArc архива перетащить выделенные файлы непосредственно с рабочего стола или из файлового менеджера.

Удаление файлов архива

Для удаления файлов из архива нужно в окне открытого архива выбрать их имена в списке файлов, а затем команду *Удалить* в меню *Действия* (рис. 1.21) или нажать кнопку *Удалить* на панели инструментов основного окна архиватора (рис. 1.18). Внимание! Эту операцию отменить нельзя !!!

Чтобы удалить целый архив, в окне открытого архива нужно выбрать в меню *Файл* команду *Удалить архив* (рис. 1.19). Другой вариант – команда *Удалить* в контекстном меню архивного файла.

Просмотр файла без извлечения из архива

Просмотреть файлы в архиве можно несколькими способами. Большинство файлов можно просмотреть, дважды щелкнув по названию в основном окне IZArc. Если это исполняемый файл (имеет расширение EXE, COM, BAT или PIF), IZArc запустит его. Другие файлы откроются в соответствующем приложении. Например, файлы с расширением .txt откроются в приложении Блокнот, с расширением .doc – в окне Word.

Другой способ просмотреть файлы – при помощи кнопки *Просмотр* на панели инструментов (рис. 1.18) или команды *Просмотр* из меню *Действия* (рис. 1.21). В обоих случаях вызывается диалоговое окно *Просмотр файлов* (рис. 1.26), которое дает возможность просмотреть выбранные файлы одним из указанных пользователем способов.

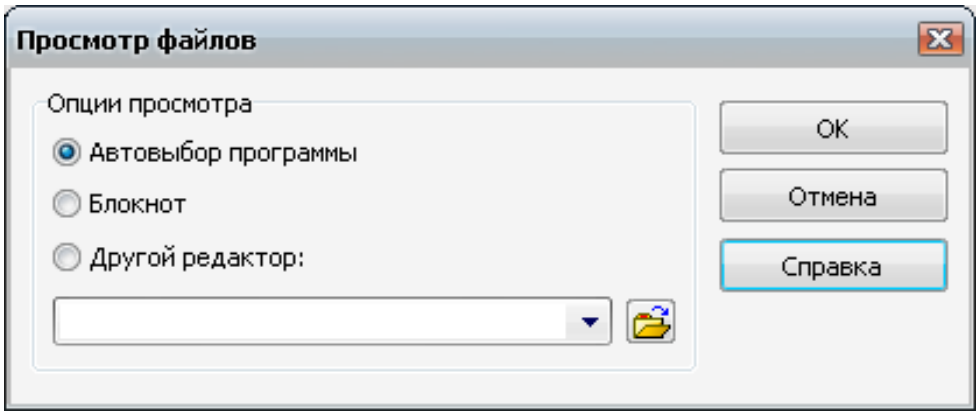


Рис. 1.26. Окно *Просмотр файлов*

Создание самораспаковывающегося архива

В IZArc можно создать самораспаковывающиеся архивы (SFX) из 7-ZIP, ACE, ARJ, BH, JAR, LHA, LZH, RAR и ZIP архивов.

Создание самораспаковывающегося архива состоит из двух этапов. На первом этапе создается обычный архив (файл с расширением, например, .zip) или открывается существующий архив в окне архиватора. Затем создается самораспаковывающейся архив (файл с расширением .exe). Для этого в меню *Действия* (рис. 1.21) нужно выбрать *Создать .EXE файл* или нажать кнопку *Создать EXE* на панели инструментов (рис. 1.18) либо в контекстном меню IZArc (рис. 1.22) выбрать *Создать .SFX архив* (*.EXE файл*). Отрывается диалоговое окно *Создать самораспаковывающиеся архив* (рис. 1.27).

В этом окне нужно указать папку, в которую будут размещены извлеченные файлы. Если ничего не указать, будет использоваться по умолчанию теку-

щая директория пользователя. Далее можно отметить и другие опции, и нажать кнопку *ОК*. Будет создан самораспаковывающейся архив с расширением .exe.

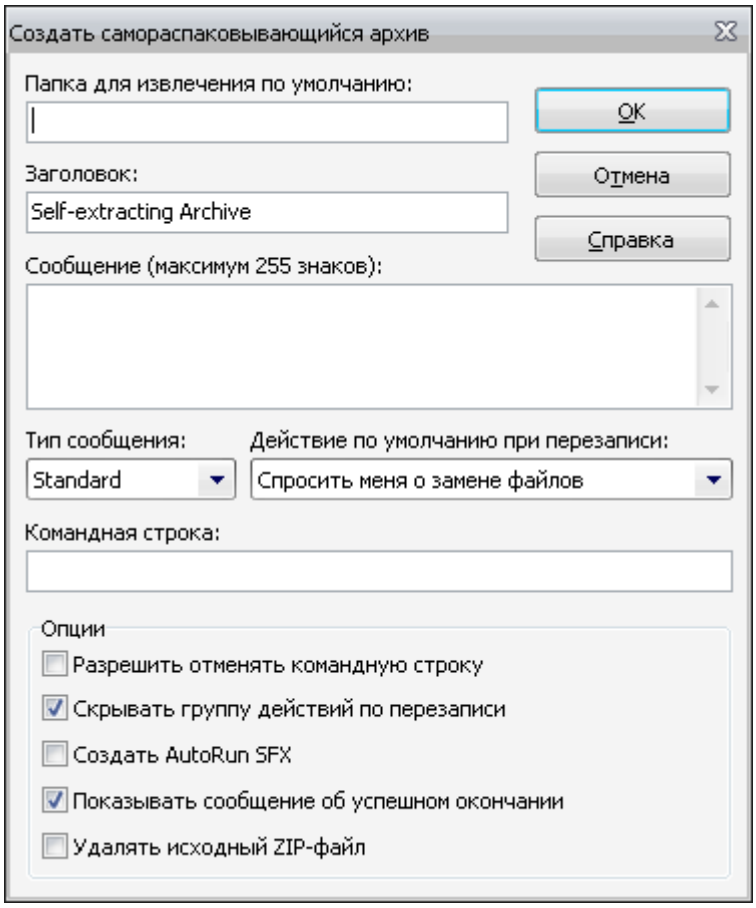


Рис. 1.27. Окно *Создать самораспаковывающийся архив*

Разделение архива на части

IZArc позволяет легко создавать IZArc-файлы, которые делятся на несколько томов – многотомные архивы. Во-первых, надо создать новый архив или открыть существующий, а затем разделить его. Для этого в основном окне IZArc (рис. 1.18) в меню *Инструменты* (рис. 1.28) необходимо выбрать *Разделить архив на части* либо нажать на кнопку *Разделить* на панели инструментов (рис. 1.18). Откроется окно *Разделить архив на части* (рис. 1.29). Здесь надо задать *Имя цельного архива* (выделить архив можно, нажав кнопку *Открыть*). Далее нужно ввести *Имя разделенного архива* и указать папку, куда необходимо поместить разделенный архив. Затем можно указать размер тома и нажать ОК.

Шифрование файлов

Чтобы зашифровать файл или архив, необходимо выбрать в меню *Инструменты* (рис. 1.28) команду *Зашифровать архив*, далее в открывшемся окне (рис. 1.30) указать *Обычный файл* и *Зашифрованный файл*, нажать клавишу *Шифровать* и ввести пароль в окне *Служба безопасности*.

Рис. 1.28. Окно меню *Инструменты* окна архиватора IZArc

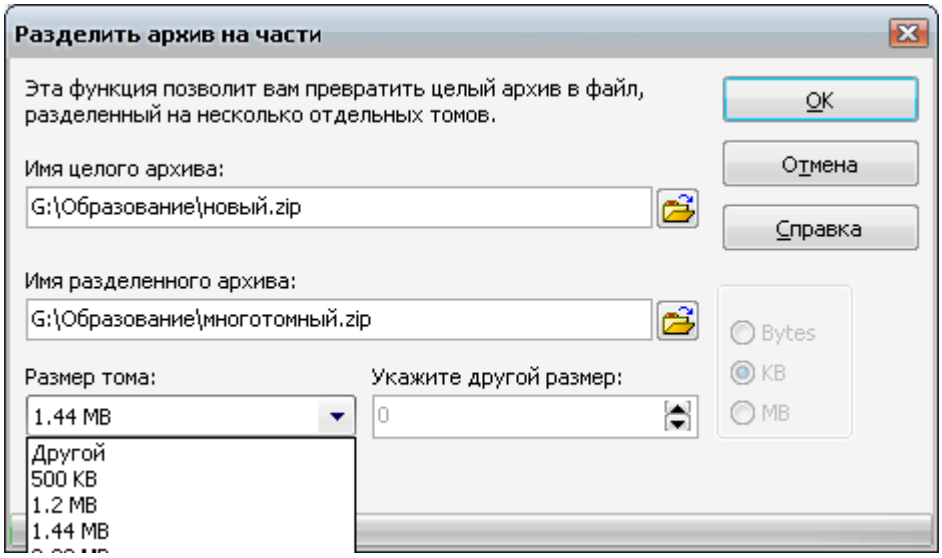


Рис. 1.29. Окно *Разделить архив на части*

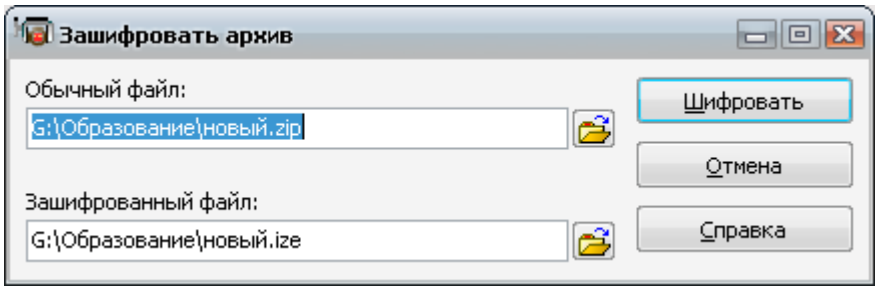


Рис. 1.30. Окно *Зашифровать архив*

Вопросы для самоконтроля

1. Какие проблемы возникают при интенсивной работе с данными на компьютере?
2. Что такое сжатие информации и для чего оно нужно?
3. Каковы цели упаковки файлов?
4. Что такое архивный файл?
5. Приведите пример расширения архивных файлов.
6. Дайте определения понятий *Архивация (упаковка)* и *Разархивация (распаковка).*
7. Что такое коэффициент сжатия*?*
8. Что такое *самораспаковывающийся* архивный файл, какое расширение он имеет?
9. Что такое *многотомный* архив, для чего он нужен?
10. Перечислите наиболее популярные лицензионные программы-архиваторы.
11. Перечислите наиболее популярные бесплатные архиваторы.
12. Дайте сравнительную характеристику архивам WinRAR и WinZIP.
13. Каковы основные особенности архиватора WinRAR?
14. В чем заключается эффективность метода сжатия solid (непрерывный архив) архиватора WinRAR?
15. Сравните *режим управления файлами* и *режим управления архивами* архиватора WinRAR.
16. Поясните порядок действий при архивации данных в архиваторе WinRAR.
17. Поясните, как архивировать данные в окне *Проводник* или *Мой компьютер*.
18. Поясните, как извлечь файлы в программах *Проводник* и *Мой компьютер*.

19. Поясните порядок действий при извлечении файлов в оболочке WinRAR.
20. Поясните порядок действий при удалении файлов из архива в оболочке WinRAR.
21. Поясните последовательность действий для архивирования файлов в архиваторе WinZip.
22. Поясните последовательность действий для выбора и добавления в архив файлов в программе WinZip.
23. Поясните различие 4-х вариантов добавления файлов в архив в программе WinZip: *Добавить (и заменить) файлы; Обновить существующие файлы; Переместить (и заменить) файлы; Обновить (и добавить) файлы*.
24. Поясните способы открытия существующего архива в программе WinZip.
25. Поясните последовательность действий при извлечении файлов из открытого архива в программе WinZip.
26. Поясните способы просмотра файлов без извлечения из архива в программе WinZip.
27. Поясните последовательность действий при создании самораспаковывающегося архива.
28. Поясните отличия и особенности создания многотомных архивов в программах WinZip и WinRAR.
29. Проведите сравнительный анализ возможностей архиваторов WinZip и IZArc, WinRAR и 7-Zip.
30. Поясните, что означает и как осуществить шифрование имен файлов.

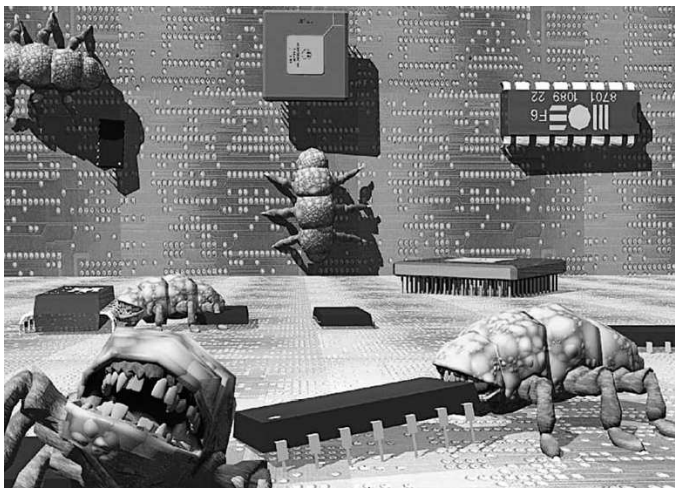
ГЛАВА 2. КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Массовое применение ПК, к сожалению, оказалось связанным с появлением *компьютерных вирусов*. В наше время возросло количество преступлений, направленных против информационной безопасности. Риску подвергаются не только крупные компании, но и частные пользователи. Преступники получают с помощью различных средств доступ к персональным данным – номерам банковских счетов, кредитных карт, паролям, выводят систему из строя или получают полный доступ к компьютеру. В дальнейшем такой ПК используется злоумышленниками для проведения атак, рассылки спама, сбора конфиденциальной информации, распространения новых вредоносных программ.

Ущерб от проникновения вируса в домашний компьютер может быть совершенно разным: от незначительного увеличения размера исходящего трафика (если внедрена программа-троян, рассылающая спам) до полного отказа работы или потери жизненно важной информации. Поэтому безопасность компьютера является первоочередной задачей каждого пользователя.

2.1. Характеристика компьютерных вирусов

Общие сведения



Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Компьютерные вирусы – это программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере: создавать или удалять объекты, модифицировать файлы данных или программные файлы, осуществлять действия по собственному распространению по локальным вычислительным сетям или по сети Интернет, создавать всевозможные помехи в работе на компьютере.

Важнейшей функцией компьютерных вирусов является *заражение* (*инфицирование*) – модификация программных файлов, файлов данных или загрузочных секторов дисков таким образом, что последние сами становятся носителями вирусного кода и, в свою очередь, могут осуществлять вышеперечисленные операции.

Самый главный вопрос: кому это нужно? Почему компьютеры, сети, мобильные телефоны стали носителями не только полезной информации, но зоной обитания разнообразных вредных программ? Как только появляется возможность использования чего-либо в хулиганских, мошеннических, вымогательских или иных преступных целях – обязательно появляются те, кто применяет новые технологии совсем не так, как было задумано изобретателями этих технологий, а совсем наоборот – в корыстных целях или в целях личного самоутверждения, во вред всем окружающим. Причины этого, с одной стороны, скрываются в психологии человеческой личности и ее теневых сторонах (зависти, мести, тщеславии непризнанных творцов, невозможности конструктивно применить свои способности), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

Создателей вредоносных программ подразделяют на следующие категории:

- компьютерные хулиганы;
- мелкие воришки;
- криминальные бизнесмены;
- полулегальные бизнесмены.

Компьютерное хулиганство

Первая группа компьютерных хулиганов состоит из студентов и школьников, которые писали и пишут вирусы по сей день только для самоутверждения их авторов. Они недавно изучили язык программирования и хотят попробовать свои силы, но не могут найти для них более достойного применения. Значительная часть подобных вирусов их авторами не распространяется, и вирусы через некоторое время умирают сами вместе с дисками, на которых хранились.

Вторую группу создателей вирусов также составляют молодые люди (чаще – студенты), которые еще не полностью овладели искусством программирования. Единственная причина, толкающая их на написание так называемых «студенческих», крайне примитивных и с большим числом ошибок вирусов, это комплекс неполноценности, который компенсируется компьютерным хулиганством.

Многие из вирусописателей, приобретая опыт, попадают в *третью*, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие виру-

сы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

Отдельно стоит *четвертая группа* авторов вирусов — «исследователи», довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Они же придумывают способы внедрения в новые операционные системы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради исследования потенциалов «компьютерной фауны». Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию вирусов. При этом опасность, исходящая от таких «исследовательских» вирусов, тоже весьма велика — попав в руки «профессионалов» из предыдущей группы, эти идеи очень быстро появляются в новых вирусах.

«Хулиганские» вирусы в последние годы становятся все менее и менее актуальными — за исключением тех случаев, когда такие вредоносные программы вызывают глобальные сетевые и почтовые эпидемии. Причин, по которым школьники и студенты утратили интерес к вирусописательству, может быть несколько: создавать вирусные программы для все более сложной операционной системы Windows стало труднее, в законодательствах многих стран появились специальные компьютерные статьи, а аресты вирусописателей широко освещались прессой. Зато у них появился новый способ проявить себя – в сетевых играх.

На текущий момент доля «традиционных» хулиганских вирусов занимает не более 5% в антивирусных базах данных.

Мелкое воровство

С появлением и популяризацией платных интернет-сервисов (почта, веб, хостинг) компьютерный андеграунд начинает проявлять повышенный интерес к получению доступа в сеть за чужой счет, т.е. посредством кражи чьего-либо логина и пароля (или нескольких логинов и паролей с различных пораженных компьютеров) путем применения специально разработанных программ.

Программы данного типа обычно создаются молодыми людьми, у которых нет средств для оплаты интернет-услуг. Характерен тот факт, что по мере удешевления интернет-сервисов уменьшается и удельное количество таких троянских программ. Но до сих пор троянцы, ворующие пароли, коды доступа к сервисам, составляют заметную часть ежедневных «поступлений» в лаборатории антивирусных компаний всего мира.

«Мелкими воришками» также создаются программы других типов: ворующие регистрационные данные и ключевые файлы различных программных продуктов, использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т.п.

В последние годы фиксируется постоянно увеличивающееся число программ, ворующих персональную информацию из сетевых игр с целью её несанкционированного использования или перепродажи.

Криминальный бизнес

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно создают вредоносные программы в корыстных целях. Для этого они создают программы, которые воруют коды доступа к банковским счетам, навязчиво рекламируют какие-либо товары или услуги, несанкционированно используют ресурсы зараженного компьютера. Диапазон деятельности данной категории граждан весьма широк. Ниже перечислены основные виды криминального бизнеса в сети:

- обслуживание спам-бизнеса;
- распределённые сетевые атаки;
- создание сетей «зомби-машин» – специализированных программ «боты» (от «robot»), которые централизованно управляются удалённым «хозяином»;
- звонки на платные телефонные номера или посылка платных SMS-сообщений;
- воровство интернет-денег;
- воровство банковской информации;
- воровство прочей конфиденциальной информации;
- кибер-шантаж;
- разработка «средств доставки» программ криминальной деятельности;
- точечные атаки;
- прочие виды криминальной деятельности (например, воровство (сбор) обнаруженных на заражённых машинах электронных почтовых адресов и продажа их спамерам).

Как видно, только перечисление видов криминального бизнеса уже впечетляет.

Полулегальный бизнес

Помимо студентов-вирусописателей и откровенно криминального бизнеса, в Интернете существует также деятельность на грани закона – бизнес «полулегальный». Системы навязывания электронной рекламы, утилиты, периодически предлагающие пользователю посетить те или иные платные веб-ресурсы, прочие типы нежелательного программного обеспечения – все они также требуют технической поддержки со стороны программистов-хакеров. Данная поддержка требуется для реализации механизмов скрытного внедрения в систему, периодического обновления своих компонент, разнообразной маскировки (чтобы защитить себя от удаления из системы), противодействия антивирусным

программам — перечисленные задачи практически совпадают с функционалом троянских программ различных типов. Поэтому создаются и распространяются программы принудительной рекламы (adware), ложные антишпионские (anti-spyware) или антивирусные утилиты и проч.

Признаки проявления вирусов

При заражении компьютера вирусом очень важно своевременно его обнаружить. Понять, заражен компьютер или нет, не всегда легко. Авторы современных вирусов, червей и троянских программ прилагают значительные усилия, чтобы скрыть присутствие вредоносного кода в системе. Для этого следует знать основные признаки проявления вирусов, первыми из которых являются:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка дисковода;
- самопроизвольный запуск на компьютере каких-либо программ;
- самопроизвольные попытки компьютера выйти в Интернет;
- неожиданное увеличение исходящего интернет-трафика;
- получение множества системных сообщений об ошибке.

Кроме того, есть некоторые характерные признаки вируса, заражающего компьютеры через электронную почту:

- друзья и знакомые сообщают о письмах от вас, хотя вы им ничего не отправляли;
- в почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Есть также косвенные признаки наличия вируса в компьютере:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке), хотя не запускались никакие программы;
- браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть);

- зафиксированы случаи несанкционированного доступа к личному банковскому счёту или факты использования кредитной карты (косвенный признак) и т. д.

Перечислить все характерные признаки заражения сложно, потому что одни и те же симптомы могут быть вызваны как воздействием вредоносного ПО, так и иными программными или аппаратными проблемами. Таким образом, вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин, например, сбоем в аппаратном или программном обеспечении. Вообще правильная диагностика состояния компьютера нередко затруднена. Однако приведенные симптомы могут быть признаками вируса в ПК, и при их появлении рекомендуется провести полную проверку компьютера антивирусной программой.

Источники распространения вирусов

Развитие современных компьютерных технологий и средств связи дает возможность злоумышленникам использовать различные источники распространения вирусов, указанные ниже.

Интернет

Глобальная сеть Интернет уникальна тем, что не является чьей-то собственностью и не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией. Сейчас любой человек может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб-ресурс.

Однако эти же особенности глобальной сети предоставляют злоумышленникам возможность совершения преступлений в Интернете, затрудняя их обнаружение и наказание. Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, «маскируют» их под полезное и бесплатное программное обеспечение. Благодаря тому, что сегодня в сети Интернет можно скачать практически все, вирусы получают очень широкое распространение, так как платить за программное обеспечение не все хотят. Кроме того, скрипты, автоматически запускаемые при открытии некоторых веб-страниц, могут выполнять вредоносные действия на компьютере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и серверы компаний. Результатом таких атак может являться выведение ресурса из строя, получение полного доступа к ресурсу, а следовательно, к информации, хранящейся на нем, использование ресурса как части зомби-сети.

В связи с появлением кредитных карт, электронных денег и возможностью их использования через Интернет (интернет-магазины, аукционы, персо-

нальные страницы банков и т.д.) интернет-мошенничество стало одним из наиболее распространенных преступлений.

Интранет

Интранет – это внутренняя сеть, специально разработанная для управления информацией внутри компании или, например, частной домашней сети. Интранет является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети. Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются значительному риску заражения. Во избежание возникновения таких ситуаций необходимо защищать не только периметр сети, но и каждый отдельный компьютер.

Электронная почта

Наличие почтовых приложений практически на каждом компьютере, а также то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых жертв, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т. д.

Помимо угрозы проникновения вредоносных программ существуют проблема внешней нежелательной почты рекламного характера (спама). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые серверы, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный финансовый урон.

Также важно отметить, что злоумышленники стали использовать так называемые спамерские технологии массового распространения и методы социального инжиниринга, чтобы заставить пользователя открыть письмо, перейти по ссылке из письма на некий интернет-ресурс и т.п.

Съемные носители информации

Съемные носители – CD/DVD-диски, флеш-карты – широко используются для хранения и передачи информации. При запуске файла, содержащего вредоносный код, со съемного носителя можно повредить данные, хранящиеся на компьютере, а также распространить вирус на другие диски компьютера или компьютеры сети.

Чаще всего поражаются вирусами файлы следующих форматов:

.bat – пакетный файл;

.com – командный файл, вид исполняемого файла, размер которого не может превышать 64 Кб;

.dll – файл библиотеки динамической компоновки;

.elf – исполняемый файл в операционных системах Linux/UNIX;

.exe – исполняемый файл;

.ini – конфигурационный файл;

.sys – системный файл.

Классификация компьютерных вирусов

В настоящее время существует огромное количество вирусов, которыми может заразиться компьютер. Периодически предпринимаются попытки выработать общую классификацию обнаруживаемых вирусов, однако они, по большей части, остаются безуспешными. Киберкриминал пребывает в непрекращающемся развитии, постоянно появляются новые угрозы, поэтому нет устоявшейся категории вирусов. Далее рассматриваются основные виды вирусов по классификации одного из ведущих производителей антивирусной продукции – компании «Лаборатория Касперского».

По типу действий, совершаемых на компьютере пользователей, вредоносные объекты разделяют на две категории (рис. 2.1): *вредоносные программы* (Malware) и *потенциально (условно) нежелательные программы* (PUPs, Potentially Unwanted Programs).

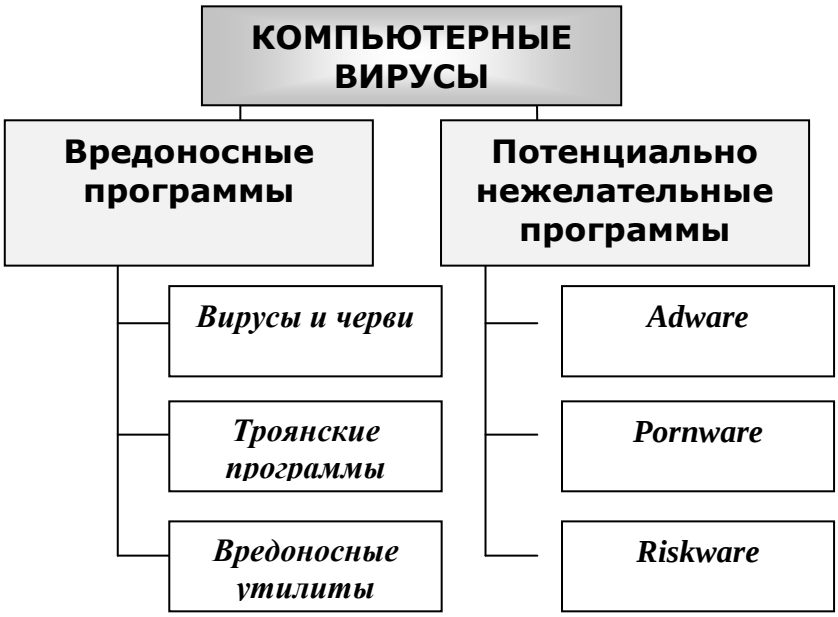


Рис. 2.1. Компьютерные вирусы

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и вредоносные утилиты – инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.).

Вирусы и черви (уровень опасности высокий) обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

Вирусы (Viruses) заражают гие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.

Название «вирус» было взято из биологии, так как процесс захвата компьютера вирусом полностью соответствует процессу захвата вирусом человеческого организма. Биологический вирус внедряется в клетку, после чего начинает размножаться. Так и компьютерный: попав в программу, вирус действует аналогичным образом.

Впервые это определение было дано Фредом Коэном[1], который сказал, что вирус является программой, способной заражать другие программы путем добавления в них копии самой себя. Сегодня компьютерный вирус – это совсем не та безобидная программка, которой являлся первый написанный вирус. Если раньше вирусы использовались ради развлечения, то на сегодняшний день такие программы пишутся профессионалами с целью нанесения крупного ущерба или кражи средств с электронных счетов.

Таким образом, основное действие, выполняемое вирусом – *заражение*. Вирус – это саморазмножающаяся программа: она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви (Worms) для распространения используют в основном уязвимости операционных систем. Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети и электронную почту. Также благодаря этому многие черви обладают достаточно высокой скоростью распространения.

Черви проникают на компьютер, осуществляют поиск сетевых адресов других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

[1] См. История компьютерных вирусов [Электронный ресурс]. – Режим доступа: http://antivibest.ru/page/istorija-kompjuternyh-virusov-computer

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. А червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен. Другими словами, червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

Троянские программы (уровень опасности высокий).

По греческому преданию, после долгих лет осады ахейцы, отступая от Трои, оставили в подарок ее жителям огромного деревянного коня. Троянцы как дар ввезли его в город. Ночью спрятавшиеся в коне воины убили часовых и открыли ворота в город, чтобы впустить основное войско. С тех пор выражение «троянский конь» стало нарицательным (дар врагу, чтобы погубить его).

По классическому определению, троянец – это программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает вредоносные действия. Эти вредоносные программы созданы для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не могут распространяться сами по себе, т.е. не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. Однако они в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

Обычно троянцы скрытно устанавливаются на компьютер и выполняют вредоносные действия без ведома пользователя. Трояны разных видов составляют большую часть современных вредоносных программ; все они пишутся специально для выполнения конкретной зловредной функции. Чаще всего встречаются backdoor-троянцы (утилиты удаленного администрирования, часто включают в себя клавиатурные шпионы), троянцы-шпионы, троянцы для кражи паролей и троянцы-прокси, превращающие компьютер в машину для рассылки спама.

Вредоносные утилиты (уровень опасности средний) представляют собой вредоносные программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации атак на удаленные сервера, взлома других компьютеров и т.п. В отличие от вирусов, червей и троянских программ, представители данной категории не представляют угрозы компьютеру, на котором исполняются.

Еще несколько лет назад угроза для пользовательских компьютеров в основном исходила от вирусов. В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, были черви. Далее по распространенности следовали вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов. У этих программ одна главная цель – распространиться как можно шире, хотя запуск некоторых из них приводит и к повреждению данных пользователя или выходу компьютера из строя. Создание и распространение такого вредоносного ПО получило название *кибервандализма*. В последние годы ситуация радикально изменилась. Сегодня наиболее значительную угрозу представляет собой мошенническое ПО, созданное злоумышленниками для получения незаконных доходов. Большинство вредоносных программ, используемых с этой целью, принимают вид разного рода вирусов, червей и троянских программ и т.п.

Потенциально нежелательные программы (PUPs, Potentially Unwanted Programs) — это программы, которые разрабатываются и распространяются абсолютно легально и могут использоваться в повседневной работе, однако обладают функциями, которые могут причинить вред пользователю — но только при выполнении ряда условий. Подобные программы могут быть использованы как во благо, так и во вред – в зависимости от того, в чьих руках они находятся. Поэтому эти программы выделяют в отдельную группу *потенциально (условно) нежелательных программ* – программ, которые невозможно однозначно отнести ни к опасным, ни к безопасным. Решение вопроса о том, опасна эта программа для вашего компьютера или нет, пользователь ПК принимает самостоятельно!

В настоящее время к потенциально (условно) нежелательным программам относят программы классов Adware, Pornware и Riskware.

Adware (уровень опасности средний) – это рекламное программное обеспечение, предназначенное для показа рекламных сообщений (чаще всего, в виде графических баннеров); перенаправления поисковых запросов на рекламные веб-страницы; а также для сбора данных маркетингового характера об активности пользователя (например, какие тематические сайты посещает пользователь).

За исключением показов рекламы, подобные программы, как правило, никак не проявляют своего присутствия в системе – отсутствует значок в системном трее, нет упоминаний об установленных файлах в меню программ. Часто у Adware-программ нет процедур деинсталляции, используются пограничные с вирусными программами технологии, позволяющие скрытно внедряться на компьютер пользователя и незаметно осуществлять на нём свою деятельность.

Попадают на компьютеры пользователей Adware-программы чаще всего двумя способами: путем встраивания рекламных компонентов в бесплатное и

условно-бесплатное программное обеспечение (freeware, shareware); путем несанкционированной пользователем установки рекламных компонентов при посещении пользователем «заражённых» веб-страниц.

Большинство программ freeware и shareware прекращает показ рекламы после их покупки или регистрации.

Базовое назначение Adware данного типа – неявная форма оплаты программного обеспечения, осуществляемая за счет показа пользователю рекламной информации (рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство — разработчику Adware).

Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Не следует путать Adware, занимающиеся сбором информации, с троянскими шпионскими программами. Отличие Adware состоит в том, что они осуществляют подобный сбор с согласия пользователя. Если Adware никак не уведомляет пользователя об осуществляемом ей сборе информации, то она относится уже к категории вредоносных программ.

Pornware (уровень опасности средний) – это программы, которые так или иначе связаны с показом пользователю информации порнографического характера. Программы категории Pornware могут быть установлены на пользовательский компьютер злоумышленниками – через использование уязвимостей операционной системы и интернет-браузера или при помощи вредоносных троянских программ. Делается это обычно с целью «насильственной» рекламы платных порнографических сайтов и сервисов, на которые пользователь сам по себе никогда не обратил бы внимания.

Riskware (уровень опасности средний) – к этой категории относятся обычные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые, тем не менее, способны причинить вред (вызвать уничтожение, блокирование, модификацию или копирование информации, нарушить работу компьютеров или компьютерных сетей).

К категории таких программ относятся программы, имеющие бреши и ошибки, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки (скачивания) файлов, программы автоматического переключения раскладки клавиатуры, мониторы активности компьютерных систем, утилиты для работы с паролями, всевозможные утилиты для остановки процессов или скрытия их работы и проч.

Все эти программы не являются вредоносными сами по себе, однако обладают функционалом, которым могут воспользоваться злоумышленники для причинения вреда пользователям. Выбор, обнаруживать или нет подобные про-

граммы, лежит на пользователе. По умолчанию обычно в антивирусных продуктах обнаружение Riskware-программ отключено.

2.2. Характеристика антивирусных программ

Антивирусная программа (синонимы: *Антивирус, Антивирусный монитор, Постоянная защита, Антивирусный сканер, Защита по требованию*) – это программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

Антивирусные программные средства по удобству и частоте применения можно довольно условно разделить на следующие типы:

- комплексные антивирусные программные пакеты;
- бесплатные версии антивирусов;
- утилиты-сканеры;
- дозагрузочные утилиты-сканеры.

Комплексные антивирусные программные пакеты – осуществляют полномасштабный мониторинг программного обеспечения компьютера и работают в теле операционной системы (как правило, включают в себя несколько одновременно работающих взаимосвязанных модулей). Примерами таких пакетов служат антивирусы Касперского, Dr.Web (или антивирус Доктор Веб), F-Prot, Mcafee, Avira, Avast, Sophos, NOD32, McAfee, Panda, Norton, AVG.

Почти все производители антивирусов дают попробовать их в действии на некоторый срок бесплатно (демонстрационные версии) – обычно от 2 недель до 3 месяцев, после чего пользователь должен принять решение о покупке продукта или удалить его со своего компьютера, потому что по истечении пробного срока антивирус теряет функциональность полностью или частично.

Бесплатные версии антивирусов – урезанные по функциональности версии полномасштабных антивирусных продуктов для «индивидуального домашнего применения» – успешный маркетинговый ход компаний. Пример – антивирусы Avira AntiVir Personal Edition Classic и Avast! 4 Home Edition.

Утилиты-сканеры – тип антивирусных продуктов, не ведущих постоянного мониторинга процессов в компьютере, а запускаемых вручную, по необходимости. Этот класс является выделением из первого и служит цели привлечения внимания клиента к более совершенным и дорогим продуктам. Относительно первого и второго типов является более упрощённым как в функциональности, так и в размере. Например – Dr.Web Cureit и адресные утилиты Касперского.

Дозагрузочные утилиты-сканеры – это *антивирусные утилиты*, производящие загрузку и проверку данных до загрузки операционной системы. Например – Avira NTFS4DOS Personal, или Avast! 7.7 for DOS , или Dr.Web сканер

командной строки. Но так как для их использования необходима квалификация пользователя выше среднего, применяются они не часто.

В настоящее время большинство ведущих антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Постоянная антивирусная защита (*монитор*) запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность действия, совершаемые другими программами. При этом проверяются не только файлы на различных носителях информации, но и оперативная память компьютера. Такая защита называется еще *резидентная защита*. Дословно в переводе *резидентный* переводится как фоновый или невидимый. Причем резидентная защита проявляет себя только при обнаружении вируса. В момент работы компьютера, когда системе ничего не угрожает, пользователю совершенно незаметно присутствие модуля в системе. Именно на данном принципе построен главный принцип антивирусного ПО – предотвращение заражения ПК. Это лежит в основе всех современных антивирусных программ: не лечить систему после заражения, а не допустить заражения на стадии проникновения в систему. Основная задача постоянной антивирусной защиты компьютера: обеспечивать максимальную безопасность при минимальном замедлении работы проверяемых на вредоносные действия программ. В принципе, монитор можно временно отключить – например, когда пользователь отключен от сети и не загружает никаких файлов с внешних носителей.

Защита по требованию (сканер) запускается самим пользователем и, как правило, заключается в полном или выборочном сканировании присутствующих на жестких и сетевых дисках компьютера файлов, а также в однократной проверке оперативной памяти компьютера. В большинстве случаев антивирусные сканеры гораздо более требовательны к ресурсам компьютера, нежели постоянная антивирусная защита. По окончании работы сканер автоматически выключается.

Файервол (firewall)

Пользователь работает на компьютере не только автономно, но у него имеется возможность работать и общаться в сети Интернет. Если на компьютере находится конфиденциальная информация, нет никакой гарантии, что она не станет достоянием общественности. Тем не менее, такие гарантии нужны, особенно тем, кто работает с очень важными, засекреченными данными. Защиту информации обеспечивает как раз firewall. В переводе с английского

слово означает горящую стену. Однако пользователи называют ее просто стеной или *брандмауэром*. Файервол нужен для того, чтобы обеспечивать некую преграду между сетью и компьютером. То есть он служит фильтром, является защитой от несанкционированного доступа. Возможными последствиями такого доступа может быть кража паролей и информации, удаление данных, дача информации о веб-предпочтениях пользователя и т.п. Принцип работы файервола заключается в том, что программа отслеживает соединения нального компьютера, после чего анализирует их и принимает решение относительно того, разрешить данное соединение или нет. Таким образом, данная программа пропускает то, что разрешил сам пользователь, при этом не пропуская больше ничего. Полную безопасность программа обеспечить не может. Однако для тех, кто хочет взломать компьютер, стена служит немалой преградой. Тут все зависит от опыта хакера.

Для того чтобы компьютер пользователя был максимально защищен, необходимо провести настройку. Основные рекомендации по настройкам заключаются в том, чтобы разрешить подключение только тем программам, которые действительно нуждаются в подключении. При этом нужно сделать так, чтобы программа имела доступ только к тем портам, по которым она работает, не более. Это кажется сложным, но в современных брандмауэрах есть помощники настройки, которые максимально упрощают процесс, подсказывая пользователю. Кроме того, нужно внимательно относиться к программе и всегда читать сервисные сообщения, которые появляются во время работы. В них часто содержатся различного рода предупреждения по работе компьютера и его соединениям.

Существует два основных вида файерволов – персональные и корпоративные. Персональная стена является программой, установленной на обычном пользовательском компьютере. Что касается корпоративного файервола, то он устанавливается на шлюз между локальной сетью и сетью Интернет и настраивается системным администратором. Если у пользователя установлен персональный файервол, то в нем имеется встроенный режим обучения. С его помощью проще разобраться в том, как работает программа и что допустить к соединению, а что запретить. Если одна из программ, которая установлена на компьютере, не имеет правил, подходящих для файервола, то появится сообщение, чтобы пользователь самостоятельно смог решить: давать разрешение на соединение или нет. Персональных файерволов на сегодняшний день очень много, и среди них легко подобрать подходящий. Вне зависимости от вида, по функциям они практически не отличаются друг от друга. Основные различия заключаются в том, насколько удобно пользоваться той или иной программой, у какой из них более интересный и удобный интерфейс, а также то, является программа платной или бесплатной.

Примерами бесплатных файерволов являются: Online Armor Personal Firewall Free, Comodo Firewall, ZoneAlarm Free, Outpost Firewall Free, PC Tools Firewall Plus, Outpost Security Suite Free, Sunbelt Kerio Personal Firewall.

Следует отметить, что многие антивирусные программы имеют в своем составе встроенный файервол. Обычно в современных антивирусных программах, кроме указанных, присутствуют еще следующие модули: модуль автоматического обновления; программа-планировщик для организации обновления по расписанию и т. п.; модуль защиты электронной почты; центр управления и др.

К сожалению, многие популярные антивирусы вместе с защитой приносят владельцу компьютера определенные неудобства: медленный запуск машины, проблемы в работе игр, а также раздражающие окна с непонятными вопросами, «всплывающие» в самый неподходящий момент. Однако нужно понимать, что без защиты использовать компьютер сегодня нельзя!

2.3. Работа с антивирусными программами

На сегодняшний день одними из наиболее распространенных (и эффективных) антивирусных программ являются антивирусы Касперского и Dr.Web.

а) б)

Рис. 2.2. Логотипы антивирусных программ:
а – антивирус Касперского; б – Dr.Web

Работу с антивирусными программами рассмотрим на примере антивируса Касперского. Приобрести эту лицензионную программу можно в коробочной или в электронной версии, распространяемой через онлайн-магазин. Лицензия для использования этой современной программы для двух компьютеров сроком на один год стоит от 43 до 87 долларов в зависимости от версии антивируса, а при продлении этого срока действуют скидки.

Если антивирус куплен на компакт-диске, то установка продукта начинается автоматически после размещения диска в дисководе. При приобретении антивируса в онлайн-магазине вместе с программой передается ссылка на исполняемый файл инсталлятора, который необходимо запустить вручную.

Вообще дистрибутивы продуктов Антивирус Касперского находятся в свободном доступе – их можно скачать с сайта производителя www.kaspersky.ru в любой момент. Для корректной работы программы ее необходимо установить, а затем активировать специальным (активационным) кодом.

Предлагается 3 варианта активации:

- *активировать коммерческую версию* – необходимо ввести 20-значный код активации, который получен при покупке лицензии (для коробочной версии этот код можно найти на первой странице краткого руководства пользователя, а если программа приобретена через Интернет, то код активации высылается в электронном письме от онлайн-магазина);
- *активировать пробную версию* – мастер установки скачает и установит ключевой файл сроком на 30 дней. Пробная бесплатная версия полностью функциональна, однако по истечении срока пробного ключа обновление баз будет недоступно;
- *активировать позже* – пропустить активацию на данном этапе. В этом случае обновление антивирусных баз будет доступно только после активации.

Все продукты Лаборатории Касперского активизируются кодом активации только при наличии соединения с сетью Интернет. В этом случае программа соединяется с серверами Лаборатории Касперского и отправляет на них ваш код активации. После установления соединения код активации проверяется. Если код активации прошел проверку, программа получает ключевой файл, который устанавливается автоматически. В завершение процесса активации в окне программы появляется подробная информация о приобретенной лицензии.

Существуют для домашнего ПК следующие современные версии программ Лаборатории Касперского:

Kaspersky Antivirus 2012 — это решение для базовой защиты компьютера от вредоносных программ. Продукт обеспечивает защиту в режиме реального времени от основных информационных угроз — как известных, так и новых.

Kaspersky Internet Security 2012 — решение для обеспечения оптимального уровня безопасности. Инновационная гибридная защита мгновенно устраняет вредоносные программы, спам и другие интернет-угрозы, экономя ресурсы компьютера за счет комбинации облачных и антивирусных технологий.

Kaspersky CRYSTAL — это не просто антивирусное решение. Продукт содержит уникальные технологии и инструменты для защиты всей информации, которую вы создаете и храните в цифровом виде – документов, фотографий, музыкальных и видеофайлов, а также персональных данных. С Kaspersky CRYSTAL можно централизованно управлять защитой нескольких компьютеров в домашней сети.

Компоненты программы

Компоненты Антивируса Касперского, предназначенные для защиты ПК от заражения, постоянно находятся в оперативной памяти компьютера и прове-

ряют все открываемые, сохраняемые и запускаемые файлы и объекты, поступающие из Интернета или через электронную почту.

По умолчанию компоненты защиты (рис. 2.3) запускаются при старте операционной системы и защищают компьютер в течение всего сеанса работы. Можно отключить работу какого-либо компонента.

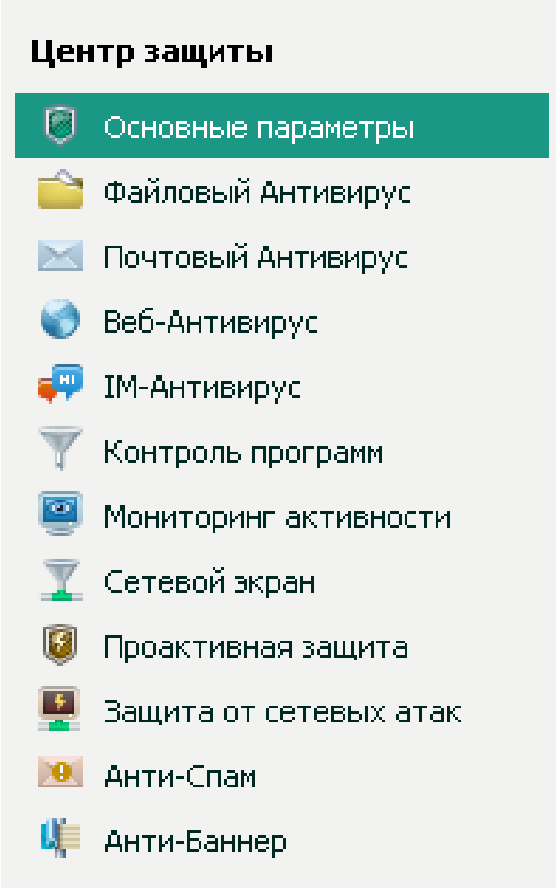


Рис. 2.3. Компоненты защиты антивируса

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках на наличие в них вирусов и других программ, представляющих угрозу.

Почтовый Антивирус перехватывает и проверяет каждое почтовое сообщение, принимаемое или отправляемое пользователем, на наличие в них опасных объектов. Если угрозы в почтовом сообщении не обнаружены, оно становится доступным для пользователя. Индикатором работы компонента служит значок в области уведомлений панели задач, который принимает вид  каждый раз при проверке письма.

Веб-Антивирус предназначен для обеспечения безопасности работы в Интернете, защищает информацию, поступающую на компьютер по протоко-

лам HTTP, HTTPS и FTP, а также предотвращает запуск на компьютере опасных скриптов.

Гео-фильтр – модуль Веб-Антивируса, который обнаруживает попытку перейти на веб-сайт, относящийся к запрещенному региональному домену, при этом в окне браузера выводится соответствующее уведомление. Домен считается запрещенным в следующих случаях: обращение к домену запрещено при настройке Веб-Антивируса; предыдущее обращение к веб-сайту из данного региона было запрещено пользователем.

IM-Антивирус обеспечивает безопасность работы с интернет-пейджерами и многими программами для быстрого обмена сообщениями.

Сообщения, переданные через интернет-пейджеры, могут содержать ссылки на подозрительные веб-сайты, а также на веб-сайты, которые используются злоумышленниками для фишинг-атак. Вредоносные программы используют интернет-пейджеры для рассылки спам-сообщений, а также ссылок на программы, которые крадут номера и пароли пользователей. IM-Антивирус обеспечивает безопасную работу со многими программами для быстрого обмена сообщениями, в том числе ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Агент и IRC.

Анти-Фишинг – защита от краж информации. Отслеживает попытки открытия фишинг-сайта и блокирует его. Фишинг-атаки, как правило, представляют собой почтовые сообщения от якобы финансовых организаций и содержат ссылки на веб-сайты таких организаций. Почтовое сообщение предлагает воспользоваться ссылкой и ввести на открывшемся веб-сайте конфиденциальную информацию, например, номер кредитной карты или имя и пароль учетной записи интернет-банка. Частным примером фишинг-атаки может служить письмо якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств. В состав баз приложения включены известные на настоящее время сайты, которые используются для фишинг-атак. Компонент встроен в Веб-Антивирус и IM-Антивирус.

Проактивная защита защищает не только от известных угроз, но за счет использования превентивных технологий защищает и от новых, информация о которых отсутствует в базах приложения. Реагирует на все подозрительные последовательности действий, блокирует активность этой программы и уведомляет пользователя.

Например, обнаружив такие действия, как самокопирование программы на сетевые ресурсы, в каталог автозапуска и системный реестр, с большой вероятностью можно предположить, что эта программа является червем. К опасным последовательностям действий относятся также попытки изменения файла HOSTS, скрытая установка драйверов и другие.

Контроль программ – предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и вашим персональным данным. Компонент отслеживает действия, которые совершают в системе программы, установленные на компьютере, и регулирует их на основании заданных правил. Эти правила регламентируют потенциально опасную активность, в том числе доступ программ к защищаемым ресурсам (например, файлам, папкам, ключам реестра, сетевым адресам).

Мониторинг активности – собирает данные о действиях программ на ПК и предоставляет эту информацию другим компонентам для более эффективной защиты. На основе этой информации программа Антивируса Касперского может выполнять откат действий, произведенных вредоносными программами, который может быть инициирован одним из следующих компонентов защиты: Мониторингом активности на основе шаблонов опасного поведения; Проактивной защитой; Файловым Антивирусом; при проверке на вирусы.

Сетевой экран – обеспечивает безопасность работы в локальных сетях и Интернете.

Защита от сетевых атак – запускается при старте операционной системы, отслеживает во входящем трафике активность, характерную для сетевых атак, и блокирует любую сетевую активность атакующего ПК. По умолчанию блокирование происходит на один час. На экран выводится уведомление о том, что была произведена попытка сетевой атаки с указанием информации об атакующем компьютере.

Анти-Спам – встраивается в почтовый клиент, установленный на ПК, контролирует все поступающие почтовые сообщения на предмет спама и анализирует почтовые сообщения на предмет фишинг-мошенничества. Анти-Спам в виде модуля расширения встраивается в следующие почтовые клиенты: Microsoft Office Outlook; Microsoft Outlook Express (Windows Mail); The Bat!; Thunderbird. Списки запрещенных и разрешенных отправителей позволяют указать, письма с каких адресов следует считать полезными, а с каких – спамом. К спаму могут быть отнесены письма, адресованные не вам. Кроме того, Анти-Спам может анализировать сообщение на наличие разрешенных и запрещенных фраз, а также фраз из списка нецензурных выражений.

Анти-Спам не требует обучения: черные списки формируются на основании опыта сообщества пользователей и находятся в «облаке»[2].

Анти-Баннер – блокирует рекламную информацию, размещенную на специальных баннерах, встроенных в интерфейс различных программ, установленных на компьютере и находящихся в Интернете. Рекламная информация на

[2]«Облако» (Kaspersky® Security Network) — это инфраструктура онлайн-служб и сервисов, которая непрерывно собирает и анализирует информацию о киберкриминальной активности по всему миру. Данные, необходимые для блокирования атак и заражений, мгновенно передаются всем пользователям Антивируса Касперского 2012, предотвращая масштабные вирусные эпидемии.

баннерах может отвлекать от дел, а загрузка баннеров увеличивает объем загружаемого трафика.

Безопасная среда и безопасный браузер – позволяет выполнить потенциально опасные действия изолированно от основной операционной системы. Для этого существуют следующие возможности: запуск отдельной программы в безопасном режиме на основном рабочем столе; работа в безопасной среде; работа в безопасном браузере. Изоляция от основной операционной системы обеспечивает дополнительную защиту компьютера, так как реальные объекты операционной системы не подвергаются изменениям. Подозрительные файлы, обнаруженные при работе в изолированном режиме, помещаются на карантин. *Карантин* – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Возможно зараженный файл может быть обнаружен и помещен на карантин в процессе проверки на вирусы, а также *Файловым Антивирусом*, *Почтовым Антивирусом* и *Проактивной защитой*.

Безопасный браузер предназначен для доступа к системам интернет-банкинга и другим веб-сайтам, работающим с конфиденциальными данными. При работе в безопасном браузере введенные данные и сделанные изменения (например, сохраненные файлы cookies, журнал посещенных веб-сайтов) не попадают в операционную систему, а значит, не могут быть использованы злоумышленниками.

Родительский контроль – компонент программы, выполняющий функции контроля доступа пользователей компьютера к веб-ресурсам. Основной задачей Родительского контроля является ограничение доступа, в первую очередь, к веб-сайтам, предназначенным для взрослой аудитории, затрагивающим темы порнографии, оружия, наркотиков, провоцирующим жестокость, насилие и т. д., а также к веб-сайтам, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы).

Родительский контроль позволяет снизить риски, связанные с работой на компьютере и в Интернете. Для этого используются следующие функции модуля: ограничение использования компьютера и Интернета по времени; создание списков разрешенных и запрещенных для доступа веб-сайтов и запуска приложений, а также временное ограничение запуска разрешенных приложений; выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов; включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на веб-сайты с сомнительным содержимым не отображаются в результатах поиска); ограничение загрузки файлов из Интернета; создание списков контактов, запрещенных или разрешенных для общения через интернет-пейджеры и в социальных сетях; просмотр текста переписки через интернет-пейджеры и в социальных сетях; запрет пересылки определенных персональных данных; поиск заданных ключевых слов в тексте переписки.

Устранение следов активности. При работе на компьютере действия пользователя регистрируются в системе. При этом сохраняются данные о вве-

денных пользователем поисковых запросах и посещенных им сайтах, о запуске программ и открытии и сохранении файлов, записи в системном журнале Microsoft Windows, временные файлы и многое другое. Все эти источники информации об активности пользователя могут содержать конфиденциальные данные (в том числе пароли) и могут оказаться доступными для анализа злоумышленниками. В то же время пользователь зачастую не обладает достаточными знаниями для того, чтобы предотвратить хищение информации из этих источников. В состав Kaspersky Internet Security 2012 входит *Мастер устранения следов активности*, который производит поиск как следов активности пользователя в системе, так и параметров операционной системы, способствующих накоплению информации об этой активности. По завершении поиска мастер сообщает о найденных следах активности и предлагаемых действиях для их устранения.

Некоторые компоненты защиты доступны только в Kaspersky Internet Security 2012. Среди них: контроль программ; родительский контроль; сетевой экран; защита от сетевых атак; гео-фильтр; блокирование доступа к небезопасным веб-сайтам; мониторинг сети; анти-спам; анти-баннер; устранение следов активности; безопасная среда.

Интерфейс приложения

Антивирус Касперского обладает достаточно простым и удобным в работе интерфейсом. Новый интуитивно понятный интерфейс позволяет получить быстрый доступ ко всем функциям и возможностям приложения. Современный анимированный дизайн облегчает восприятие информации и позволяет упростить процесс работы с программой.

Значок приложения. Сразу после установки Антивируса Касперского в области уведомлений панели задач появляется его значок  .

Он является своего рода индикатором работы антивируса, отражая состояние защиты и показывая ряд основных выполняемых им действий. В зависимости от выполняемой операции значок меняет вид. Если значок активный (цветной), это означает, что защита компьютера включена. Неактивный значок (черно-белый) значит, что все компоненты защиты выключены.

С помощью этого значка можно получить доступ к основным элементам интерфейса приложения: контекстному меню и главному окну программы. Щелчок по значку приведет к открытию главного окна.

Контекстное меню значка приложения Kaspersky Internet Security 2012 (рис. 2.4) позволяет сразу перейти к выполнению основных задач защиты. Среди его команд следует отметить:

- *Менеджер задач* – открывает окно Менеджера задач, где можно просмотреть список задач проверки, которые были выполнены или выполняются в текущий момент. Менеджер задач впервые появился в версии KIS 2012.

- *Обновление* – запускает обновления модулей и сигнатур угроз для антивируса и их установку на компьютере.
- *Инструменты* – открывает вложенное меню, содержащее пункты:
  - *Контроль программ* — открывает окно Активность программ;
  - *Мониторинг сети* — открывает окно Мониторинг сети;
  - *Виртуальная клавиатура* — выводит на экран виртуальную клавиатуру.
- *Безопасная среда* — запускает безопасный рабочий стол для работы с программами, которые, по мнению пользователя, могут быть небезопасны. Если безопасный рабочий стол уже запущен, то выполняется переключение на него.
- *Kaspersky Internet Security* — открывает главное окно программы.
- *Приостановить защиту/Возобновить защиту* — временно выключает/включает работу компонентов постоянной защиты. Данный пункт меню не влияет на обновление программы и на выполнение задач поиска вирусов.
- *Включить /Выключить Родительский контроль* — включает/выключает *Родительский контроль* для текущей учетной записи.
- *Настройка* — открывает окно настройки параметров работы программы.
- *О программе* — открывает информационное окно со сведениями о программе.
- *Новости* — открывает окно новостного агента. Этот пункт меню отображается при наличии непрочитанных новостей.
- *Выход* — завершает работу антивируса; программа выгружается из оперативной памяти компьютера.

Если в момент открытия контекстного меню запущена какая-либо задача проверки на вирусы или задача обновления программы, ее название будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав пункт меню с названием задачи, вы можете перейти к главному окну с отчетом о текущих результатах ее выполнения.

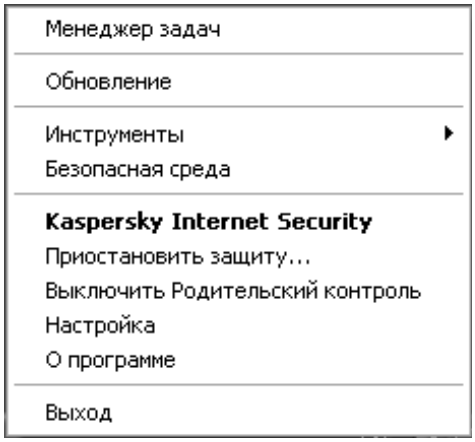


Рис. 2.4. Контекстное меню значка приложения

В *главном окне приложения* (рис. 2.5) сосредоточены элементы интерфейса, предоставляющие доступ ко всем основным функциям программы.

Вы можете открыть главное окно программы одним из следующих способов:

- щелчком по значку программы в области уведомлений панели задач;
- выбрав пункт Kaspersky Internet Security в контекстном меню значка программы на панели задач;
- нажав на область монитора Kaspersky Gadget (только для операционных систем Windows 7 и Vista).

Главное окно приложения условно можно разделить на две области: *верхняя область* окна содержит информацию о состоянии защиты компьютера, *нижняя область* окна позволяет быстро перейти к работе с основными функциями программы (например, к выполнению задач проверки на вирусы, обновлению баз и модулей программы и т. п.).

При выборе одного из разделов в нижней области окна открывается окно соответствующей функции программы, например, проверки на вирусы (рис. 2.6). Вы можете вернуться к выбору любой другой функции, нажав на кнопку *Назад* в верхнем левом углу окна.

Рис. 2.5. Главное окно программы

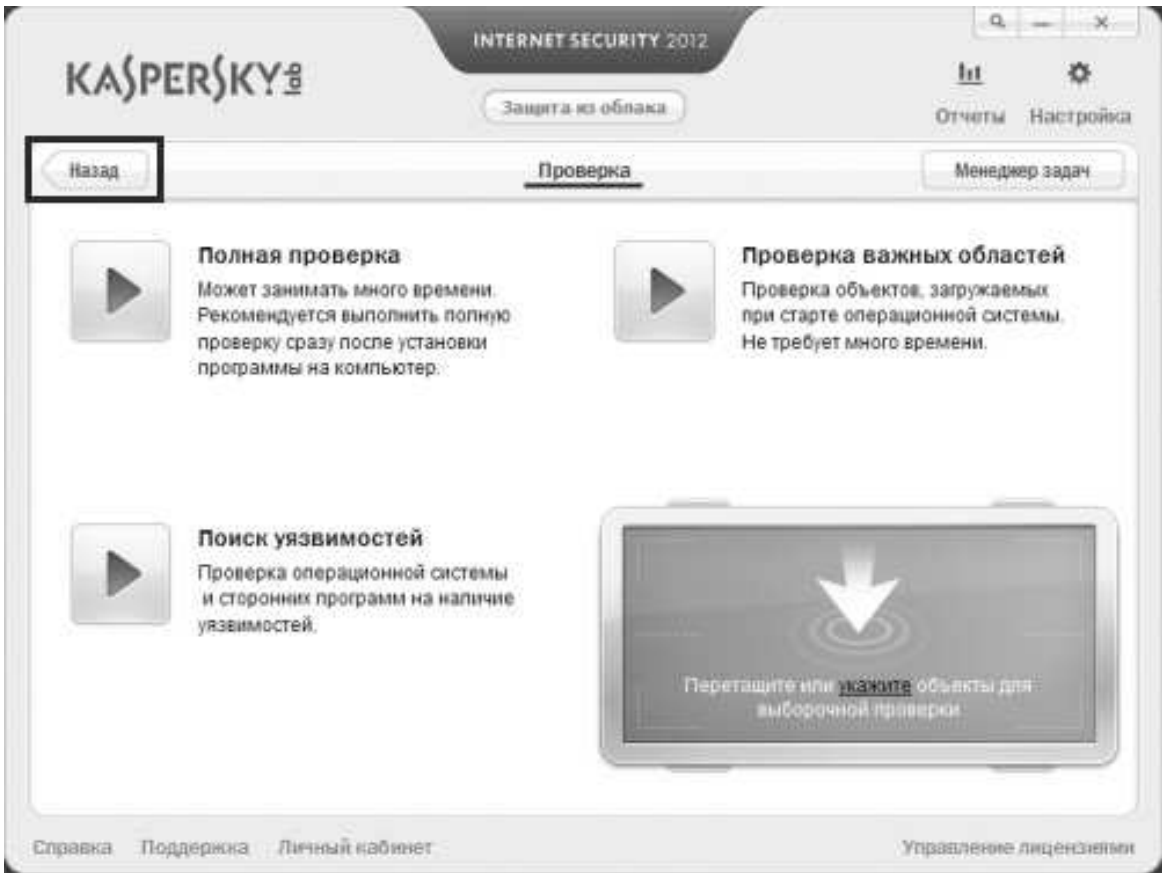


Рис. 2.6. Окно программы проверки на вирусы

Из главного окна программы (рис. 2.5) можно воспользоваться также следующими кнопками и ссылками:

- *Защита из облака* – переход к окну с описанием сервисов сети Kaspersky Security Network и полученной от них информации. Элемент отображает статус доступа к сервисам Лаборатории Касперского, расположенным в Интернете.
- *Настройка* – переход к окну настройки параметров программы.
- *Отчеты* – переход к отчетам о работе программы.
- *Новости* – переход к просмотру новостей в окне новостного агента. Ссылка отображается после получения новости.
- *Справка* – переход к справочной системе антивируса.
- *Личный кабинет* – переход в Личный кабинет пользователя на веб-сайте Службы технической поддержки.
- *Поддержка* – открытие окна с информацией о программе и ссылками на информационные ресурсы (сайт Службы технической поддержки, форум).
- *Управление лицензиями* — переход к активации антивируса, продлению срока действия лицензии.

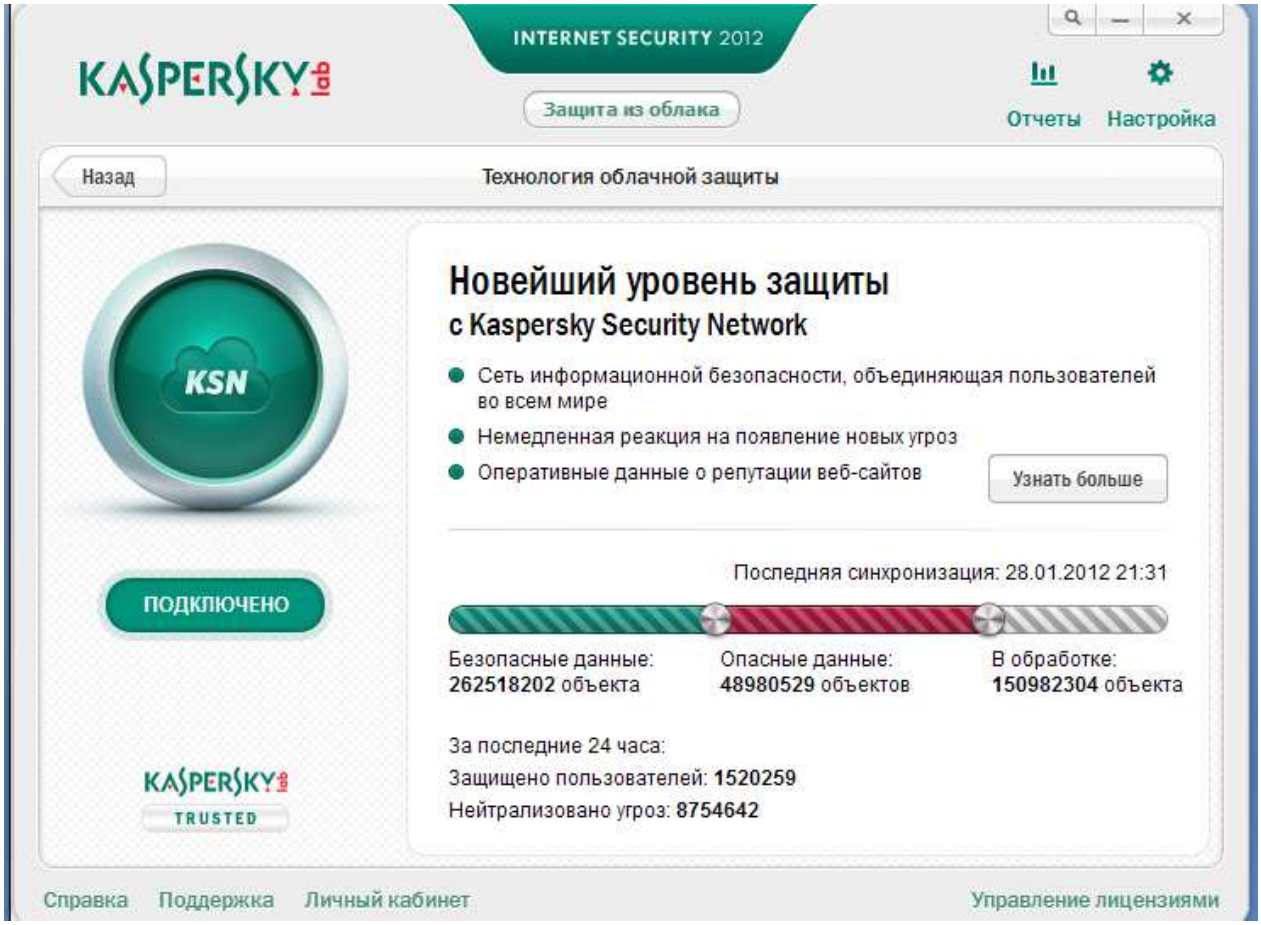


Рис. 2.7. Окно программы *Защита из облака*

Чтобы повысить эффективность защиты компьютера, Kaspersky Internet Security 2012 использует данные, полученные от пользователей со всего мира. Для сбора этих данных предназначена сеть Kaspersky Security Network, которая обеспечивает так называемую *Защиту из облака* (рис. 2.7). Kaspersky Security Network (KSN) — это глобальный сервис оперативного анализа угроз, объединяющий миллионы пользователей во всем мире. Когда KIS 2012 обнаруживает подозрительные или непроверенные данные на компьютере участника KSN, эти данные автоматически отправляются в Лабораторию Касперского. Вирусные аналитики круглосуточно анализируют потенциальные угрозы и выпускают обновления защиты для пользователей в режиме реального времени.

В левой части окна Защита из облака (рис. 2.7) отображается текущий статус сервиса – *Подключено/Отключено*. В правой части окна можно просмотреть информацию, полученную сервисом на текущий момент, а также узнать более подробно о технологии облачной защиты KSN, нажав на кнопку *Узнать больше*.

Уведомления и всплывающие сообщения

При возникновении значимых событий в процессе работы антивируса над значком программы на панели задач выводятся окна уведомлений и всплывающих сообщений.

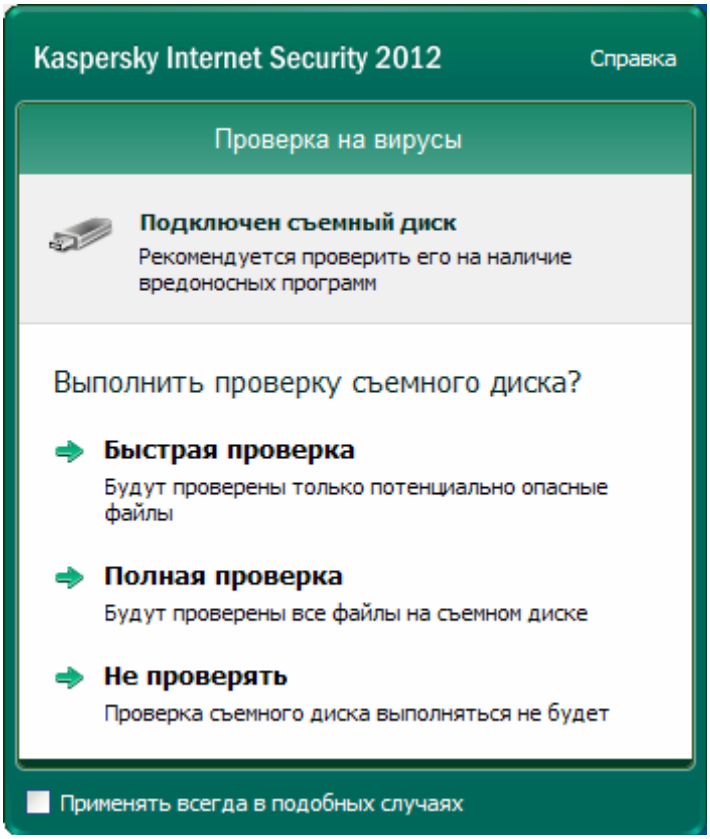


Рис. 2.8. Пример окна уведомления программы

Окна уведомлений (см., например, рис. 2.8) антивирус выводит на экран в тех случаях, когда возможны различные варианты действий в связи с событием, например, при обнаружении вредоносного объекта можно заблокировать доступ к нему, удалить его или попытаться вылечить. Окно уведомления исчезает с экрана только после того, как будет выбрано одно из предложенных действий.

Всплывающие сообщения выводятся на экран, чтобы проинформировать о событиях, не требующих обязательного выбора действия, и автоматически исчезают с экрана вскоре после появления. В некоторых всплывающих сообщениях доступны ссылки, с помощью которых можно выполнить предлагаемое действие (например, запустить обновление баз или перейти к активации программы).

В зависимости от степени важности события с точки зрения безопасности компьютера, уведомления могут быть следующих типов и цветовой гаммы.

Критические (сообщения такого типа имеют красный цвет) – информируют о событиях, имеющих первостепенную важность с точки зрения безопас-

ности компьютера, например, об обнаружении вредоносного объекта или опасной активности в системе.

Важные (желтый цвет) – информируют о событиях, потенциально важных с точки зрения безопасности компьютера, например, об обнаружении возможно зараженного объекта или подозрительной активности в системе.

Информационные (зеленый цвет) – информируют о событиях, не имеющих первостепенной важности с точки зрения безопасности.

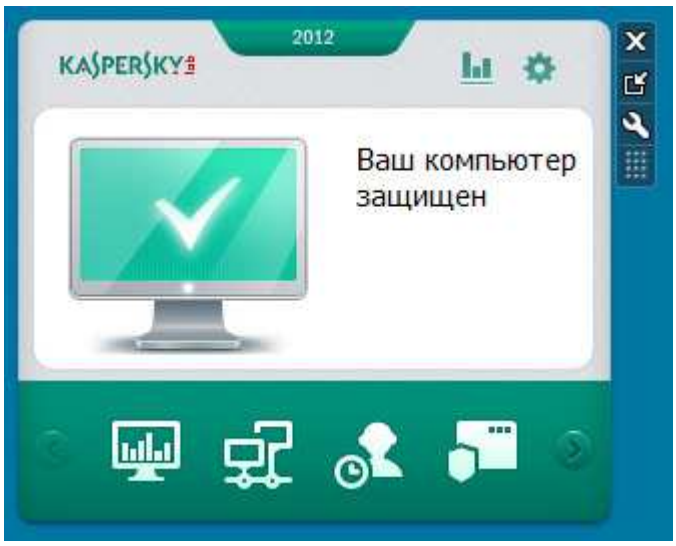
Рис. 2.9. Пример окна критического сообщения

Kaspersky Gadget

При использовании Антивируса Касперского на компьютере под управлением операционных систем Windows 7 и Vista доступен гаджет Kaspersky Gadget. Он предназначен для быстрого доступа к основным функциям программы (например, индикации состояния защиты компьютера, проверке объектов на вирусы, просмотру отчетов о работе программы).

Kaspersky Gadget доступен в двух видах — свернутом и развернутом (рис. 2.10). Цветовой индикатор гаджета сигнализирует о состоянии защиты компьютера, так же, как индикатор, расположенный в главном окне программы. Зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Серый цвет индикатора означает, что работа программы остановлена.

Свернутый вид



Развернутый вид

Рис. 2.10. Kaspersky Gadget

Во время обновления баз и модулей программы в центре гаджета отображается значок вращающегося глобуса. С помощью гаджета можно выполнять следующие действия:

- возобновлять работу программы, если она была приостановлена;
- открывать главное окно программы;
- проверять отдельные объекты на вирусы;
- открывать окно просмотра новостей.

Нажав на кнопку с изображением гаечного ключа во всплывающей панели справа от гаджета, можно настроить его кнопки для выполнения дополнительных действий: запускать обновление; изменять параметры работы программы; просматривать отчеты программы; приостанавливать защиту; открывать виртуальную клавиатуру; открывать окно Менеджера задач.

Новостной агент

Новостной агент информирует обо всех важных событиях, касающихся Антивируса Касперского и защиты от компьютерных угроз в целом. Программа уведомляет о появлении новостей с помощью значка в области уведомлений панели задач и всплывающего сообщения. Информация о количестве непрочитанных новостей также отображается в главном окне программы. В интерфейсе гаджета Антивируса Касперского появляется значок новости. Прочитать новости можно в окне новостного агента одним из следующих способов:

- нажав на значок в области уведомлений панели задач;
- перейдя по ссылке *Читать новости* во всплывающем сообщении о новостях;
- перейдя по ссылке *Новости* в главном окне программы;
- нажав на значок, который отображается в центре гаджета при появлении новости.

Открытие окна новостного агента доступно только при наличии непрочитанных новостей.

Проверка на вирусы

Для поиска вирусов в состав антивируса включены следующие задачи.

Полная проверка. Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память; объекты, исполняемые при старте системы; резервное хранилище системы; почтовые базы; жесткие, съемные и сетевые диски.

Проверка важных областей. Проверка объектов, загружаемых при старте операционной системы (системная память, объекты автозапуска и загрузочные секторы).

Выборочная проверка. Можно проверить любой объект файловой системы компьютера. Также можно сформировать свой список объектов для выборочной проверки, добавив или отключив при этом объекты, находящиеся в списке по умолчанию.

Запустить указанные задачи проверки на вирусы можно из главного окна программы (рис. 2.5) или с помощью ранее созданного специального ярлыка. Из главного окна программы следует в нижней части окна, на панели управления, нажать на кнопку *Проверка*. В открывшемся окне (рис. 2.6) следует запустить необходимую задачу. Задачи полной проверки и проверки важных областей являются специфическими, поэтому для этих задач не рекомендуется редактировать списки объектов для проверки.

Для запуска выборочной проверки на вирусы (файла, папки, диска или другого объекта) надо воспользоваться ссылкой *Укажите* для выбора объекта или, удерживая левую клавишу мыши, перетащить нужный объект в правую нижнюю область окна *Проверка*. Чтобы узнать о последних запущенных задачах проверки, надо нажать на кнопку *Менеджер задач* в правом верхнем углу этого же окна.

Запустить задачу проверки на вирусы удобно в окне *Проводника* из контекстного меню объекта (рис. 2.11), выбрав пункт *Проверить на вирусы*.

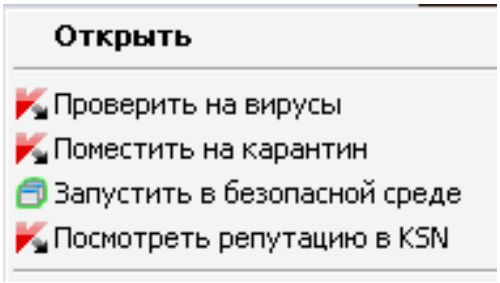


Рис. 2.11. Фрагмент контекстного меню объекта

В операционных системах Windows 7 и Vista проверить объекты на вирусы можно просто, перетащив объект проверки на гаджет антивируса (рис. 2.10).

При обнаружении угрозы антивирус присваивает найденному объекту один из следующих статусов: *вредоносная программа* (например, *вирус*, *троянская программа*) или *возможно зараженный* (подозрительный) объект, если в результате проверки невозможно однозначно определить, заражен он или нет. Когда антивирус работает в интерактивном режиме, программа при обнаружении опасных объектов выводит на экран уведомление, в котором пользователь может выбрать нужное действие из числа вариантов, предлагаемых антивирусом, отдельно для каждого объекта. Если же антивирус работает в автоматическом режиме, при обнаружении опасных объектов будут автоматически применяться рекомендуемые действия. Для вредоносных объектов такими действиями будут *Лечить; Удалять, если лечение невозможно*, а для подозрительных – *Поместить на карантин*.

Перед лечением или удалением зараженного объекта антивирус формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин, для них можно включить автоматическую их проверку после каждого обновления. Информация о результатах проверки и обо всех событиях, произошедших при выполнении задач, записывается в отчет антивируса.

Проверка репутации программ

Антивирус позволяет осуществлять проверку репутации программ. Для этого требуется при установке антивируса согласие участвовать в Kaspersky Security Network. Чтобы узнать репутацию какой-либо программы в контекстном меню (рис. 2.11) исполняемого файла программы, нужно выбрать пункт *Посмотреть репутацию в KSN*. При этом отображаются следующие показатели: название производителя; информация о цифровой подписи; информация о группе, в которую программа помещена большинством пользователей KSN; количество пользователей KSN, использующих программу, если программа отнесена к группе *Доверенные* в базе KSN; время, когда программа стала известна в KSN, и страны, в которых программа наиболее распространена.

Восстановление после заражения

Мастер восстановления после заражения позволяет устранить следы пребывания в системе вредоносных объектов. Рекомендуется запускать его после лечения компьютера с целью убедиться, что все возникшие угрозы и повреждения устранены. (Можно также использовать мастер при подозрении на заражение ПК).

В ходе работы мастер проверяет наличие каких-либо повреждений в системе, таких как: заблокирован доступ к сетевому окружению, изменены расширения файлов известных форматов, заблокирована панель управления и т. п. Затем выполняется анализ собранной информации, чтобы оценить, есть ли повреждения в системе, которые требуют немедленного вмешательства. Результатом является список действий, которые следует выполнить для устранения повреждения. Действия группируются по категориям исходя из серьезности найденных проблем.

Чтобы запустить мастер восстановления после заражения, в главном окне приложения в нижней части окна (рис. 2.5) надо выбрать *Инструменты* и в открывшемся окне (рис. 2.12) в блоке *Восстановление после заражения* нажать на кнопку *Выполнить* для запуска мастера.

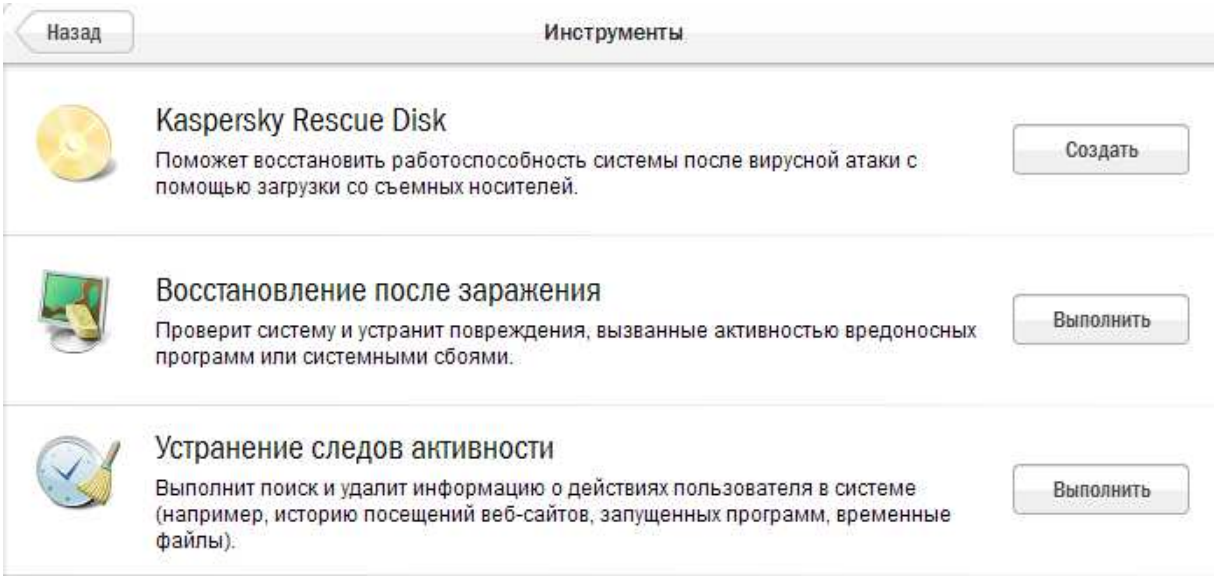


Рис. 2.12. Фрагмент окна *Инструменты*

Удаление следов активности

При работе на компьютере действия пользователя регистрируются в системе. При этом сохраняются данные о введенных пользователем поисковых запросах и посещенных им сайтах, о запуске программ и открытии и сохранении файлов, записи в системном журнале Microsoft Windows, временные файлы и многое другое. Все эти источники информации об активности пользователя могут содержать конфиденциальные данные (в том числе пароли) и могут оказаться доступными для анализа злоумышленниками. В состав Антивируса Касперского входит *мастер устранения следов активности*. Этот мастер производит поиск и удаление как следов активности пользователя в системе, так и параметров операционной системы, способствующих накоплению информации об этой активности.

Для запуска мастера устранения следов активности следует в нижней части главного окна программы выбрать команду *Инструменты* и в открывшемся окне (рис. 2.12) в блоке *Устранение следов активности* нажать на кнопку *Выполнить* для запуска мастера. Для того чтобы устранение следов активности в дальнейшем выполнялось автоматически при завершении работы антивируса, на завершающем шаге работы мастера следует установить флажок *Выполнять устранение следов активности при каждом завершении работы антивируса*. В противном случае этот флажок не надо устанавливать.

Виртуальная клавиатура

При работе за компьютером часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это про-

исходит при регистрации на интернет-сайтах, при совершении покупок в интернет-магазинах и т. д. В таких случаях существует опасность перехвата персональной информации с помощью аппаратных перехватчиков либо клавиатурных шпионов – программ, регистрирующих нажатие клавиш. Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры, только при работе с браузерами Microsoft Internet Explorer, Google Chrome или Mozilla Firefox!

Для использования виртуальной клавиатуры надо в нижней части главного окна программы (рис. 2.5) воспользоваться кнопками прокрутки или развернуть панель управления и выбрать элемент *Виртуальная клавиатура*. Можно открыть виртуальную клавиатуру из контекстного меню значка программы на панели задач (рис. 2.4), выбрав пункт *Инструменты* и далее *Виртуальная клавиатура*. Удобный способ открыть виртуальную клавиатуру – непосредственно из окна браузера, нажав на кнопку  *Виртуальная клавиатура* в панели инструментов браузера или набрав горячие клавиши *Ctrl+Alt+Shift+P*.

В ОС Windows 7 и Vista открыть виртуальную клавиатуру можно с помощью Kaspersky Gadget, выбрав соответствующую команду в панели управления развернутого варианта гаджета (рис. 2.10).

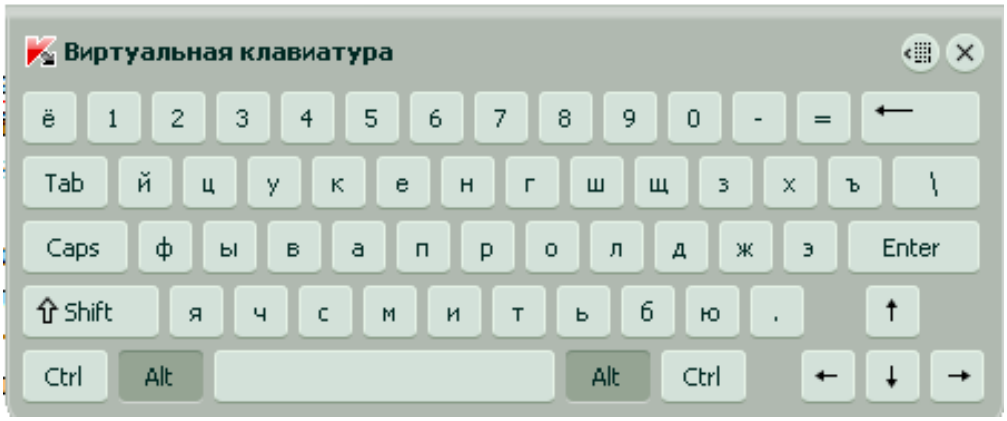


Рис. 2.13. Виртуальная клавиатура

После появления виртуальной клавиатуры (рис. 2.13) при необходимости можно открыть ее расширенный вариант, нажав на кнопку в правом верхнем углу клавиатуры. Далее можно вводить нужные данные, нажимая кнопки виртуальной клавиатуры.

Настройка антивируса

В процессе установки программы на ПК запускается мастер настройки приложения, который проводит первичную настройку параметров антивируса. При выборе варианта стандартной установки (флажок *Изменить параметры*

установки снят) программа полностью устанавливается на компьютер с рекомендуемыми параметрами защиты.

Впоследствии для проведения настроек программы нужно будет открыть окно настройки (рис. 2.14), для чего нажать кнопку *Настройка* в правой верхней части главного окна (рис. 2.5) либо выбрать одноименный пункт в контекстном меню значка приложения (рис. 2.4).

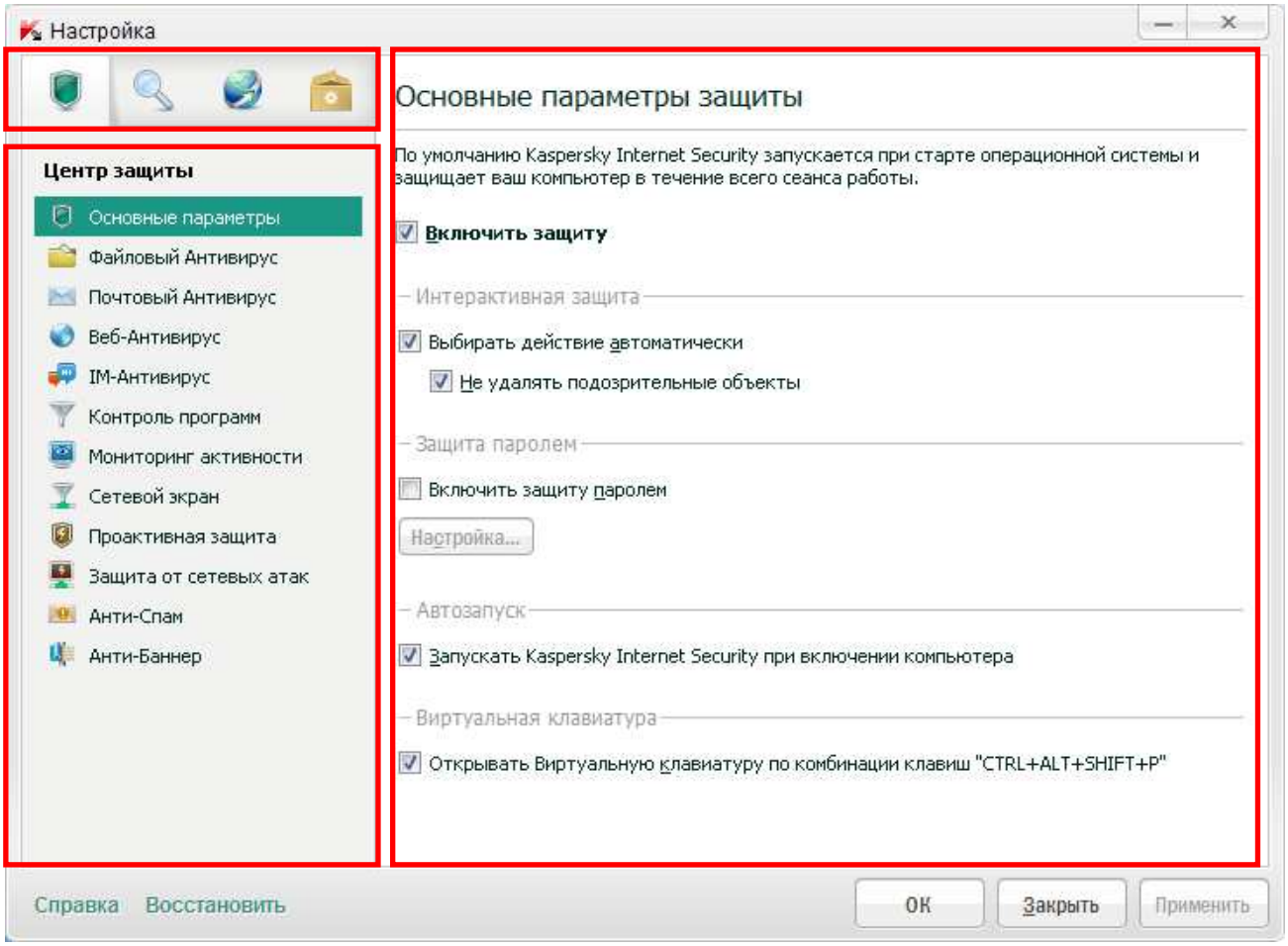


Рис. 2.14. Окно настройки параметров программы

Окно (рис. 2.14) предназначено для настройки параметров работы программы в целом, отдельных компонентов защиты, задач проверки и обновления. Окно настройки состоит из трех областей. В левой верхней области окна можно выбрать раздел настройки программы (рис. 2.15).

Рис. 2.15. Блок выбора раздела настройки программы

В левой области окна под разделами можно выбрать компонент программы, задачу или другую составляющую, соответствующую выбранному разделу, которую нужно настроить. В правой области окна содержатся элементы управления, с помощью которых можно настроить работу составляющей, выбранной в левой области окна.

Обновление антивируса

Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы. Информация об угрозах и способах их нейтрализации содержится в базах антивируса, поэтому регулярное обновление баз и программных модулей антивируса необходимо для обеспечения безопасности компьютера и своевременного обнаружения новых угроз. Для регулярного обновления требуется действительная лицензия на использование программы. При отсутствии лицензии выполнить обновление можно только один раз.

По умолчанию антивирус Касперского автоматически проверяет наличие обновлений на серверах обновлений. Для этого требуется только соединение с Интернетом. Если на сервере содержится набор последних обновлений, антивирус загружает и устанавливает их в фоновом режиме. Можно легко в любой момент самостоятельно запустить обновление антивируса, выбрав пункт *Обновление* в контекстном меню значка программы (рис. 2.4), или в нижней части главного окна (рис. 2.5), выбрав раздел *Обновление* в открывшемся окне, нажать на кнопку *Обновить*. В ОС Windows 7 и Vista можно запустить обновление с помощью Kaspersky Gadget, предварительно настроив его соответствующим образом. Будет запущено обновление антивирусных баз и программных модулей. В окне *Обновление* будет отображаться информация о текущем состоянии баз, дате последнего обновления и режиме запуска.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении этой задачи, записывается в отчет. Чтобы просмотреть отчет программы по процессу Обновления в главном окне программы (рис. 2.5), надо нажать на кнопку *Отчеты* и в открывшемся окне нажать кнопку *Подробный отчет*, далее в левой части окна *Подробный отчет* следует выбрать раздел *Обновление*. В правой части окна будет представлена информация обо всех процедурах обновления.

Аварийное восстановление операционной системы

В антивирусе Касперского реализован сервис создания диска аварийного восстановления. Такой диск предназначен для восстановления работоспособности системы после вирусной атаки, в результате которой повредились системные файлы операционной системы, ее первоначальная загрузка стала невоз-

можной, и систему нельзя вылечить другим способом (например, с помощью антивирусных программ).

Поэтому после установки антивируса Касперского и первой проверки компьютера рекомендуется создать диск аварийного восстановления. Такой диск предназначен лишь для того компьютера, на котором он был создан. Диск аварийного восстановления представляет собой программу Kaspersky Rescue Disk, записанную на съемный носитель (CD / DVD-диск или USB-устройство). При этом эффективность лечения повышается за счет того, что находящиеся в системе вредоносные программы не получают управления во время загрузки операционной системы.

Для создания диска надо в нижней части главного окна программы (рис. 2.5) выбрать команду *Инструменты*, в открывшемся окне (рис. 2.12) в блоке Kaspersky Rescue Disk нажать кнопку *Создать* и далее следовать указаниям мастера.

Чтобы воспользоваться созданным диском аварийного восстановления, надо предварительно в параметрах BIOS включить загрузку с CD / DVD-диска или USB-устройства, поместить в дисковод зараженного ПК CD / DVD-диск или подключить USB-устройство с предварительно записанной программой Kaspersky Rescue Disk и перезагрузить компьютер. Более подробную информацию об использовании диска аварийного восстановления можно найти в руководстве пользователя Kaspersky Rescue Disk.

Аналогичная программа от другого производителя – Dr.Web® LiveCD. Это тоже уникальный пакет для восстановления операционной системы после вирусной атаки. Если вредоносная программа сделала невозможной загрузку ПК под управлением Windows или Unix, то с помощью Dr.Web® LiveCD можно легко восстановить работоспособность системы: выявить и очистить ПК от инфицированных и подозрительных файлов, вылечить зараженные, но важные файлы, скопировать необходимую информацию на сменные носители.

Другая лечащая утилита – Dr.Web® LiveUSB – необходима в случае, если атака вирусных программ привела к сбою операционной системы. С помощью этой утилиты легко можно провести аварийное восстановление операционной системы с загрузочной USB-флешки.

Далее можно отметить загрузочный диск ESET NOD32 LiveCD с антивирусной утилитой для проверки системы на вирусы и их успешного удаления. Основное достоинство ESET NOD32 LiveCD заключается в том, что он работает независимо от операционной системы, в то же время имеет прямой доступ к диску и всей файловой системе. Благодаря этому возможно удалить то проникновение, которое обычно не может удалиться, когда операционная система работает или вообще уже не запускается.

Еще одна лечащая утилита – Avira Antivir Rescue System 10.02.12, которая позволяет создать загрузочный CD для восстановления системы, сканирования ее на предмет угроз или лечения уже зараженной системы. Существуют еще

много других аварийных лечащих программ, которые можно использовать в случае необходимости.

2.4. Выбор антивируса

Каждый пользователь персонального компьютера и Интернета, который недостаточно серьезно относится к вопросу безопасности, может легко потерять важную информацию. Именно поэтому вопросу выбора антивируса и его установке нужно уделять должное внимание. У пользователя, стоящего перед выбором подходящего ему антивирусного решения, если он желает себе поставить продукт, обеспечивающий хороший уровень защиты от компьютерных вредоносных программ, возникает проблема: как принять верное решение, какой же антивирус выбрать? Покупать лицензионную или установить бесплатную программу? На сегодняшний день на рынке антивирусов огромный выбор программ на любой вкус, однако никто не может выделить среди них абсолютного лидера. В любом случае выбор антивируса нужно делать самостоятельно, отталкиваясь от личных предпочтений, обращая внимание на различные тесты и советы квалифицированных специалистов.

Пробные версии антивирусов

Сегодня существуют практически у каждого производителя платных продуктов пробные версии антивирусов, которые дают превосходную возможность для обычного пользователя не покупать «кота в мешке», а сделать осознанный выбор в пользу того или иного антивируса. Пробная версия антивируса – это, как правило, обычный антивирус, лицензионный ключ у которого работает 30 дней. За это время можно узнать все возможности программы, посмотреть удобство работы, а также узнать эффективность защиты системы. Пробный антивирус легко удалить после окончания периода использования и установить для тестирования другой.

Например, пробная версия Антивируса Касперского имеет полнофункциональную версию и не имеет ограничений на функциональность программы. Поэтому, устанавливая ее на свой ПК, можно полностью познакомиться с возможностями программы. Похожим образом поступают и другие производители – предоставляют полноценный продукт, который просто ограничен во времени.

Большим плюсом демонстрационной версии является то, что если принято решение о покупке антивируса, у которого заканчивается пробный период, нет необходимости заново скачивать и переустанавливать программу. Вся история и антивирусная программа, настроенная под систему пользователя, будут продолжать работать как обычно, необходимо лишь приобрести и ввести лицензионный ключ.

Можно установить один пробный антивирус, а если не понравится, то через месяц скачать бесплатно без регистрации пробную версию антивируса от другого производителя и так далее. Например, можно выбирать из следующих версий антивирусов различных производителей: Norton AntiVirus 2012,

Kaspersky CRYSTAL, Kaspersky Internet Security 2012, Антивирус Касперского 2012, Panda Antivirus Pro 2012, Panda Internet Security 2012, PC Tools Spyware Doctor, ESET NOD32 Smart Security, ESET NOD32, IKARUS Antivirus virus.utilities, Dr Web Security Space Pro, Dr Web, AVG Internet Security 2012, AVG Anti-Virus 2012 и др. Таким образом, платных антивирусов очень много и, перебирая пробные их версии, можно найти лучший антивирус, который понравится.

Бесплатные антивирусы

Альтернативой платным антивирусам являются бесплатные программы. Если нет желания покупать лицензионный антивирус, то можно установить бесплатную антивирусную программу.

Производители антивирусных программ предлагают бесплатные версии своих продуктов, которые менее функциональны, чем их платные аналоги. Это делается по многим причинам, одна из главных – это продвижение и популяризация своего бренда среди пользователей. Некоторые бесплатные антивирусы защищают ПК не хуже коммерческих антивирусов от неизвестных или малоизвестных производителей. Как правило, для того чтобы бесплатный антивирус полноценно работал, необходима его регистрация. Обычно она заключается в заполнении регистрационной формы, с внесением своих контактных данных.

Также в некоторых бесплатных антивирусах встречается назойливая реклама, которая постоянно напоминает о необходимости купить платную версию программы.

Примерами бесплатных антивирусов являются следующие программы:

- *Microsoft Security Essentials* – новый антивирус от Microsoft предназначен для домашних пользователей и предприятий малого бизнеса, в которых установлено до 10 компьютеров только с лицензионной копией Windows. Программа не требует регистраций, имеет понятный интерфейс и обновляется автоматически.
- *Avira AntiVir Personal* – антивирусная программа, которая по функциональности может посоревноваться со многими платными продуктами. Этот антивирус ограждает компьютер как от вирусов и троянов, так и от шпионских программ, руткитов и мистификаторов. Поддерживает автоматическое обновление вирусных баз через Интернет и проводит постоянный мониторинг системы, отслеживая вирусную активность в Интернете. Антивирус имеет многоязычную поддержку (в том числе русский язык), не нагружает системные ресурсы компьютера, способен сканировать входящие и исходящие электронные письма на наличие вредоносных программ.
- *AVG Anti-Virus Free* – антивирусная программа, позволяющая обеспечить защиту компьютера в реальном времени. Данный антивирус отличается простотой использования и возможностью применения

как на ОС Windows XP, так и на более современных Windows Vista и Windows 7.

- *Avast! 4 Home Edition* – антивирус для домашнего пользования, который обеспечивает максимально возможную защиту компьютера. Данный антивирус обладает всеми достоинствами платных аналогов и является одной из самых популярных программ для защиты от вирусов и вредоносных программ.
- *NANO Антивирус* – совершенно новый высокотехнологичный антивирусный продукт, при разработке которого учтены все недостатки и достоинства подобных продуктов иных компаний, а также требования и пожелания пользователей к антивирусным программам.

Бесплатные утилиты-сканеры

В случае заражения компьютера можно воспользоваться бесплатными специальными средствами полной проверки компьютера, обнаружения и лечения от вирусов и других типов вредоносных программ. Эти утилиты предназначены для разового применения и только для лечения личного компьютера. При этом они могут работать одновременно с установленными антивирусными программами и других компаний. Обычно они загружаются в безопасном режиме работы ПК. Такие сканеры могут лечить системы, зараженные вирусами до такой степени, что невозможно запустить полноценный антивирус. Однако такие программы не являются заменой антивируса, они не предназначены для постоянной защиты компьютера. И в самих программах отсутствует функция обновления баз. Чтобы получить программу с актуальным набором баз, ее необходимо каждый раз скачивать с серверов производителей и устанавливать на компьютер, при этом предварительно удалив ранее установленную на ПК программу. Эти утилиты включают в себя только опцию проверки по требованию и не работают в режиме постоянной защиты. Обычно при скачивании бесплатной утилиты некоторые производители предлагают соглашаться с тем, что при сканировании ПК утилита отсылает в компанию статистические данные о ходе сканирования и программно-аппаратном обеспечении ПК. Данная информация помогает компании более точно анализировать глобальную вирусную обстановку и совершенствовать алгоритмы детектирования и лечения продуктов.

Примерами таких бесплатных утилит являются хорошо зарекомендовавшие себя программы Kaspersky Virus Removal Tool 2011, Dr.Web Cureit, VIPRE Rescue Scanner v.11491, а также недавно появившиеся NANO Антивирус Онлайн-сканер и др.

Если на компьютере установлен, например, Антивирус Касперского, – можно использовать утилиту Dr.Web, и наоборот. А если на ПК установлен другой антивирус или его нет вообще, можно взять любую из перечисленных утилит на выбор.

Никогда не устанавливайте новый антивирус, не удалив предшествующий. Одновременное присутствие двух или более антивирусных программ в системе может привести к невозможности загрузки компьютера.

Облачные антивирусы

Основная критика настольного антивирусного ПО часто заключается в том, что данное программное обеспечение слишком громоздкое и малоэффективное. Оно замедляет работу компьютера и требует от пользователя частых обновлений. В последнее время в антивирусной индустрии наметилась тенденция перехода на новые, более совершенные технологии защиты от вредоносного и нежелательного программного обеспечения. Предполагается, что в ближайшей перспективе растущее в геометрической прогрессии количество вредоносных приложений достигнет критической точки и приведет к тому, что любая использующая сигнатурный анализ антивирусная программа останется не у дел – слишком уж велико будет потребление вычислительных ресурсов пользовательского компьютера. Постоянно увеличивающееся количество угроз вынуждает антивирусные компании искать новые пути снижения ресурсоемкости своих приложений.

В поисках перспективных направлений борьбы с цифровой «нечистью» некоторые компании сделали ставку на так называемые *облачные вычисления* (cloud computing – клауд компьютинг), активно продвигаемые нынче на рынке под лозунгами "инновационный", "революционный" и т.д. Cloud computing – это способ обработки существующих данных, при которой мощности компьютеров позиционируются исключительно в качестве интернет-сервиса. Появилось поколение так называемых облачных приложений по обеспечению безопасности, которые имеют два основных преимущества перед настольными комплексами.

Идея, положенная в основу облачных антивирусных продуктов, состоит в том, что выделяются клиентская и серверная части cloud-антивируса. Первая часть (клиент) устанавливается на ПК пользователей, имеет минимальный размер, осуществляет сканирование данных и отправляет контрольные суммы подозрительных файлов на сервер. Дислоцированный в облаках сервер принимает от клиентов данные потенциально небезопасных программ, проверяет их с помощью базы сигнатур вирусов и выдает свой вердикт относительно чистоты той или иной программы. В случае обнаружения вредоносных программ сервер отсылает клиенту на зараженный компьютер необходимые сценарии устранения проблемы (соответствующие скрипты), выполнение которых очищает пользовательский ПК от обнаруженной «заразы». Подобная схема взаимодействия не только позволяет существенно снизить нагрузку на аппаратные ресурсы компьютера, но и освобождает пользователя от необходимости постоянно скачивать базы сигнатур, а также обеспечивает наилучшую защиту за счет

применения системы "коллективного разума", использующей полученную от многомиллионной аудитории информацию для автоматического обнаружения и классификации новых видов вредоносных программ.

Таким образом, основным преимуществом является то, что облачное антивирусное программное обеспечение устраняет необходимость выполнять частые обновления антивирусных баз. Ежедневное обновление быстро начинает раздражать, и многие пользователи отключают всплывающие сообщения в области уведомлений до тех пор, пока антивирусное ПО не становится слишком устаревшим для обеспечения защиты ПК. А так как настольные комплексы, как правило, не обновляются несколько раз в день, они не могут предложить такой же сиюминутный набор сигнатур угроз, как у облачных приложений по обеспечению безопасности. Теоретически вторым преимуществом является то, что облачные приложения для сканирования файлов используют ресурсы удаленных серверов вместо использования ресурсов локального компьютера. На компьютере пользователя будет работать облегченное приложение, которое будет передавать большую часть процесса обработки в облако и, таким образом, это должно повысить общую производительность настольной системы.

В большей или меньшей степени облачная архитектура применяется сегодня во многих антивирусных программных продуктах таких компаний-гигантов, как ESET, Лаборатория Касперского, F-Secure, Symantec, Agnitum, F-Secure, Alwil Software. Однако далеко не все разработчики решились целиком перевести свои продукты на облачную технологию. К числу пионеров можно причислить Panda Security, презентовавшую свой новый продукт Panda Cloud Antivirus, Immunet Protect от американских разработчиков Immunet и компанию Prevx.

На практике же пока что эффективность применения облачных антивирусных приложений постоянно зависит от скорости интернет-канала. Еще более серьезным недостатком облачной концепции является тенденция отправки на сервер персональных пользовательских данных. И хотя разработчики облачных антивирусов гарантируют абсолютную конфиденциальность и безопасность передаваемых пакетов данных, этот факт является самым большим препятствием на пути использования таких антивирусов в корпоративных сетях из-за боязни утечки информации. Кроме того, протестированные облачные антивирусы не смогли обойти своих настольных конкурентов. Например, облачные антивирусы Trend Micro Titanium Antivirus Plus 2011 и Panda Antivirus Pro 2011 обладают достойной защитой, но они не смогли заблокировать больше угроз, чем их настольный конкурент Norton Antivirus 2011. Также облачные антивирусы пока не могут обойти своих настольных конкурентов и по показателям производительности системы. Тем не менее, в ближайшие годы ожидается быстрое улучшение производительности и функциональных возможностей этих облачных приложений, особенно когда ведущие производите-

ли настольных антивирусных комплексов начнут перемещать свои приложения в облако.

2.5. Основные правила антивирусной безопасности ПК

Порой самые надежные и разумные меры не могут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ. Одним из основных методов борьбы с вирусами является своевременная профилактика. Компьютерная профилактика состоит из определенных правил, соблюдение которых позволяет значительно снизить вероятность заражения вирусом и степень возможного ущерба от потери каких-либо данных. Ниже перечислены основные правила антивирусной безопасности ПК:

- оснастите свой компьютер современной антивирусной программой, желательно лицензионной, например пакетом антивирусных программ Касперского, Doctor Web или ESET NOD32, обязательно постоянно обновляйте их версии и задавайте рекомендуемые параметры защиты ПК;
- осторожно относитесь к почтовым сообщениям – старайтесь не открывать почту от незнакомых адресатов, особенно если имя отправителя невразумительно; не открывайте письма с откровенно рекламным или непонятным заголовком;
- не открывайте ответы от адресатов, которым вы не писали – тема такого письма часто содержит «Re:». Не скачивайте и не открывайте файлы, вложенные в такие письма, независимо от их расширений (особенно если в письме говорится, что все инструкции или пояснения – в файле). Желательно иметь антивирусную утилиту, позволяющую проверять почтовые сообщения без их скачивания, а лучше – иметь почтовый ящик в Интернете, что позволяет просматривать почту без загрузки ее на свой компьютер;
- не отвечайте на электронные письма от любых адресатов, просящих уточнить номера ваших телефонов, счетов, паролей;
- отключайтесь от локальной сети и Интернет, когда они не используются;
- внимательно относитесь к выбору посещаемых интернет-ресурсов, остерегайтесь посещения хакерских и порносайтов – очень многие из них заражены опасными скрипт-вирусами или интернет-червями;
- не кликайте на баннеры, предлагающие бесплатный заработок, отличную работу, огромные скидки, предлагающие вступить в бесплатную игру;
- по возможности установите и наладьте сетевой экран – файервол;
- при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами, либо установите в настройках антивируса проверку содержимого архивов;

- проверяйте на присутствие вирусов все съемные диски (дискеты, CD/DVD, флеш-карты и пр.) перед их использованием; всегда проверяйте флеш-носители перед считыванием с них информации, записанной на других ПК, запуская антивирусные программы своего компьютера;
- всегда защищайте свои флеш-носители от записи при работе на других компьютерах, если на них не будет производиться запись информации;
- своевременно делайте архивные копии ценной информации на других носителях;
- обязательно создайте диск аварийного восстановления, с которого при необходимости можно будет загрузить ПК, используя «чистую» операционную систему;
- регулярно просматривайте список установленных на компьютере программ для своевременного обнаружения программного обеспечения, которое было установлено на компьютере без разрешения пользователя;
- используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
- внимательно относитесь к информации от производителей антивирусной продукции – зачастую они заблаговременно сообщают о начале новой эпидемии;
- регулярно устанавливайте обновления операционной системы;
- покупайте дистрибутивные копии программного обеспечения только у официальных продавцов;
- ограничьте круг людей, допущенных к работе на вашем компьютере;
- если обнаружены один или несколько перечисленных в разд. 2.1 симптомов заражения, отключите компьютер от Интернета или, если компьютер подключен к локальной сети, отключите его от сети и проведите полную антивирусную проверку компьютера;
- если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивируса, которые часто предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей;
- если возникли проблемы с удалением вредоносных файлов, проверьте, нет ли на сайте производителя антивируса информации о специальных утилитах, необходимых для удаления конкретной вредоносной программы;
- если необходимо, обратитесь за помощью в службу технической поддержки производителя антивируса, установленного на компьютере.

Соблюдение этих мер поможет вам сберечь информацию вашего ПК и минимизировать время и усилия на восстановление работоспособности компьютера.

Вопросы для самоконтроля

1. Перечислите, какие проблемы возникают в связи с преступлениями, направленными против информационной безопасности?
2. Что такое компьютерные вирусы?
3. Каковы причины создания компьютерных вирусов?
4. Дайте краткую характеристику категориям создателей вредоносных программ.
5. Перечислите явные и косвенные признаки проявления вирусов.
6. Перечислите источники распространения вирусов.
7. Файлы каких форматов чаще всего поражаются вирусами?
8. На какие категории разделяют вредоносные объекты?
9. Дайте краткую характеристику категориям компьютерных вирусов.
10. Перечислите типы антивирусных программных средств.
11. Приведите пример комплексных антивирусных программных пакетов.
12. Дайте краткую характеристику следующим антивирусным программным продуктам: бесплатные версии антивирусов, утилиты-сканеры, дозагрузочные утилиты-сканеры.
13. Дайте краткую характеристику антивирусной защите «монитор».
14. Дайте краткую характеристику антивирусной защите «сканер».
15. Дайте краткую характеристику антивирусной защите «файервол».
16. Перечислите, какие современные версии программ предлагает Лаборатория Касперского для домашнего ПК.
17. Перечислите основные компоненты Антивируса Касперского, предназначенные для защиты ПК, и дайте им краткую характеристику.
18. Что такое проактивная защита?
19. Что такое *Безопасная среда* в антивирусе Касперского?

20. Что такое *Защита из облака*?
21. Что такое и для чего предназначен *Kaspersky Gadget*?
22. Поясните, какие задачи включены в состав антивируса Касперского для поиска вирусов.
23. Поясните, в чем заключается задача проверки репутации программ в антивирусе Касперского.
24. Поясните, в чем заключается задача восстановления после заражения.
25. Поясните, какую задачу решает *мастер устранения следов активности*.
26. Поясните, для чего нужна виртуальная клавиатура.
27. Поясните, для чего нужно обновление антивируса.
28. Поясните, в чем заключается задача аварийного восстановления операционной системы.
29. Поясните, что дают *Пробные версии антивирусов* для обычного пользователя.
30. Приведите примеры бесплатных антивирусов, поясните их достоинства и недостатки.
31. Приведите примеры бесплатных утилит-сканеров, поясните их назначение.
32. Поясните, допускается ли одновременное присутствие двух или более антивирусных программ в системе?
33. Перечислите основные правила антивирусной безопасности ПК.

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ

К главе «Архиваторы»

Архивация (упаковка) – помещение (загрузка) исходных файлов в архивный файл в сжатом или несжатом виде.

Архивный файл или **архив** – это специальным образом организованный файл, содержащий в себе один или несколько файлов в сжатом или несжатом и/или зашифрованном виде и служебную информацию об именах файлов, дате и времени их создания или модификации, размерах и т.п.

Добавление (и замена) файлов – копирование указанных файлов в архив, оставляя их в своей папке (т.е. получается две копии для каждого файла – исходная и упакованная).

Многотомные архивы – это обычно большие по объему архивные файлы, разбитые на несколько частей, которые называются *томами*. Создавая архив из нескольких частей, можно копировать и хранить его части на нескольких носителях.

Непрерывный архив – это специальный метод архивирования файлов, при котором данные упаковываются в виде непрерывного потока. Метод позволяет существенно увеличить коэффициент сжатия, если в архив помещается много небольших файлов одинакового формата.

Обновление (и добавление) файлов – копирование указанных файлов в архив, но при этом добавляются в архив файлы, которых ранее не было в этом архиве.

Обновление существующих файлов – обновляются уже имеющиеся в архиве файлы на их более новые варианты (сравниваются время и даты создания файлов).

Перемещение (и замена) файлов – копирование указанных файлов в архив, но после добавления в архив их исходные копии удаляются с диска.

Разархивация (распаковка) – процесс восстановления файлов из архива точно в таком виде, какой они имели до загрузки в архив.

Самораспаковывающийся архивный файл (*SFX-архив*) – это загрузочный, исполняемый модуль, который способен к самостоятельной разархивации находящихся в нем файлов без использования программы-архиватора.

Сжатие – это специальный метод кодирования данных с целью уменьшения их размера. Точнее, сжатие информации — это процесс преобразования информации, хранящейся в файле, к виду, при котором уменьшается избыточность в ее представлении и, соответственно, требуется меньший объем памяти для хранения.

Степень сжатия файлов – характеризуется коэффициентом *Кс*, определяемым как отношение объема сжатого файла *Vc* к объему исходного файла, *Vo*, выраженное в процентах.

Тестирование архива – проверка архива на целостность и отсутствие ошибок.

Том — это фрагмент архива, состоящего из нескольких частей. Обычно тома используются для сохранения большого архива на нескольких сменных носителях.

Шифрование имен файлов – шифруются не только данные файлов, но и другие важные области архива: имена файлов, размеры, атрибуты, комментарии и другие блоки. Зашифрованный в таком режиме архив нельзя без пароля не только распаковать, но даже просмотреть список находящихся в нём файлов.

К главе «Компьютерные вирусы и методы защиты от них»

Антивирусная программа (Anti-virus program) – программа поиска, диагностики, профилактики и лечения файлов, зараженных компьютерным вирусом. В процессе поиска и диагностики определяются зараженные файлы и тип вируса. Профилактика позволяет предотвращать заражение. Лечение подразумевает удаление вируса и восстановление поврежденных файлов.

Анти-антивирусный вирус (Anti-antivirus Virus, Retrovirus) – компьютерная вирусная программа, объектом нападения которой являются антивирусные программы.

Антивирусный сканер (Anti-virus scanner) – программа, способная обнаруживать программный код вирусов (сигнатуру) в зараженных ими файлах при помощи базы данных о вирусах, известных такой антивирусной программе, или исходя из априорных предпосылок об устройстве такого кода. Сканеры периодически, например, по запросу пользователя, проверяют определенные объекты (диски, каталоги или файлы, а также оперативную память и загрузочные секторы) на наличие программного кода.

Аплеты (applets) – прикладные программы, небольшие Java-приложения, встраиваемые в HTML страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях. Особенно аплеты опасны для любителей онлайновых игр, т.к. в них аплеты Java требуются обязательно. Аплеты, как и шпионское ПО, могут использоваться для отправки собранной на компьютере информации третьей стороне.

Атаки методом подбора пароля (Brute force attacks) – так называемые атаки методом «грубой силы». Как правило, пользователи применяют простейшие пароли, например "123", "admin" и т.д. Этим и пользуются компьютерные злоумышленники, которые при помощи специальных троянских программ вычисляют необходимый для проникновения в сеть пароль методом подбора – на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.

База данных антивирусной программы, вирусная база (Anti-virus program virus database) – содержит информацию о фрагментах кода (сигнатурах) известных данной антивирусной программе вирусов, а также необходимые

сведения для восстановления (излечения) пораженных этими вирусами объектов. Для современных компьютерных вирусов характерна огромная скорость распространения. В течение нескольких дней, а иногда и часов, вновь появившийся вирус может заразить миллионы компьютеров по всему миру. Разработчики антивирусного комплекса непрерывно пополняют вирусные базы новыми вирусными записями (сигнатурами). После установки таких дополнений антивирусный комплекс делается способным обнаруживать новые вирусы, блокировать их распространение, а в ряде случаев – лечить зараженные файлы.

Веб-жучки (Web bugs) – средство слежения за пользователями сети Интернет. Представляют собой прозрачные, размером 1x1 пиксель графические файлы, используемые для сбора статистической информации о заходящем на сайт пользователе, которая может включать дату и время просмотра, тип браузера, данные монитора, настройки JavaScript, cookie, адрес в сети Интернет. Такие жучки используют и спамеры, включая их в рассылаемые письма, что дает им возможность определять, существует или нет в действительности такой адрес.

Вирусная программа-червь (Worm-virus) – паразитическая программа, обладающая механизмом саморазмножения. Программа способна размножать свои копии, но не поражать другие компьютерные программы. Проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через сеть Интернет) и рассылает свои функциональные копии на другие компьютерные сети.

Вирусный код, сигнатура (Signature) – система символов и однозначных правил их интерпретации, используемая для предоставления информации в виде данных. Представляет собой набор символов или последовательность байтов, которые, как предполагается, могут быть свойственны, а следовательно, и обнаружены в каком-то определенном вирусе, в каждой его копии, и только в нем. Антивирусные сканеры используют сигнатуру для нахождения вирусов. Полиморфные вирусы не имеют сигнатуры.

Вирусный мистификатор (Hoax) – не являющееся вирусом почтовое сообщение. На компьютер пользователя мистификация приходит в виде письма, написанного в подчеркнуто нейтральном тоне, в котором, например, может указываться на якобы распространяющийся новый вирус. Большинство вирусных мистификаций обладают следующими особенностями. Имя вируса, на которое ссылается автор сообщения, составляется не по правилам, используемым большинством антивирусных компаний. Особо отмечается, что «вирус» пока не обнаруживается антивирусными программами. Пользователю предлагается найти некий файл с помощью поискового средства ОС Windows и удалить его с диска. В письме содержится призыв в случае обнаружения указанного файла сообщить об этом всем своим знакомым и всем тем, чьи адреса есть в адресной книге пользователя. Несмотря на всю безобидность подобного розыгрыша опасность его очевидна – массовая рассылка копий этого бесполезного сообщения загружает почтовый трафик и отнимает время пользователей.

Вирусы-спутники, вирусы-компаньоны (Virus-companion) – формально являются файловыми вирусами. Не внедряются в исполняемые программы. Такие вирусы используют особенность системы DOS, позволяющую программному файлу с тем же названием, но другим расширением действовать с разными приоритетами. Под приоритетом понимают присваиваемый задаче, программе или операции признак, определяющий очередность их выполнения вычислительной системой. Большинство таких вирусов создают .COM файл, который обладает более высоким приоритетом, нежели .EXE файлы с тем же самым названием. При запуске файла по имени (без указания расширения) будет запущен файл с расширением .COM. Такие вирусы могут быть резидентными и маскировать файлы-двойники.

Вишинг (Vishing) – технология интернет-мошенничества, разновидность фишинга, заключающаяся в использовании в злонамеренных целях «war diallers» (автонабирателей) и возможностей Интернет-телефонии (VoIP) для кражи личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. Потенциальные жертвы получают телефонные звонки, якобы от имени легальных организаций, в которых их просят ввести с клавиатуры телефона, смартфона или КПК пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

Вредоносные действия вирусов (Damage). На компьютере пользователя вирусы могут производить следующие вредоносные действия:

- вызывать отказ в выполнении той или иной функции в работе системы, инициировать ошибки и сбои, вызывать зависание системы сразу после ее загрузки;
- выполнять действия, не предусмотренные программой;
- разрушать файлы, диски (форматировать диски, удалять файлы);
- выдавать на экран дисплея раздражающие пользователя ложные сообщения;
- создавать звуковые или визуальные эффекты (падающие буквы, проигрывание мелодии и т.д.);
- блокировать доступ к системным ресурсам (разрастание зараженных файлов за счет их многократного повторного заражения, замедление работы компьютера и т.д.);
- имитировать сбои аппаратуры (перевод части кластеров в «псевдосбойные»).

Следует отметить, что наиболее опасны не катастрофические повреждения винчестера или дискет, а мелкие, незаметные изменения файлов данных.

Всплывающие окна (pop-ups) – не вредоносные программы, вид рекламного ПО, имеющие вид внезапно возникающих на экране монитора рекламных окошек маленького формата.

«Горшочки с медом» (honey pots) – страницы-приманки, по описанию ресурса в поисковике и ключевым словам отвечающие требованиям поиска, но которые, на самом деле, только завлекают пользователя, а реально содержат на своих страницах всевозможные программы-эксплойты и различный нежелательный или вредоносный софт.

DoS-атаки (DoS-attacks) – или атаки на отказ в обслуживании. Популярный у злоумышленников вид сетевых атак, граничащий с терроризмом, заключающийся в посылке огромного числа запросов с требованием услуги на атакуемый сервер с целью выведения его из строя. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера), последний не справляется с такими запросами, что приводит к отказу в обслуживании. Как правило, такой атаке предшествует спуфинг. DoS-атаки стали широко используемым средством запугивания и шантажа конкурентов.

Деструктивное действие вируса (Destructiveness) – стратегия его функционирования, предпринимаемые им, подчас незаметные для пользователя, вредоносные действия, направленные на нарушение нормального функционирования операционной системы, а иногда ее полного краха, а также условия, при которых вирус вступает в фазу своего проявления и его алгоритм работы в ней.

«Дикая природа» («Wild») – компьютерная среда. Выражение «вирус» в «дикой природе» означает, что такой вирус вызвал инфицирование компьютеров или сайтов вне стен антивирусной лаборатории. Список «диких вирусов», составленный специалистом по вирусам Joe Wells, содержит перечень наиболее часто встречающихся вирусов в компьютерах во всем мире.

Дифейсмент (Defacement) – искажение веб-страниц. Вид компьютерного вандализма, иногда являющийся для хакера забавой, а иногда средством выражения политических пристрастий. Искажения могут производиться в какой-то части сайта или выражаться в полной замене существующих на сайте страниц (чаще всего, стартовой).

Дозвонщики (Dialers) – специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон жертве или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

«Дроппер» (Dropper) – файл-носитель, устанавливающий вирус в систему. Техника, иногда используемая вирусописателями для «прикрытия» вирусов от антивирусных программ.

Зомби (Zombies) – маленькие компьютерные программы, разносимые по сети Интернет компьютерными червями. Программы-зомби устанавливают себя в пораженной системе и ждут дальнейших команд к действию.

Зоологический вирус (Zoo virus) – вирус, который существует только в антивирусных лабораториях, в коллекциях исследователей вирусов и не встречается в «дикой природе».

IRC – вирусные программы-черви, которые распространяются, используя среду Internet Relayed Chat channels.

Исполняемый файл (Executable file) – файл, готовый к выполнению операционной системой. Например, в операционной системе MS DOS исполняемые файлы имеют расширения .exe, .com и .bat. Файлы с расширением .exe, .com – это программы. Файлы с расширением .bat – это пакетные файлы.

Клавиатурные перехватчики (Keyloggers) – вид троянских программ, основной функцией которых является перехват данных, вводимых пользователем через клавиатуру. Объектами похищения являются персональные и сетевые пароли доступа, логины, данные кредитных карт и другая персональная информация.

Компьютерные вирусы (Computer viruses) – это программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере – создавать или удалять объекты, модифицировать файлы данных или программные файлы, осуществлять действия по собственному распространению по локальным вычислительным сетям или по сети Интернет. Модификация программных файлов, файлов данных или загрузочных секторов дисков таким образом, что последние сами становятся носителями вирусного кода и, в свою очередь, могут осуществлять вышеперечисленные операции, называется заражением (инфицированием) и является важнейшей функцией компьютерных вирусов. В зависимости от типов заражаемых объектов выделяются различные типы вирусов.

Компьютерные вирусы являются высокоспециализированными программами и сильно зависят от среды своего функционирования. Используемая операционная система является наиболее важной характеристикой среды распространения вируса.

Логические бомбы (Logic bombs) – вид троянского коня – скрытые модули, встроенные в ранее разработанную и широко используемую программу. Являются средством компьютерного саботажа. Такой модуль является безвредным до определенного события, при наступлении которого он срабатывает (нажатие пользователем определенных кнопок клавиатуры, изменение в файле или наступление определенной даты или времени).

Люки (Backdoors) – программы, обеспечивающие вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода существующей системы безопасности. Люки не инфицируют файлы, но прописывают себя в реестр, модифицируя, таким образом, ключи реестра.

Макро-вирусы для MS Office – эти вирусы используют особенности форматов файлов и встроенные макроязыки приложений MS Office.

MtE вирусы (MtE viruses) – полиморфные вирусы, созданные с помощью генератора полиморфизма MtE (Mutant Engine). Такой генератор представляет собой специальный алгоритм, который отвечает за функции шифровки/расшифровки и генерацию расшифровщиков и присоединяется к любому объектному коду вируса. Такой расшифровщик не имеет ни одного постоянного бита, длина его всегда разная.

Пакетный файл (то же, что командный файл) (Batch file) – исполняемый файл, содержащий команды операционной системы. Обычно имеет расширение .bat и представляет собой текстовый файл, каждая строка которого – команда операционной системы. Выполняется командным процессором.

Перехватчики страниц (highjackers) – от английского highjack – «захватывать», вид нежелательной компьютерной программы, целью написания которой является принудительная установка нужной ее заказчику страницы в качестве стартовой на компьютере, в который смог проникнуть такой троянец. Программы используют бреши в системе безопасности Интернет-браузеров и прописывают себя в системный реестр. Как правило, ручная чистка реестра не помогает, так как такие троянцы имеют функцию восстановления нужных им данных в реестре и средства маскировки под системные файлы. Использование таких программ практикуется владельцами массово посещаемых сайтов – музыкальных, игровых, сайтов для взрослых.

Подключаемый модуль (Plug-in) – вспомогательная программа, выполняющая дополнительные функции в главной прикладной программе.

Полиморфизм (Polymorphism) – технология, посредством которой вирус изменяет свой код таким образом, чтобы разные экземпляры одного и того же вируса различались, а в идеале – не совпадали ни в одном байте.

Полиморфные вирусы (Polymorphic viruses) – или вирусы с самомодифицирующимися расшифровщиками (по Н. Н. Безрукову) – вирусы, использующие помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у него байтовых сигнатур. Расшифровщик не является постоянным – он уникален для каждого экземпляра вируса.

Почтовые бомбы (Mail bombs) – один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение либо множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя. В антивирусных продуктах Dr.Web для почтовых серверов предусмотрен специальный механизм защиты от таких атак.

Ревизор (Revisor) – программа, периодически проверяющая изменения в потенциально заражаемых файлах, сверяя части системы с эталонными. Ревизор сначала сохраняет контрольные суммы контролируемых файлов и секторов, а впоследствии проверяет соответствие эталонных и текущих значений контрольных сумм. Срабатывает в момент несовпадения (вследствие проникновения вируса). Позволяет выявить вирусную активность после заражения и в ряде

случаев восстановить состояние файлов до заражения. Ревизор не в состоянии определить, в результате чего изменилась программа – ее поразил вирус или просто перетранслировали.

Реестр (Registry) – иерархическая база данных, в которой операционная система централизованным образом хранит всю системную информацию, в частности, конфигурацию вычислительной системы, значения различных параметров, сведения об установленных программах и т.д. Изменения в реестре производятся пользователем в окне редактирования реестра. Настоятельно рекомендуется перед внесением каких-либо изменений в реестр сделать его резервную копию. Некорректные изменения в реестре могут привести к полной потере данных или повреждению файлов!

Резервная копия (Backup copy) – запасная копия содержимого диска, программы, файла, документа, создаваемая для использования в случае повреждения оригинала.

Резидентный (в памяти) вирус (Memory resident virus) – постоянно присутствующий в памяти вирус, написанный, как правило, на языке Ассемблер или Си. Такие вирусы обладают возможностью более эффективно заражать программы и противодействовать антивирусным средствам. Занимает небольшой объем памяти. Пребывает в состоянии готовности к продолжению выполнения своей задачи до выгрузки, перезагрузки или выключения компьютера. Активизируется и выполняет заданные вирусописателем действия, например, при достижении компьютером определенного состояния (срабатывания таймера и др.). Все бутовые вирусы резидентны.

Руткит (Rootkit) – вредоносная программа, предназначенная для перехвата системных функций операционной системы (API) с целью сокрытия своего присутствия в системе. Кроме того, Rootkit может маскировать процессы других программ, различные ключи реестра, папки, файлы. Rootkit распространяются как самостоятельные программы, а также как дополнительные компоненты в составе иных вредоносных программ – программ-люков (backdoor), почтовых червей и проч. По принципу своей работы Rootkit условно разделяют на две группы: User Mode Rootkits (UMR) – т.н. Rootkit, работающие в режиме пользователя, и Kernel Mode Rootkit (KMR) – т.н. Rootkit, работающие в режиме ядра. Работа UMR базируется на перехвате функций библиотек пользовательского режима, а работа KMR базируется на установке в систему драйвера, который осуществляет перехват функций на уровне системного ядра, что значительно усложняет его обнаружение и обезвреживание.

Silly-вирусы. Вирусы, которые не обладают никакими особенными характеристиками (такими как текстовые строки, специальные эффекты и т.д.), вследствие чего нет возможности присвоить таким вирусам особенные названия.

Системный файл (System file) – файл, содержащий один из модулей операционной системы или набор данных, которые она использует.

Скамминг (Scamming) – от английского «scamming», что означает «жульничество», вид интернет-мошенничества. Заключается в привлечении клиентов, якобы брачными агентствами (на самом деле скам-агентствами), с целью выуживания у них денег брачными аферами.

Скрипт, сценарий (Script) – программа, особый вид программного кода, как правило, написанная на интерпретируемом (не компилируемом) языке и содержащая команды-инструкции.

Скрипт-вирусы (Script virus) – вирусы, написанные на языках Visual Basic, Basic Script, Java Script, Jscript. На компьютер пользователя такие вирусы чаще всего проникают в виде почтовых сообщений, содержащих во вложениях файлы-сценарии. Программы на языках Visual Basic и Java Script могут располагаться как в отдельных файлах, так и встраиваться в HTML-документ и в таком случае интерпретироваться браузером, причем не только с удаленного сервера, но и с локального диска.

Скрытый файл (Hidden file) – файл, имя которого согласно политике безопасности не отражается в списке файлов каталога. Для этого он снабжается специальным знаком.

Сниффинг (Sniffing) – вид сетевой атаки, также называется «пассивное прослушивание сети». Несанкционированное прослушивание сети и наблюдение за данными производятся при помощи специальной не вредоносной программы – пакетного сниффера, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение. Перехваченные таким сниффером данные могут быть использованы злоумышленниками для легального проникновения в сеть на правах фальшивого пользователя.

Спуфинг (Spoofing) – вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения. Используется для обхода систем управления доступом на основе IP-адресов, а также для набирающей сейчас обороты маскировки ложных сайтов под их легальных двойников или просто под законные бизнесы.

Стелс вирусы (Stealth virus) – вирусные программы, предпринимающие специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в зараженных объектах. Так называемая стелс-технология может включать в себя:

затруднение обнаружения вируса в оперативной памяти;

затруднение трассировки и дезассемблирования вируса;

маскировку процесса заражения;

затруднение обнаружения вируса в зараженной программе и загрузочном секторе.

Сторож (Guard) – резидентная программа, контролирующая части операционной системы, потенциально открытые для проникновения вирусов, и срабатывающая в момент такого проникновения. Сторож обнаруживает и блокирует попытки заражения файлов. При этом также обнаруживаются программы, пытавшиеся совершить подозрительное действие, вероятно, зараженные каким-

либо вирусом. Обычно антивирусный резидентный сторож (монитор) контролирует в режиме реального времени все обращения к файлам, выявляет и блокирует подозрительные действия программ. Подозрительные программы могут быть на «лету» проверены с использованием общей для всего пакета вирусной базы и общего алгоритма сканирования. Заведомо зараженные файлы могут быть немедленно вылечены.

Технологии социальной инженерии – способы получения конфиденциальной информации у пользователей путем введения их в заблуждение. Очень часто это приводит к добровольной выдаче самими пользователями такой информации. Социальная инженерия не использует специальных компьютерных программ, мошенничество построено на тривиальном обмане, использовании доверчивости и наивности людей. Чаще всего рассылаются правдоподобно выглядящие письма от реально существующих кредитных организаций, в которых Вас просят подтвердить пароль доступа к счету и PIN- код кредитной карточки.

Типы вирусов. В зависимости от видов заражаемых объектов, компьютерные вирусы классифицируют по следующим типам:

Файловые вирусы (File viruses) – вирусы, заражающие двоичные файлы (в основном, исполняемые файлы и динамические библиотеки). Чаще всего, такие файлы имеют расширение **.EXE, .COM, .DLL, .SYS**. Также могут инфицировать файлы с расширениями **.DRV, .BIN, .OVL** и **.OVY**. Такие вирусы внедряются в файлы операционной системы, активируются при запуске пораженной программы и затем распространяются.

Загрузочные (бутовые) вирусы (Boot viruses) – вирусы, которые заражают загрузочные записи (Boot record) дискет, разделов жестких дисков, а также MBR (Master Boot Record) жестких дисков.

Макрокомандные вирусы (макровирусы) (Macroviruses) – вирусы, заражающие файлы документов, используемые приложениями Microsoft Office и другими программами, допускающие наличие макрокоманд (чаще всего на языке Visual Basic). Благоприятным фактором распространения вируса служит то, что все основные компоненты Microsoft Office могут содержать встроенные программы (макросы) на полнофункциональном языке программирования, а в Microsoft Word эти макросы автоматически запускаются при открытии любого документа, его закрытии, сохранении и т.д. Кроме того, имеется так называемый общий шаблон NORMAL.DOT и макросы, помещенные в общий шаблон, автоматически запускаются при открытии любого документа. Учитывая то, что копирование макросов из документа в документ (в частности, в общий шаблон) выполняется всего одной командой, среда Microsoft Word идеальна для существования макрокомандных вирусов.

Троянский конь (Троянец) (Trojan Horse) – вирусная программа, содержащая скрытый модуль, осуществляющий несанкционированные пользователем действия в компьютере. Эти действия не обязательно будут разрушительными, но всегда направлены во вред пользователю. Название этого типа атак происходит от известной легенды о деревянной статуе коня, использованной

греками для проникновения в Трою. Троянские программы-вандалы подменяют какую-либо из часто запускаемых программ, выполняют ее функции или имитируют такое исполнение, производя, вместе с тем, какие-либо вредоносные действия (стирают файлы, разрушают каталоги, форматируют диски, отсылают пароли или другую конфиденциальную информацию, хранящуюся на ПК пользователя). Некоторые троянские программы содержат механизм обновления своих компонент из сети Интернет. **PWS** – троянский конь, который ворует пароли. Как правило, префикс такой вирусной программы дополняется словом «Trojan» – «Trojan.PWS». **Backdoor** – вирусная троянская программа, которая содержит в себе RAT-функцию (RAT – Remote Administration Tool – утилита удаленного администрирования).

Утилиты удаленного администрирования – не вредоносные программы, которые могут использоваться во вредоносных целях. Позволяют осуществлять доступ в сеть и проводить в ней действия на расстоянии – из любой точки сети Интернет.

Уязвимость (Vulnerability) – часть программного кода, позволяющая использовать его для нарушения работы системы и проникновения в сети. Сегодня прогресс в скорости применения уязвимостей достиг таких высот, что временной интервал между публикацией данных об обнаружении «дыры» и изобретением злоумышленниками средств проникновения в систему через такую уязвимость исчисляется всего несколькими днями. Особенно «популярны» у хакеров и вирусописателей многочисленные уязвимости в самом распространенном в мире ПО корпорации Microsoft.

Файлы cookies – файлы с данными о пользователе, собираемые веб-серверами и хранящиеся на жестком диске компьютера. При посещении любого веб-сервера в специальных файлах, называемых cookie, сохраняется информация о предпочтениях посетителя ресурса, которая служит средством идентификации пользователя сервером. Данные, полученные из файлов cookie, используются спамерами для составления списков рассылок. Сбор информации в файлы cookie можно отключить в Internet Explorer через панель меню Сервис/Свойства обозревателя/Дополнительно.

Фарминг – сравнительно новый вид интернет-мошенничества. Фарминг-технологии позволяют изменять DNS (Domain Name System) записи либо записи в файле HOSTS. При посещении пользователем легитимной, с его точки зрения, страницы производится перенаправление на поддельную страницу, созданную для сбора конфиденциальной информации. Чаще всего такие страницы подменяют страницы банков – как оффлайновых, так и онлайновых.

Фишинг (Phishing) – технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма, якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками "сайт" такого учреждения и подтвердить паро-

ли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

Форматы файлов, чаще всего поражаемые вирусами (Target file formats):

.bat – пакетный файл;

.com – командный файл, вид исполняемого файла, размер которого не может превышать 64 Кб;

.dll – файл библиотеки динамической компоновки;

.elf – исполняемый файл в операционных системах Linux/UNIX;

.exe – исполняемый файл;

.ini – конфигурационный файл;

.sys – системный файл.

«Шароварный софт» (Shareware soft) – бесплатно распространяемое программное обеспечение, но предполагающее оплату его автору. Если после пробного просмотра пользователь не желает пользоваться данным программным обеспечением, он обязан его удалить. Использование «шароварного софта» без оплаты автору считается пиратством.

Шифрованные вирусы (Encrypted viruses) – вирусы, которые сами шифруют свой код для затруднения их дизассемблирования и обнаружения в файле, памяти или секторе. Каждый экземпляр такого вируса будет содержать только короткий общий фрагмент, процедуру расшифровки которого можно выбрать в качестве сигнатуры. В случае каждого инфицирования он автоматически зашифровывает себя, и каждый раз по-разному. Таким способом вирус пытается избежать обнаружения антивирусными программами.

Шпионские модули-роботы (spybots) – не являющиеся вирусами программы, самостоятельные функциональные модули, автономно решающие ту или иную задачу. Используются хакерами для слежения за жизнедеятельностью сети.

Шпионское ПО (spyware) – опасные для пользователя программы (не вирусы), предназначенные для слежения за системой и отсылки собранной информации третьей стороне – создателю или заказчику такой программы. Среди заказчиков шпионского ПО – спамеры, рекламщики, маркетинговые агентства, скам-агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы «интересуют» системные данные, тип браузера, посещаемые веб-узлы, иногда и содержимое файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-нибудь «шароварным» софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты

от присутствия шпионского ПО на компьютере – нестабильная работа браузера и замедление производительности системы.

Эвристический анализатор (эвристик) (Heuristic) – компонент антивирусной программы, который позволяет обнаруживать новые и неизвестные ранее вирусы. Эвристик анализирует как файлы, так и загрузочные сектора дисков. При эвристическом анализе осуществляется проверка исполняемого кода в исследуемом объекте и делается попытка выявить присутствие характерных для вирусов функций. Если эвристик находит подозрительный код, пользователю выдается сообщение о возможном инфицировании объекта неизвестным вирусом с указанием категории, к которой этот код относится.

HLL (High Level Language) вирусы – вирусы, написанные на языках программирования высокого уровня, таких как C, C++, Pascal, Basic и другие. В некоторых случаях вирусный код компилированных HLL-вирусов сжимают с использованием различных утилит уплотнения (PKLITE, LZEXE, DIET и др).

В группе HLL-вирусов выделяют несколько классов:

HLLC (High Level Language Companion) – вирус-компаньон, написанный на языке программирования высокого уровня. Такой вирус использует алгоритм инфицирования, который базируется на манипулировании именами файлов в файловой системе. Обычно HLLC-вирус переименовывает оригиналы исполняемых файлов (или перемещает их в другие директории), а затем использует названия оригинальных исполняемых файлов для создания на их месте вирусной копии.

HLLO (High Level Language Overwriting) – перезаписывающий вирус, написанный на языке программирования высокого уровня. HLLO-вирус перезаписывает данные файла-жертвы.

HLLP (High Level Language Parasitic) – паразитический вирус, написанный на языке программирования высокого уровня. HLLP-вирус поражает исполняемые файлы, не повреждая оригинальные данные файла-жертвы.

HLLW (High Level Language Worm) – вирусная программа-червь, написанная на языке программирования высокого уровня. Для распространения эти вирусы не нуждаются в хост-файле, а копируют себя в системные директории.

HLLM (High Level Language MassMailing Worm) – вирусные программы-черви массовой рассылки, написанные на языке программирования высокого уровня.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основные источники

1. Кирвас В. А. Информатика. Модуль 1 «Операционная система Windows и сервисные программы»: практикум для студентов фак. «Референт-переводчик», обучающихся по направлению подготовки 6.020303 – Филология – (кредит.-модул. система) / В. А. Кирвас ; Нар. укр. акад., [каф. информ. технологий и математики]. – Харьков : Изд-во НУА, 2011. – 92 с.
2. Інформатика, комп’ютерна техніка, комп’ютерні технології : підручник (затв. МОН України) / В. А. Баженов, П. С. Венгерський, В. С. Гарвона та ін. ; за ред. Г. А. Шинкаренка, О. В. Шишова. – 3-є вид. – К. : Вид-во Каравела, 2011. – 592 с.
3. Апатова Н. В. Інформатика для економістів : підручник для ВНЗ (затв. МОН України) / Н. В. Апатова, О. М. Гончарова, Ю. Ю. Дюлічева. – К. : Вид-во ЦУЛ, 2011. – 456 с.
4. Мельникова О. П. Економічна інформатика : навч. посіб. для ВНЗ (рек. МОН України) / О. П. Мельникова/. – К. : Вид-во ЦУЛ, 2010. – 424 с.
5. Національна економіка : навч. посіб. для ВНЗ (рек. МОНМС України). / В. І. Мельникова, О. П. Мельникова, Т. В. Сідлярук та ін. – 2-е вид. – К. : Ви-дво ЦУЛ, 2012. – 248 с.
6. Дибкова Л. М. Інформатика і комп'ютерна техніка : навч. посіб. для ВНЗ (рек. МОН України) / Л. М. Дибкова. – 3-є вид. – К. : Вид-во Академія, 2011. – 464 с.

Дополнительные источники

7. Дьячкова О. В. Персональный компьютер / О. В. Дьячкова, В. А. Кирвас. – Харьков : Фолио, 2010. – 730 с. – (Учеб. курс).
8. Грошев А. С. Информатика : учебник для вузов / А. С. Грошев. – Архангельск : Арханг. гос. техн. ун-т, 2010. – 470 с.
9. Леонтьев В. П. Безопасность в сети Интернет / В. П. Леонтьев. – М. : ОЛМА Медиа Групп, 2008. – 256 с.
10. Немцова Т. И. Практикум по информатике : учеб. пособие / Т. И. Немцова, Ю. В. Назарова ; под ред. Л. Г. Гагариной.– М. : ФОРУМ : ИНФРА-М, 2011. – Ч. 1. – 320 с.

Приложение

Сравнение WinRAR 3.91 и WinZip 14 Pro[3]

Параметр	WinRAR 3.91	WinZip 14 Pro
Цена		
Цена однопользовательской лицензии	29,00 у.е.	49,95 у.е.
Поддержка по электронной почте	Бесплатно для пользователей, купивших лицензию	Стоимость поддержки многопользовательской лицензии составляет 18% от покупной цены за каждый год
Поддерживаемые языки		
Количество языков локализации	46 +	7
Поддержка Unicode	+	+
Поддерживаемые операционные системы		
	Windows 95, 98, Me, 2000, XP, Vista, 7, Mac OS X, FreeBSD, Linux (граф. интерфейс только под Wine), OS/2	Microsoft Windows 2000, Windows XP, Windows Vista, Windows 7
Windows 7: поддержка "списков" на панели задач	+	+
Windows 7: поддержка библиотек	+	+
Возможности сжатия		
Стандартное сжатие по алгоритму ZIP	+	+
Стандартное сжатие по алгоритму RAR	+	–
Непрерывное сжатие	+	–

[3] http://www.win-rar.ru/winzipcomparison.php

Опции сжатия		
Добавление с заменой файлов	+	+
Добавление с обновлением файлов	+	+
Обновление только существующих файлов	+	+
Синхронизация содержимого архива	+	+
Запись даты / времени изменения с высокой точностью	+	+
Распаковка архивов с опцией "Сохранять поврежденные файлы"	+	–
Возможность поместить каждый файл в отдельный архив	+	–
Возможность установить размер словаря сжатия	+	–
Возможность преобразовать архив в SFX	+	+
Возможность протестировать архивы	+	+
Отображение информации об архиве	+	+
Добавление комментария к архиву	+	✓
Создание архивов, разбитых на несколько частей (томов)	+	+
Пауза после создания каждого тома	+	–
Возможность задать размер каждого тома	+	–
Пользовательский интерфейс		
Встроенный Мастер	+	+
Поддержка перетаскивания файлов	+	+
Режим управления файлами	+	+
Режим управления архивами	+	+
Поиск по содержимому архива	+	+
Создание профилей сжатия	+	+
Закладки для папок	+	+
Настройка панели инструментов	+	+

Безопасность		
Защита архива от повреждений	+	+
Восстановление недостающих частей многотомного архива	+	+
Защита архивов от случайного изменения	+	+
Возможность добавления данных, подтверждающих подлинность	+	–
Интеграция с антивирусными сканерами	+	+
Блокирование файлов с подозрительным расширением	+	+
Запрет запуска файлов типа *. PIF	+	+
Запрет запуска файлов, имена которых содержат 5 или более пробелов подряд	+	+
Защита паролем	+	+
Шифрование имен файлов	+	+
Поддержка стандарта AES (Advanced Encryption Standard)	+	+
Поддержка функций безопасности NTFS	+	+
Поддерживаемые типы архивов		
Извлечение	RAR, ZIP, CAB, ARJ, LZH, TAR, GZ, ACE, UUE, BZ2, JAR, ISO, 7Z, Z	ZIP, ZIPX, RAR, 7Z, BZ2, LHA / LZH, CAB, IMG, ISO, TAR, GZIP, GZ, TAZ, TGZ, TZ, Z, UU, UUE, XXE, B64, MIM, BHX, HQX
Сжатие	RAR, ZIP	ZIP, ZIPX
Поддержка дополнительных расширений имен файлов для форматов архивирования	+	+
RAR, ZIP	Создание	+
	Распаковка	+
	Восстановление	+
RAR	Преобразование в формат	почтовый

ZIP	Преобразование в формат	+
CAB	Распаковка	+
	Преобразование в формат	RAR, ZIP
ARJ	Распаковка	+
	Преобразование в формат	RAR, ZIP
LZH	Распаковка	+
	Преобразование в формат	RAR, ZIP
TAR	Распаковка	+
	Преобразование в формат	RAR, ZIP
GZIP	Распаковка	+
	Преобразование в формат	RAR, ZIP
ACE	Распаковка	+
	Преобразование в формат	RAR, ZIP
UUE	Распаковка	+
	Преобразование в формат	RAR, ZIP
BZIP2	Распаковка	+
	Преобразование в формат	RAR, ZIP
ISO	Распаковка	+
	Преобразование в формат	+
ISO 13346 (UDF)	Распаковка	+
	Преобразование в формат	RAR, ZIP
Z	Распаковка	+

	Преобразование в формат	RAR, ZIP
7-ZIP	Распаковка	+
	Преобразование в формат	RAR, ZIP
Опции SFX		
SFX-модуль	+	+
Формат ZIP SFX	+	–
Модуль RAR SFX для MSDOS	+	–
Модуль RAR SFX для командной строки Win32	+	–
Модуль RAR SFX для графического интерфейса пользователя Win32	+	–
Поддержка базовых функций	+	–
Добавление ярлыков в ОС Windows	+	+
Добавление диалогового окна установки в SFX	+	–
Выбор собственного логотипа SFX-архива	+	–
Создание SFX-архива из командной строки	+	–
Добавление собственного текста лицензии	+	–
Запуск программы установки после извлечения	+	–
Удаление файлов перед началом установки	+	–
Поддержка «тихого» режима (без вывода начального диалога)	+	–
Выбор собственного значка SFX-архива	+	–
Возможность использовать HTML в окне вывода текста	+	–
Поддержка специальных сценариев	+	+
Запрос прав учетной записи администратора	+	+

Опции резервного копирования		
Возможность добавления только файлов с отмеченным атрибутом «Архивный»	+	+
Снятие атрибута «Архивный» после сжатия	+	+
Сохранение предыдущих версий файлов	+	+
Создание имени архива по маске	+	+
Прочее		
Скрины / темы оформления	+	–
Архивирование в фоновом режиме	+	+
Автоматическое выключение ПК по завершении архивирования	+	+
Оценка сжатия	+	–
Оценка степени сжатия	+	–
Сжатие и отправка архива по электронной почте с помощью контекстного меню Проводника Windows	+	+
Создание отчета об архиве	+	–
Печать отчета об архиве	+	–
Тест быстродействия	+	–
Тест надежности аппаратуры	+	–
Опция «Ждать, если работает другая копия WinRAR»	+	–
Многопоточность	+	+
Выбор профилей из контекстного меню	+	+
Опция «Уничтожить файлы» (перед удалением данные файлов перезаписываются нулевыми байтами, что делает восстановление этих файлов невозможным)	+	+
Загрузка архивов по FTP	+	+
Интеграция с почтовым клиентом	–	Outlook 2007

СОДЕРЖАНИЕ

Навчальне видання

КІРВАС Віктор Андрійович

ІНФОРМАЦІЙНА БЕЗПЕКА. АРХІВАТОРИ ТА АНТИВІРУСИ

Навчальний посібник для студентів першого курсу вищих навчальних закладів

(російською мовою)

В авторській редакції
Комп'ютерний набір *В. А. Кірвас*

Підписано до друку 10.04.2012. Формат 60×84/16.
Папір офсетний. Гарнітура «Таймс».
Ум. друк. арк. 6,28. Обл.-вид. арк. 7,56.
Тираж 300 пр. Зам №

План 2011/12 навч. р., поз. № 4 в переліку робіт кафедри

Видавництво
Народної української академії
Свідоцтво № 1153 від 16.12.2002.

Надруковано у видавництві
Народної української академії

Україна, 61000, Харків, МСП, вул. Лермонтовська, 27.