5. Компьютерные вирусы и борьба с ними

Кто не курит и не пьет,
Тот здоровеньким помрет.

Народная мудрость

Компьютерные вирусы – это программы, написанные хулиганами и вредителями, возможно, страдающими комплексом неполноценности или, наоборот, манией величия (что на самом деле почти одно и то же). Хуже того, их могут писать и террористы, ставящие своей целью отомстить кому-то, может, даже всему человечеству. Впрочем, чаще всего это просто мелкие жулики и вымогатели, бессовестные рассыльщики спама, которые хотят воспользоваться вашим компьютером как собственной станцией рассылки. Поэтому эмоциям тут не место, а нужны разумные меры защиты, подобно защите от рэкетиров, мошенников, холеры, СПИДа и резкого ужесточения налогового законодательства.

Вирус чаще всего приходит под видом программы или игры. Может и вправду запуститься какая-то программа или игра, но «под ее покровом темным вершатся тайные дела», как сказал поэт... Сперва вирус работает скрытно, повсюду внедряется, заражает все, что может, а уж потом дает о себе знать. Некоторые вирусы сидят тихо до определенной даты, как, например, «Чернобыльский вирус», срабатывающий один раз в год, 26 апреля, или «Пятница тринадцатое», срабатывающий именно при таком сочетании дня недели и числа. Другие начинают вредить сразу же.

Вредоносный вирус мешает работать операционной системе (работа сильно замедляется), уничтожает файлы и папки, да так, что потом не найти и следов. Блокирует компьютер, не давая работать до тех пор, пока вы не пошлете на указанный номер платную SMS-ку. Иные могут полностью разрушить информацию на диске, который приходится заново форматировать и заново устанавливать все программы, а о результатах своего многомесячного труда, если у вас нет копий на внешних носителях, можете забыть. Самые же злобные вирусы (вроде нашумевшего в свое время Win95.CIH) способны даже вывести из строя аппаратуру компьютера и выставить вас на крупную сумму.

Но есть особая категория вирусов, которые ведут себя совершенно иначе. Живут тихонько, маскируются под пустое место. А сами через интернет пересылают своему хозяину всяческую информацию о ваших кодах и паролях, о содержимом ваших файлов. Хозяин такого засланца, такого троянского коня может не просто получить доступ в интернет за ваш счет (украв пароль), но и прочесть, а также стереть в любой момент любые ваши файлы, запустить любые программы на вашем компьютере. Конечно, для этого должна быть установлена связь с интернетом.

Именно троянские вирусы используются для так называемого зомбирования компьютеров. Компьютер-зомби в тайне от своего хозяина и за его счет станет тысячами рассылать

рекламные письма (**спам**), будет участвовать в хакерских атаках на другие компьютеры, в распространении вирусов и прочих нехороших вещах. А беспечный владелец компьютера, не удосужившийся поставить себе надежный антивирус, будет платить за неожиданно большой объем перекачанных данных и удивляться, отчего это связь с интернетом такая медленная стала...

Вирусы могут приходить с электронной почтой – в приложенных к письму файлах. Иногда обманутый пользователь сам, своими руками скачивает и запускает вирус, полагая, что нашел интересную программку или игру. Но вирусы могут перелезать на другие компьютеры сети и без участия неопытного пользователя – сами. Такой вирус (**сетевой червь**) проверяет все компьютеры локальной сети на предмет дырок в защите. Найдя таковую, засылает туда свою копию. Копия поступает так же.

Другой весьма распространенный способ заражения – **через флэшку**, побывавшую на зараженном компьютере. Вирус копирует себя на вашу флэшку и вдобавок изменяет на ней так называемый файл автозапуска **autorun.inf** (или создает, если его там не было), чтобы запуститься первым. Поэтому сначала надо такой внешний носитель проверить антивирусом, а уж потом заходить на него и что-то иное с ним делать.

Вирусы способны заражать не только программы. Иногда заражаются служебные участки жесткого диска, например область, откуда система загружается. Тогда вирус включается прямо в момент загрузки, беря под свой контроль все остальные программы, включая и операционную систему. Это так называемые **бутовые вирусы** (от boot sector – «загрузочная область»).

Может быть заражен даже текстовый документ или электронная таблица.

– Но как это может быть, чтобы заражался текст? – спросите вы. – Ведь было сказано, что вирус – это программа, которая все и портит. А текст сам не работает (работает за него программа – текстовый редактор), а значит, он не может начать безобразничать, так ведь?

– Так, да не совсем. Документы современного текстового или табличного редактора (например, Microsoft Word и Excel) могут иметь собственные наборы макрокоманд – маленькие программки, часть из которых запускается при загрузке файла в редактор и выполняет некоторые полезные действия по оформлению документа. Вот сюда-то, в макрокоманды файла, и может забраться вирус. Точнее, **макровирус**. То есть заразу несет все-таки программа, только встроенная в документ.

Вот в силу всего изложенного (и многого еще не изложенного) каждый должен иметь программу защиты от вирусов и копии всех важных файлов на внешних носителях.

Ноутбуки часто продаются уже с установленным антивирусом. Здорово, конечно, но обычно это пробная версия, которая поработает у вас месяц или два. По истечении этого срока антивирус предлагает себя купить и полноценную деятельность прекращает. Можете либо заплатить и продлить использование еще на год, либо удалить этот антивирус и поставить другой – например, бесплатный.

Есть несколько бесплатных антивирусов вполне приличного качества. Это программы Avira AntiVir, avast!, AVG Free и Microsoft Security Essentials. Есть также десятка полтора известных платных антивирусов, таких как Антивирус Касперского, Доктор Веб, Eset Nod32, Symantec, McAfee или Panda.

А вот незнакомые защитные программы я бы ставить не советовал, как бы их авторы ни расхваливали свой «продукт». Есть такая интересная забава – распространять под видом бесплатных антивирусов или программ-антишпинов как раз шпионские программы и вирусы. Будьте начеку.

Как работают антивирусы

Лет десять-пятнадцать назад антивирусы действовали так: вы их запускали, а они проверяли оперативную память компьютера и просматривали файлы на дисках, найдя заразу, удаляли ее или пытались вылечить зараженные файлы, а потом выключались. Такие программы называются **антивирусными сканерами**. Их и сегодня включают в состав антивирусных пакетов, но главные теперь не они.

Чтобы не пришлось долго и мучительно лечиться, лучше просто не болеть. В качестве главного профилактического средства предлагается **система непрерывного наблюдения – антивирусный монитор**. Он берет под свой контроль входящую электронную почту, проверяет файлы, поступающие из интернета и по локальной сети, программы, которые вы запускаете, следит за тем, какие данные записываются на жесткий диск...

Непрерывная защита должна быть максимально быстрой, легкой и незаметной, чтобы не мешать своими действиями системе, программам и, конечно, их владельцам (увы, далеко не всегда это так!..). А вот сканер может мучить компьютер по полной программе, отыскивая вирусы внутри архивов, пытаясь узнать вирусы новых разновидностей, отсутствующие в антивирусных базах, применяя для этого сложные эвристические алгоритмы. Запускается сканер либо по расписанию (раз в сутки, раз в неделю), либо при простое компьютера (когда включается заставка), либо вручную – самим пользователем, когда ему придет в голову мысль провести углубленную проверку своих данных. Или когда у него есть основания подозревать, что в компьютере завелся вирус.

В составе любого антивируса обязательно имеется **блок для обновления антивирусных баз через интернет**. Вирусов развелось очень много, новые появляются ежедневно, а то и по нескольку штук в день, поэтому и антивирусы обновляются ежедневно, а то и по нескольку раз в день. Идет постоянная гонка между новыми опасными мутантами и лекарственными препаратами, которые призваны весь этот птичий грипп обнаруживать и уничтожать.

А теперь от теории перейдем к практике – посмотрим, как пользоваться антивирусами. В качестве примера я выбрал бесплатную программу avast! Но вовсе не потому, что это самый из всех лучший антивирус – тут очень трудно выбрать чемпиона. А потому, хотя бы, что этой программой я пользовался достаточно долгое время – и на XP, и на Висте, и на Windows 7 – успел кое в чем разобраться и кое в чем убедиться...

Антивирус Avast!

Avast! Free Antivirus представляет собой программу начального уровня среди антивирусных программ чешской компании Alwill Software. Помимо бесплатной имеются и платные редакции, например avast! Pro Antivirus (стоит 600 рублей в год) и пакет безопасности avast! Internet Security (1000 рублей). В состав платных версий входят некоторые дополнительные средства защиты вроде брандмауэра или фильтра нежелательной почты.

Когда я писал эту главу, программа имела номер версии 6, весила немало – почти 60 МБ. Вполне возможно, что в тот момент, когда вы пойдете ее скачивать, на сайте **avast.com** окажется более новая версия, и не исключено, что еще более тяжелая. Вирусов с каждым днем все больше, а вслед за ними растут и антивирусные базы программ. Тот же avast! еще четыре года назад был в шесть раз легче...

Программа проработает у вас пару месяцев, а потом потребует себя зарегистрировать – впрочем, тоже бесплатно. Выскочит окно с сообщением о том, что срок истек, вы введете в этом же окне свое имя, телефон и адрес электронной почты[1]. И еще на год получите полный комплект халявы. Важно только, чтобы в этот момент компьютер был подключен к интернету.

После установки программы в области уведомлений появляется ее значок – шарик со стилизованным (ну очень стилизованным!) изображением буквы *a*. Глядя на него, мы понимаем, что непрерывная (**резидентная**, как это обычно называется) защита компьютера включена. А когда шарик принимается вращаться, это означает, что санитарный инспектор наш уже кого-то проверяет.

У Аваста работает одновременно несколько служб, осуществляющих непрерывную защиту компьютера, – они называются тут **экранами**. Так, **Экран файловой системы** берет под свое неусыпное наблюдение все обращения к жесткому диску (проверяется каждый файл, который вы собрались копировать, просматривать или запускать). Проверкой содержимого веб-страниц занимается **Веб-экран**, входящую почту обезвреживает **Экран почты**, атаки сетевых червей отражает **Сетевой экран**, попытки переслать вирус по ICQ или через иную программу обмена короткими сообщениями пресекает **Экран интернет-чатов** и т. п.

Обнаружив заразу, любая их этих служб выдает примерно такое сообщение, как на рисунке 5.1 (тут у нас сработал экран файловой системы). Опасная операция блокируется, а опасный файл отправляется в карантин – в некую надежно защищенную папку, где он не будет представлять никакой опасности.

Но если вы на сто процентов уверены, что перед вами не вирус, а нормальный файл, можете щелкнуть по ссылке **Пометить файл как «ложную тревогу»** (нижняя строка на нашем рисунке). Заполните некую форму, информация из которой отправится к разработчикам антивируса, и подозреваемый будет выпущен

[1] Если у вас пока нет своего электронного адреса, сходите на один из почтовых сайтов (вроде **mail.ru**, **mail.yandex.ru** или **gmail.com**) и зарегистрируйтесь там. Процедура займет от силы минут пять, денег за это не просят.

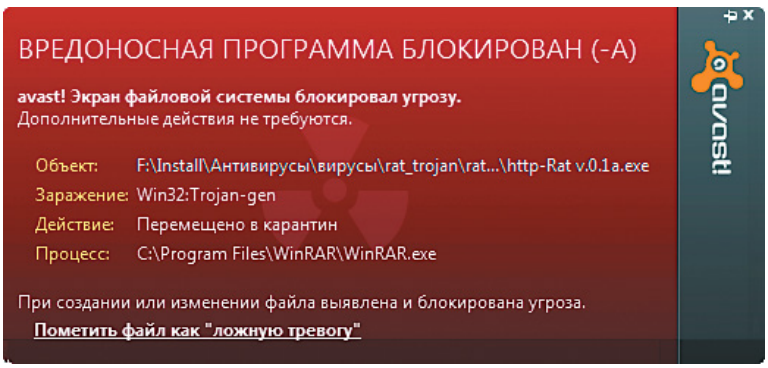

Рис. 5.1. Экран файловой системы предотвратил извлечение из архива опасного файла и отправил его в карантин

из пункта временного содержания – как неопасный и незаразный[1].

Ошибки такого рода с антивирусами, увы, случаются. Лучшие из них ошибаются редко, а вот с, так сказать, вторым эшелоном такое нет-нет, да и произойдет.

Если у вас когда-нибудь возникнут сомнения по поводу некоего файла – действительно ли в нем вирус? – для проверки скормите его какому-нибудь интернетовскому сайту, который может проверять файлы антивирусами без их установки в ваш компьютер, например сайту **virscan.org**. Если самые авторитетные антивирусы (Касперский, Доктор Веб, Nod32, Symantec, McAfee) опасности не находят, значит «антивирус второго эшелона» скорее перебдел, чем недобдел...

Щелчок мышкой по шарику Аваста в лотке открывает главное окно антивируса, устроенное в виде многостраничного диалога. Страницы его можно переключать щелчками по кнопкам слева. Например, со страницы **Сканировать компьютер** вы сможете выбрать один из четырех вариантов проверки: экспресс-сканирование (программа проверит оперативную память и системные файлы на предмет того, нет ли в компьютере активной заразы), полная углубленная проверка всех дисков или только съемных (флэшек, дискет, оптических дисков), а также выборочное сканирование (будет предложено пометить в дереве те папки или диски, которые надо проверить).

Впрочем, когда вам понадобится проверить флэшку, подозрительный файл или папку на жестком диске, вы сможете сделать это и без захода в главное окно антивируса: avast! добавляет в контекстное меню файлов, папок и дисков свою команду **Сканировать "xxx"** – вместо **xxx** будет стоять буква проверяемого

[1] Некоторые экраны (например, **Веб-экран** или **Сетевой экран**) никогда не отправляют файлы в карантин. Соединение с опасным сайтом или другим компьютером сети просто блокируется, едва программа заметит исходящую от него угрозу, так что опасный файл (даже если он запакован в ZIP- или RAR-архив!) просто не сможет оттуда скачаться. Во всплывающем уведомлении, которое вам при этом покажут, ссылки «ложная тревога» уже не будет.

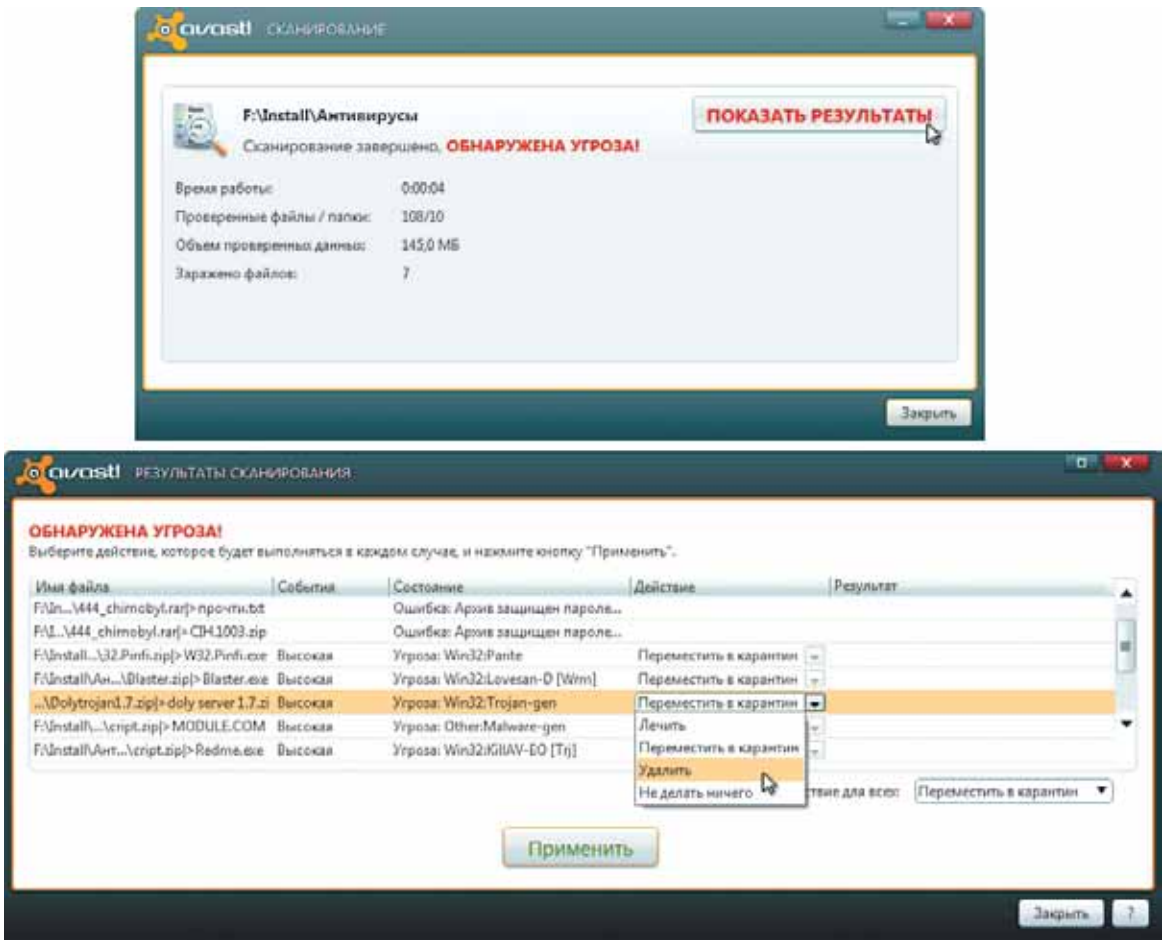

Рис. 5.2. При сканировании папки обнаружено семь вирусов! Как поступим?

диска, имя файла или папки. Этой командой вы и воспользуетесь. Это, кстати, типично для антивирусов – каждый из них добавляет подобные команды в контекстные меню.

При длительном простое компьютера антивирус сможет сам запускать сканирование – в момент, когда срабатывает заставка. После установки Аваста в списке заставок появится новая строка – **avast! antivirus**. Если ее выбрать, то вместе с показом летающих и плавающих разноцветных кривулек пойдет у вас сплошная проверка компьютера – полное сканирование.

Закончив проверку, антивирус выдает окошко с сообщением о ее результатах. Если вирусы не обнаружены, просто закрываем окно и живем себе, не тужим. Если же зараза найдена, нажимаем кнопочку **Показать результаты**. Нам предъявят список предполагаемых больных, и для каждого будет указан диагноз и степень опасности данного заболевания (рис. 5.2). Останется решить, что делать с этими файлами, и нажать кнопку **Применить**. Варианты имеются следующие.

- Строка **Лечить** позволяет избавить зараженный файл от внедренного внутрь вируса. Лечение возможно далеко не всегда: одно дело, когда имеется программа, текстовый или табличный документ, где прячется фрагмент вируса, и совсем другое, когда в файле кроме вируса ничего и нет. В первом случае в столбце **Результат** появится зеленая галочка и сообщение об успешном излечении, во втором – красный крестик и сообщение о неудаче: **Ошибка. Файл не был вылечен**. Такого только прибить и остается.

- «Прибитием» неизлечимых файлов ведает строка **Удалить**.

- Но по умолчанию программа выбирает другой режим изоляции заразы – **Переместить в карантин**. Если вам потом понадобится просмотреть содержимое карантина, вы щелкнете в главном окне Аваста по строке **Обслуживание** (откроется соответствующая группа команд), а потом – по строке **Карантин**. Увидите список изолированных файлов, через контекстное меню любой строки в этом списке можно будет этот файлик удалить насовсем, восстановить в прежнем месте его обитания, извлечь в другую, заданную вами папку и даже переслать в антивирусную лабораторию на исследование (надо будет заполнить простенькую форму: ложная тревога или, наоборот, неизвестный Авасту опасный файл, название программы, ее автор, версия и т. п.).

- Ну, и можно продолжать работу, не выполняя никаких действий. Так поступать стоит, только если вы на 100% уверены, что это не вирус и чешский атас!.. – то есть avast! – вспылошился зря. В спорных случаях (антивирус подозревает инфекцию, а друзья в один голос говорят, что это другое заболевание – паранойя) не забывайте о возможности проверить файл по интернету.

Антивирусы не могут проверять архивы, которые защищены паролем, – в такой архив без пароля даже заглянуть невозможно. В этом случае сканер пишет: **Ошибка: Архив защищен паролем**. *Но когда вы решите извлечь файлы из этого архива, введя пароль, вступит в игру* **Экран файловой системы**, *который немедленно их проверит, а если они опасны, то и заблокирует.*

Если вирус не просто лежит где-то в дальнем уголке жесткого диска, ожидая своего часа, а включился и активно работает, то ему вполне по силам помешать сканеру себя обнаружить и, тем более, удалить. Устраненная, вроде бы, зараза может появляться снова и снова. Попробуйте тогда еще один вариант – **Сканирование при загрузке** (есть в главном окне Аваста вкладка с таким названием; предложение об этом может выдаваться и по результатам обычного сканирования). Если вы нажмете там кнопку **Запланировать**, то сканер будет запущен при следующей загрузке компьютера – до старта операционной системы и, хочется верить, до запуска вируса.

На черном экране появится сообщение о начале проверки. Обнаружив зараженный файл, сканер сообщает об этом на русском языке, но latinskimi bukvami, и предлагает выбрать вариант поведения. Варианты те же, что и при обычной проверке: удалить, переместить в хранилище, лечить и т. п., только сообщать о своем решении вы будете, вводя цифру от 1 до 8 (с номером варианта).

Если не хотите этой проверки, нажмите **Esc**. Но лучше все же дождаться ее завершения.

Еще один новый механизм защиты, появившийся только в самой новой, шестой версии Аваста, называется **песочницей** (sandbox). Если антивирус не уверен во вредоносности программы, которую вы запускаете (например, это установщик некой новой программы, скачанной из интернета), но находит в ней нечто подозрительное, позволяющее предположить, что программка эта – замаскированный шпиён и вражеский лазутчик, он не помешает вам работать с ней, раз уж вы сами ее запустили, но предложит на пробу запустить ее в защищенном режиме – в песочнице. Окно программы, запущенной в песочнице, будет обведено красной каемкой.

Песочницей тут называется некая условная, виртуальная среда, полностью изолированная от остальной системы, – именно в ней будет работать подозрительная программа. Даже если это окажется злобный разрушительный вирус, все результаты его деятельности будут виртуальными, а все файлы, которые он, как ему кажется, записал на жесткий диск вашего компьютера, будут удалены, едва только вы закроете запущенную таким способом программу.

Даже если программа эта работает не сама, а встраивается, к примеру, в браузер Internet Explorer в качестве дополнительной панельки или иного вспомогательного модуля, после закрытия программы все эти дополнения пропадут.

Но антивирус, конечно же, не станет делать этого автоматически. Вам будет предложено (рис. 5.3) выбрать самим, разрешить ли запуск данной программы в песочнице, запретить (программа будет запущена обычным образом) или вообще отменить ее запуск и чуток поразмыслить над тем, стоит ли ее вообще запускать...

Если же вы пользуетесь запускаемой программой давно и ничего плохого от нее не видели, сможете пометить строчку **Запомнить мой выбор для этой программы**, чтобы раз

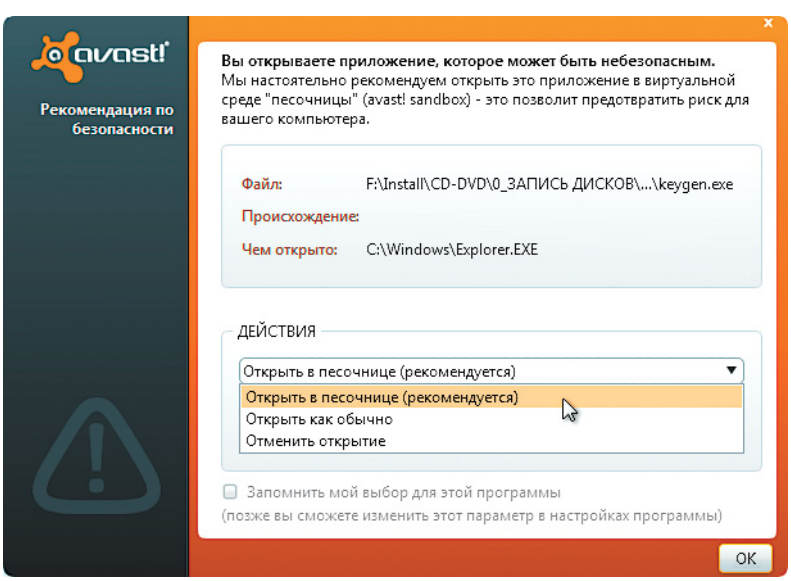

Рис. 5.3. Запускается подозрительный файл. Пусть порезвится в песочнице!

и навсегда отменить для нее ссылку в песочницу.

Из главного окна программы, со страницы **Обслуживание** ▸ **Обновить** (а также из контекстного меню значка avast! в области уведомлений) вы сможете запустить обновление антивирусных баз и самой программы, если вышла ее новая версия. Впрочем, делать этого обычно не приходится, потому что все необходимые обновления происходят автоматически[1].

Вообще, основное достоинство современных антивирусов в том и состоит, что они действуют полностью автономно, все необходимое делают сами. Наше участие требуется только в одном случае: если найдены зараженные файлы.

У Аваста есть даже такой режим работы, при котором он вообще перестает выдавать какие-либо уведомления о своей деятельности. Например, вы смотрите фильм в компьютере или играете в игру. На что вам сдались в это время радостные сообщения антивируса о том, что он обновил свою антивирусную базу? Ведь всякое такое сообщение, помимо прочего, скидывает проигрыватель или игру из полноэкранного режима в обычный оконный... Так что если не хотите, чтобы вас дергали по пустякам, щелкните правой кнопкой мыши по значку Аваста в лотке и поставьте галочку в строке **Режим «Без уведомлений / игровой»**.

Советовал бы вам заглянуть в настройки антивируса (кнопка **Настройки** с гаечным ключиком имеется в главном окне программы, вверху). Можно будет, к примеру, запретить выдачу звуковых сигналов (на странице **Звуки**), а не то программа примется время от времени немножко вас пугать, ни с того ни с сего объявляя вслух о столь значительных событиях вашей жизни, как очередное обновление или блокировка небезопасного сайта.

[1] Если быть более точным, автоматически обновляются только антивирусные базы, а о выходе новой версии программы вас будут лишь информировать.