Глава 5

Защита от вредоносных программ

К большому сожалению, существуют не только полезные для пользователей приложения, облегчающие работу или доставляющие удовольствие. Есть целый класс программ, присутствие которых на вашем компьютере крайне нежелательно. Общее их название — *программы-вирусы*. Вирусы — это вредоносные программы. Название, конечно, придумано по аналогии с биологическими вирусами. Однако программы-вирусы для здоровья человека не опасны, так как они выполняются на компьютере и несут угрозу другим программам и хранящимся на компьютере файлам с данными. Хотя и здоровью человека программы-вирусы могут нанести удар. Представим, что вы целый год писали на компьютере книгу, и вот, когда вы уже готовы нести ее в издательство, коварная программа-вирус удаляет файл с книгой с вашего компьютера! Тут и до сердечного приступа недалеко. Хотя ряд мер, о которых поговорим ниже, позволяет свести риск к минимуму.

Как вирусы попадают на ваш компьютер? Они могут распространяться по сети, через модем, подключенный к Интернету, или на внешних носителях информации (Flash-Drive, CD- и DVD-диски, дискеты).

Широкое распространение локальных вычислительных сетей и Интернета способствует массовому заражению компьютеров вирусами. При этом вирусы могут распространяться очень быстро не только в пределах одного предприятия или игровой сети, но и по всему миру, если зараженные файлы рассылаются через электронную почту.

Типы вирусов

Приведем классификацию программ-вирусов, которой придерживаются в известной компании, производящей антивирусные средства, Symantec Corporation.

Загрузочные вирусы

Загрузочные вирусы отличаются тем, что исправляют главную загрузочную запись жестких дисков. Таким образом, когда ваш компьютер начинает загружаться, управление передается вирусу.

Получив управление, вирус остается в памяти и заражает все диски при обращении к ним. А вы об этом ничего не знаете, так как до поры до времени видимых проявлений вируса нет.

Программные вирусы

Программные вирусы получили такое название, так как они внедряются в исполняемые файлы, имеющие расширение *.com*, *.exe* и *.dll*, и вставляют свои команды в программы, содержащиеся в этих файлах. Когда зараженный файл запускается на выполнение, часть программы, принадлежащая вирусу, тоже выполняется. В результате могут заразиться другие файлы или произойти какие-либо действия по нанесению ущерба вашему компьютеру. И в этом случае вы можете не заметить работы вируса, поскольку зараженная программа может продолжить работать нормально.

Есть несколько видов программных вирусов. Рассмотрим их.

- *Резидентные* — они постоянно находятся в оперативной памяти компьютера и обычно заражают все исполняемые файлы.
- *Прямого действия* — заражают другие файлы в момент выполнения зараженной программы, но не остаются в памяти после завершения ее работы.
- *Компаньоны* — не изменяют исполнимые файлы, а записывают себя на диск в виде файла-двойника. При этом первым выполняется файл с вирусом, а затем он запускает на выполнение нормальный файл с программой.

Макровирусы

Мы говорили, что вирусы — это программы. Это означает, что для того, чтобы они начали свою вредную работу, их должен кто-то запустить. Именно поэтому они привязываются к нормальным программам, чтобы вы, ничего не подозревая, запуском обычной программы запустили и программу-вирус.

Следуя этой логике, вирус не может заразить текстовый или графический файлы. В их составе нет программ. И это правда. Однако в файлах мощных текстовых редакторов (как, например, Microsoft Word) есть раздел, где могут находиться наборы исполнимых команд — *макросы*. По определению, данному в Справке по Microsoft Word, «макрос — это серия команд, сгруппированных вместе для упрощения ежедневной работы». Именно в эту область файла и может прокрасться макровирус (поэтому он так и называется).

Программы обработки табличных данных, таких как Microsoft Excel, также хранят в своих файлах с таблицами макросы. Такие файлы тоже не застрахованы от заражения.

Поскольку макровирусы для программы Microsoft Word могут заразить и шаблон, на основе которого создаются новые документы, все они окажутся зараженными.

Антивирусные программы

Программ для обнаружения и обезвреживания вирусов довольно много. Среди них есть и бесплатные, и платные.

Программы-антивирусы, пользующиеся наибольшей популярностью: Антивирус Касперского (KAV), Symantec AntiVirus, Dr.Web, NOD32.

Прежде чем решить, каким антивирусом пользоваться, надо выяснить, есть ли версии, работающие в операционной системе Windows 7. Если антивирусная программа не предназначена для работы в установленной на вашем компьютере операционной системе, категорически запрещается ее устанавливать.

Антивирус Касперского

Серия антивирусов лаборатории Касперского очень распространена в России и некоторых других странах. Сам Касперский занимается борьбой с вирусами достаточно давно, практически с момента появления персональных компьютеров серии IBM PC в России. Базы данных вирусов для этих антивирусных средств обновляются регулярно, разработчики достаточно оперативно реагируют на появление новых вирусов.

Антивирус Касперского 2010 может работать в операционной системе Windows 7.

Установка Антивируса Касперского 2010

Установка Антивируса Касперского не должна вызвать у вас затруднений. Она сделана по общепринятым стандартам.

Для установки запустите на выполнение файл setup.exe из установочного комплекта. Если установочный комплект у вас в виде самораспаковывающегося архива (один файл с расширением .exe), запустите его на выполнение. Если антивирус вы приобрели на диске, скорее всего, при помещении диска в привод запрос на установку появится автоматически.

Может появиться окно Windows 7 с запросом, разрешать ли устанавливать новое программное обеспечение на ваш компьютер. Для продолжения установки следует в этом окне щелкнуть мышью по кнопке Да.

Первое окно программы установки представлено на рис. 5.1. Если вы желаете установить антивирус с параметрами по умолчанию (при этом программа установки не задает вам дополнительных вопросов), сразу щелкните мышью по кнопке Далее.

Если же вы опытный пользователь и хотите выбрать путь для установки и набор устанавливаемых компонентов самостоятельно, сначала установите флажок Выборочная установка, а уж затем щелкните мышью по кнопке Далее.

Во втором окне (рис. 5.2) показывается лицензионное соглашение. Изучив его, щелкните мышью по кнопке Я согласен.

Если вы не включали флажок Выборочная установка, следующим появится окно, показанное на рис. 5.3. Вам предлагается поучаствовать в программе обмена информацией по проблемам с вирусами. Прочитайте внимательно условия участия и сделайте свой выбор. Если вы решились участвовать, установите флажок Я принимаю

условия участия в Kaspersky security network. Либо снимите этот флажок, если не хотите тратить на это время. Сразу после щелчка мышью по кнопке Установить начнется установка антивируса на ваш компьютер.

Если вы выбрали выборочную установку, появится окно, представленное на рис. 5.4. В этом окне в поле Папка назначения можно выбрать папку, куда будет устанавливаться программное обеспечение антивируса. Можно щелкнуть мышью по кнопке Обзор и указать любую папку, например созданную вами заранее специально для установки этого антивируса. Затем щелкните мышью по кнопке Далее.

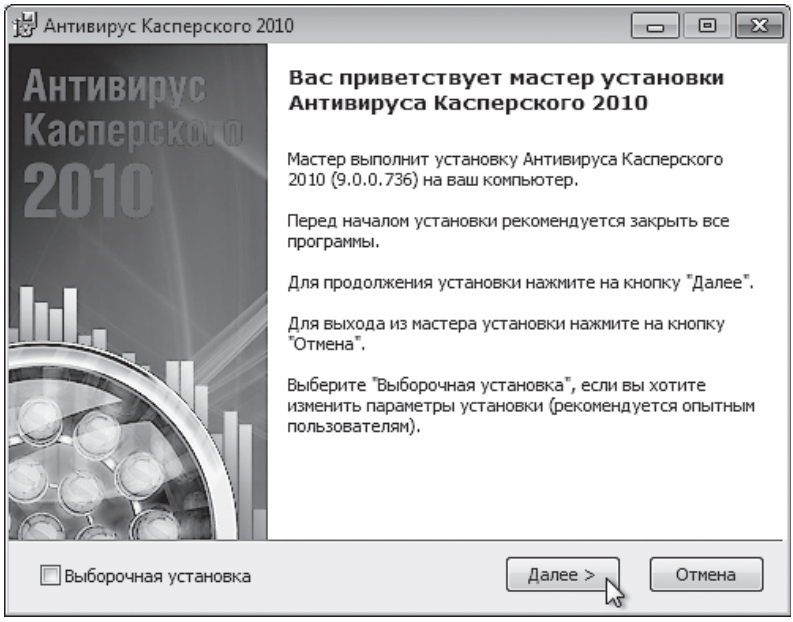

Рис. 5.1. Первое окно программы установки Антивируса Касперского

В появившемся окне (рис. 5.5) показаны компоненты антивируса. По умолчанию они все включены для установки. Можно не устанавливать часть компонентов, если вы считаете, что они вам не нужны. Для этого щелкните по значку слева от названия соответствующего компонента и выберите значение «Не устанавливать». После отключения ненужных компонентов щелкните мышью по кнопке Далее.

Следующее окно (рис. 5.6) оповещает, что все готово к установке. Щелкните в нем мышью по кнопке Установить.

Начнется процесс установки. При этом отображается окно с индикатором (рис. 5.7), позволяющим вам судить о доле проделанной работы.

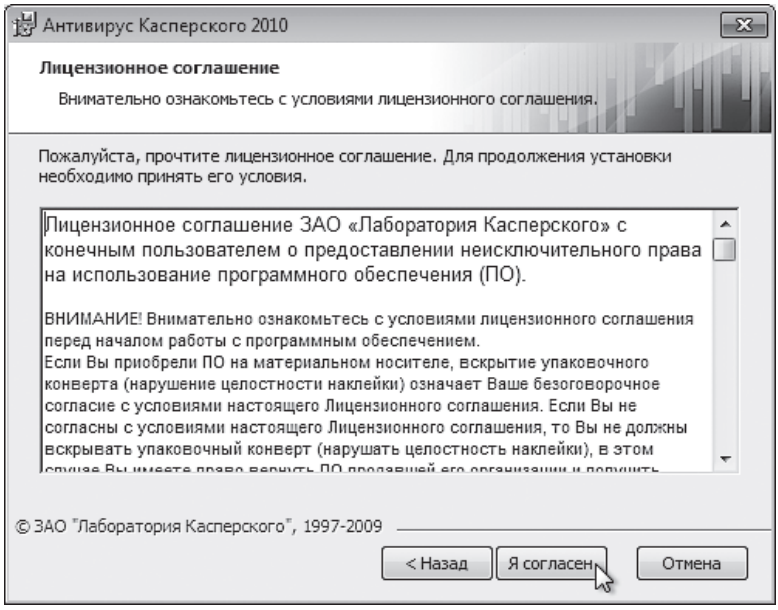

Рис. 5.2. Отображение лицензионного соглашения

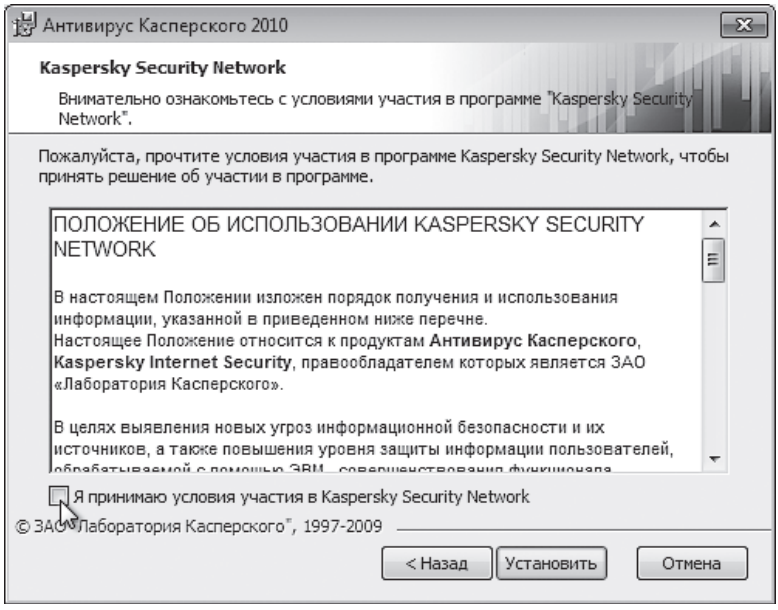

Рис. 5.3. Предложение участия в Kaspersky security network

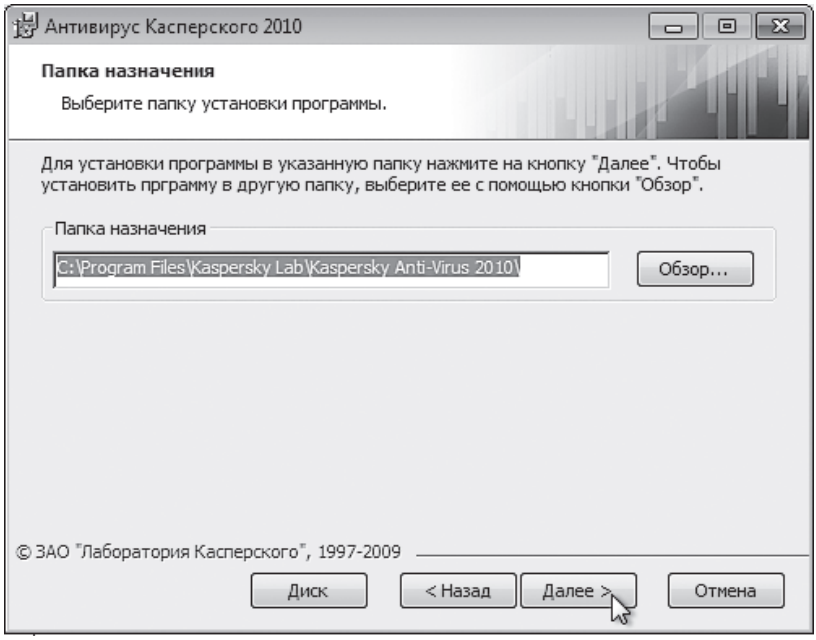

Рис. 5.4. Указание папки для установки Антивируса Касперского

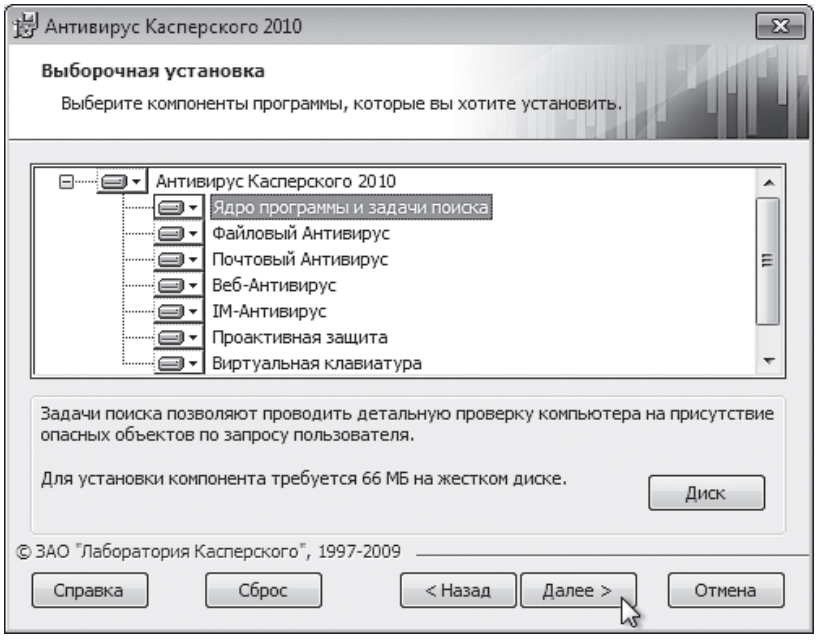

Рис. 5.5. Выбор устанавливаемых компонентов Антивируса Касперского

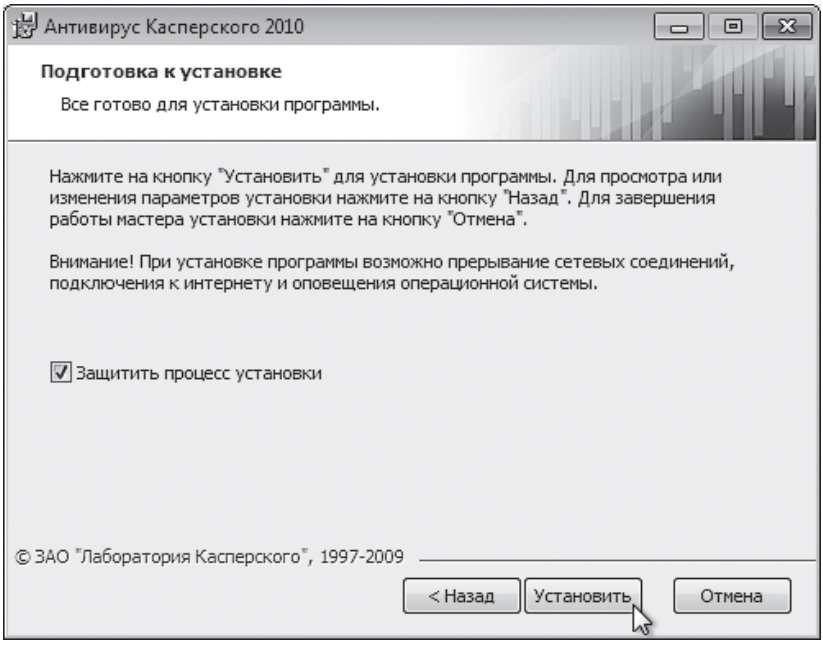

Рис. 5.6. Оповещение о готовности к установке

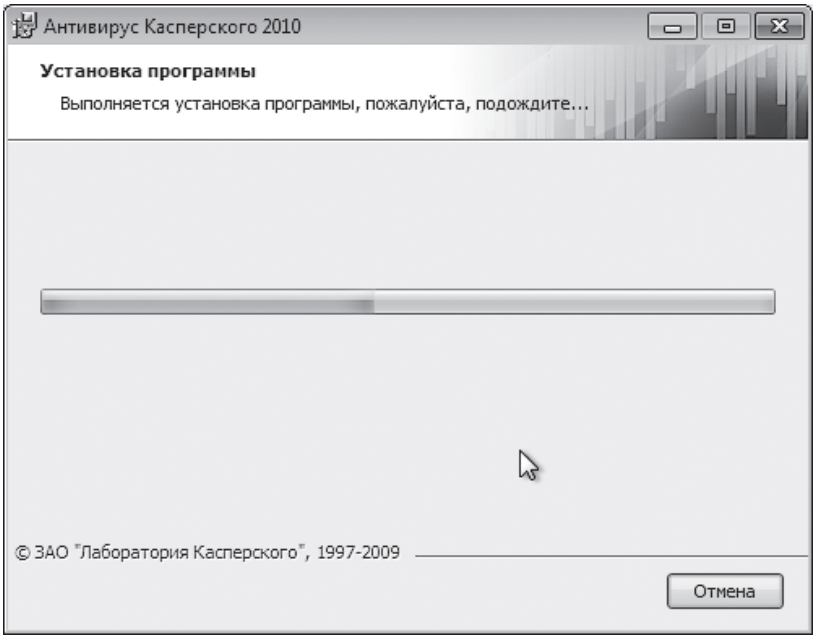

Рис. 5.7. Индикатор проделанной работы по установке

После завершения установки появится окно с предложением активации установленного антивирусного средства. Вы можете ввести код активации, полученный при покупке антивируса, либо использовать пробную версию (она будет работоспособной некоторое время), но для ее активации потребуется установленное подключение к Интернету. Можно отложить активацию на какое-то время, для чего надо выбрать пункт Активировать позже.

Работа с Антивирусом Касперского 2010

Для запуска антивируса щелкните мышью по кнопке Пуск, в Главном меню выберите пункт Все программы, в появившемся списке папок и приложений выберите папку Антивирус Касперского 2010, а в появившемся списке приложений этой папки выберите пункт Антивирус Касперского 2010 (Пуск ▸ Все программы ▸ Антивирус Касперского 2010 ▸ Антивирус Касперского 2010).

Вид окна Антивируса Касперского представлен на рис. 5.8.

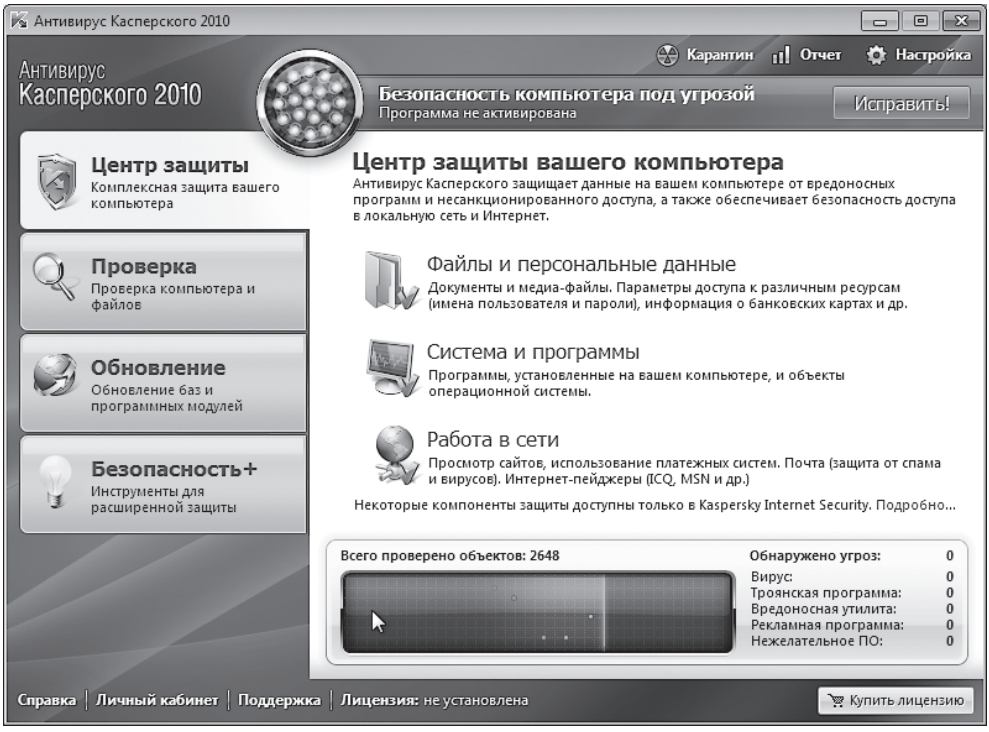

Рис. 5.8. Окно Антивируса Касперского 2010

В левой части окна расположено вертикальное меню, оформленное в виде вкладок. Щелкая мышью по ярлычкам вкладок (Центр защиты, Проверка, Обновление, Безопасность+), вы увидите вкладки со списками команд и режимов работы.

Первая вкладка — Центр защиты — содержит в себе список компонентов антивируса, которыми вы можете воспользоваться. Можно включать и отключать те или иные компоненты в зависимости от вашего желания. Для этого нужно щелкнуть мышью по кружку, расположенному в правой части окна напротив соответствующего компонента. Если кружок зеленый, значит, компонент включен и работает. При щелчке мышью по названию компонента в центральной части окна антивируса появляются кнопки и ссылки для управления ею.

Файловый Антивирус. При включении файлового антивируса в постоянном режиме будет работать монитор файлов, который проверяет файлы в момент их открытия. Например, вы открываете в Microsoft Word свой документ для редактирования. В этот момент, прежде чем документ появится на экране, он будет проверен на наличие вирусов.

В такой оперативной проверке есть и плюсы, и минусы. Большой плюс в том, что вы не забудете проверить принесенный с другого компьютера или загруженный из Интернета файл перед его открытием — за вас это автоматически сделает антивирус. Минус в том, что файлы в таких условиях открываются медленнее. Иногда это замедление очень действует на нервы, особенно если ваш компьютер не очень мощный. Выбирать вам. Хотя на некоторых предприятиях существует жесткое правило не выключать антивирусную проверку файлов при открытии.

Для включения проверки файлов при открытии надо установить флажок Включить Файловый Антивирус.

Следующий компонент — Почтовый Антивирус. Он отвечает за антивирусный контроль сообщений, поступающих по электронной почте. Если вы ведете активную переписку по Интернету, настоятельно рекомендуется включить этот компонент. Делается это также установкой флажка Включить Почтовый Антивирус.

Очередной компонент — Веб-Антивирус. Как видно из названия, он предназначен для оперативной защиты вашего компьютера при путешествиях по просторам Интернета.

Еще один компонент — IM-Антивирус. Его назначение — защита трафика для систем обмена сообщениями Интернета (например, ICQ, MSN, IRC и др.).

Последний компонент по списку — Проактивная защита. Этот компонент — попытка противодействовать новым вирусам, информации о которых еще нет в базе данных вирусов. Как же антивирус распознает, что программа, работающая на вашем компьютере, похожа на вирус. Проактивная защита анализирует поведение программ и замечает подозрительные программы по набору нетипичных действий, например, если программа начинает копировать сама себя или пытается менять модули других программ.

Конечно, включение всех модулей разом позволяет наиболее эффективно защитить ваш компьютер от большинства угроз, однако каждый работающий компонент замедляет работу вашего компьютера. Необходимый набор компонентов определять вам. Естественно, если вы не работаете в Интернете и ваш компьютер не подключен

к вычислительной сети, смело можно отключить Почтовый Антивирус и Веб-Антивирус.

Кроме постоянно работающих на ваше благо компонентов антивируса, можно (и нужно!) самостоятельно устраивать проверки логических дисков на наличие вирусов и проверять все файлы, которые вы принесли с другого компьютера или загрузили из Интернета. Логические диски надо проверять периодически, например раз в неделю. Принесенные или загруженные файлы нужно проверять сразу после записи на жесткий диск вашего компьютера. Как это сделать?

Для проверки логических дисков, папок или конкретных файлов перейдите на вкладку Проверка. При этом в центральной части окна антивируса появится список логических дисков вашего компьютера (под словами «Выполнить проверку объектов»). Для включения в список проверки любого из них щелкните мышью по квадратику слева от имени логического диска так, чтобы в нем появилась галочка. Если диск проверять не нужно, щелкните по этому квадратику, чтобы галочка исчезла.

Для включения в список проверки папок или файлов щелкните мышью по кнопке Добавить. В появившемся окне найдите нужную папку или файл, щелкните по ней мышью, а затем по кнопке Добавить. Можно сделать так несколько раз. Когда все нужные папки и файлы выбраны, щелкните мышью по кнопке ОК. Все выбранные вами папки и файлы появятся в списке для проверки с установленными слева галочками (рис. 5.9).

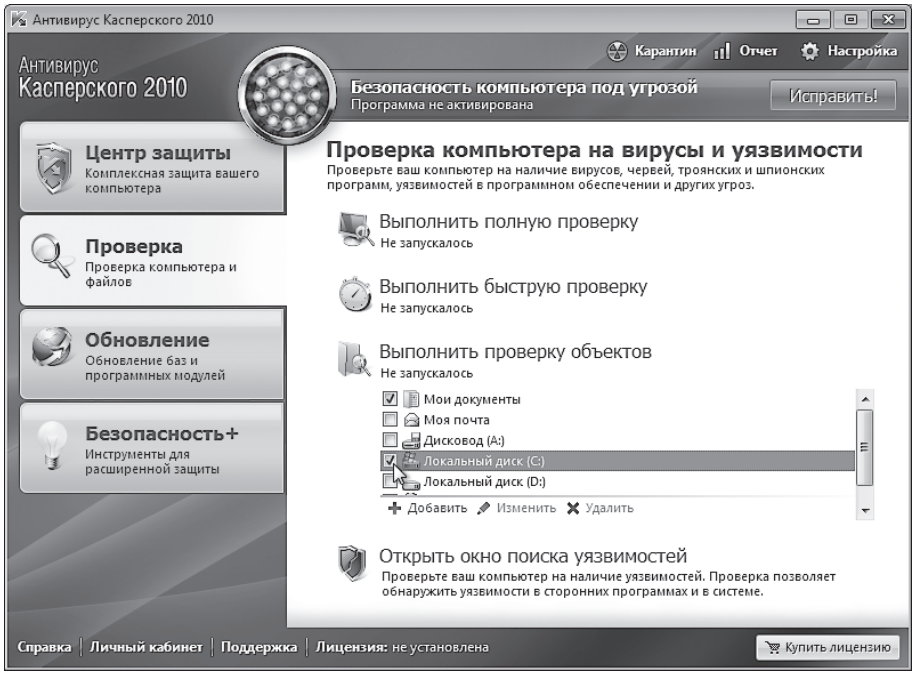

Рис. 5.9. Выбор дисков, папок и файлов для проверки