УДК 004.056.52;
УДК 004.056.53;
УДК 004.056.57

Ю.А. Родин, С.Г. Самохвалова

ДОСТУПНЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ УГРОЗАМ

В статье представлен краткий обзор наиболее распространенных компьютерных угроз, предлагаются простые и эффективные способы защиты от проникновения и закрепления в системе вредоносного ПО.

Ключевые слова: информационная безопасность, компьютерные вирусы, вредоносное программное обеспечение, съемные носители информации.

AVAILABLE METHODS TO COUNTER CYBER THREATS

The article provides a brief overview of the most common computer threats and provides simple and effective ways to protect against penetration and retention of malwares in the system.

Key words: information security, computer viruses, malicious software, removable media.

Характерной чертой современного общества стало распространение информационных технологий в различных сферах человеческой деятельности. Процесс информатизации общества развивается стремительно, и это влечет за собой целый ряд негативных последствий. С одной стороны, возможность быстрого обмена политической, экономической, научной и другой информацией, применение новых информационных технологий, безусловно, позволяет решить или упростить решение многих задач, но, с другой стороны, вычислительные системы, средства телекоммуникации и информационного обмена становятся уязвимым местом в условиях нарастающей значимости информации.

Побочный эффект внедрения новых информационных технологий – возникновение новых видов угроз, – например, заражение компьютерными вирусами, искажение или уничтожение информации, ограничение доступа законных пользователей, подавление информационного обмена в сетях, нарушение работы аппаратуры и компьютерных систем [1].

Коротко рассмотрим примерную классификацию вредоносных программ.

Зловредная программа – исполняемый программный модуль, скрипт, макрос или прочий программный код, созданный с целью нарушить информационную безопасность[1]. Задачи зловредной программы: минимально – несанкционированное использование части информационных ресурсов, максимально – приобретение полного контроля над объектом или информационной системой с целью дальнейшего несанкционированного использования. К зловредным программам относятся виру-

[1] Информационная безопасность – состояние защищенности информационной среды, включающее все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности и достоверности информации или средств ее обработки.

сы, троянские программы, логические бомбы, средства скрытого удаленного администрирования, клавиатурные шпионы, программы, осуществляющие хищение паролей и прочей конфиденциальной информации.

Вирус – зловредная программа, основным свойством которой является возможность автоматического размножения (возможно, с самомодификацией) и распространения на новые информационные системы, без контроля со стороны создателя. Обычно основная цель вирусов – выполнение деструктивных действий, хотя встречаются вирусы, созданные для развлечения. Чаще всего никакой материальной выгоды создатель вируса от его функционирования не получает, но иногда (например, в рамках промышленной конкурентной борьбы) создание вирусов может быть оплачено заказчиком.

Троянская программа, троян, троянский конь (англ. Trojan) – зловредная программа, зачастую клавиатурный шпион, выполняющая не санкционированные пользователем и недокументированные действия, порой даже с функциями удаленного управления со стороны злоумышленника; создается с целью намеренного нарушения информационной безопасности данной системы. Часто при этом троянские программы маскируют несанкционированную деятельность выполнением ряда полезных для пользователя документированных действий. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособности зараженного компьютера (например, разработанные для массированных DoS-атак на удаленные ресурсы сети).

Гибриды – с развитием сетевых технологий появились троянские программы, проникающие в систему по принципу компьютерных вирусов. Подобные гибриды используют (в целях, поставленных злоумышленником) свойства и первого и второго классов зловредных программ. Наиболее сложные из них, будучи запущенными в сети предприятия и размножаясь как обычный вирус, могут со временем добраться до своей основной цели, которая, возможно, хорошо защищена от прямых атак извне. После этого троян выполняет задачу по нарушению безопасности и информирует создателя о том, что его задача выполнена.

Примитивные варианты вредоносных программ – могут делать мелкие пакости типа рассылки от имени пользователя, неосторожно запустившего программу, угроз или ругательств в адрес других пользователей сети.

Закладка (логическая бомба) – зловредная функциональность, реализованная как одна из скрытых функций системы или объекта. В отличие от троянских программ, попадающих в систему извне, создается в подавляющем большинстве разработчиками системы, срабатывание происходит при определенных условиях.

В настоящее время значительная часть практически любой информационной системы построена на использовании персональных компьютеров и периферийных устройств. Малые габариты и вес, наличие устройств сопряжения с каналами связи, массовость производства и относительно низкая стоимость благотворно повлияли на распространение типовых ПК практически во всех сферах деятельности современного общества. Это позволяет разрабатывать универсальные методики защиты для множества систем, а не разрабатывать индивидуальные средства защиты для каждого ПК или каждой информационной системы. Среди операционных систем – Windows, DOS, Linux, MAC OS, UNIX и других – наибольшую популярность получили операционные системы семейства Windows корпорации Microsoft. По данным компании Net Applications, наиболее популярными операционными системами для ПК в мире являются ОС семейства Windows, доля которых по состоянию на январь 2012 г. составляла 92.05% рынка (Net Application занимается веб-аналитикой, широко известна тем, что ведет исследования и глобальную статистику доли мирового рынка для веб-браузеров и операционных систем). Поэтому большинство вредоносных программ ориентировано именно на уязвимость – ОС Windows и их алгоритмы не работоспособны в других операционных системах. Для большинства пользователей активность вредоносных программ, помимо серьезных последствий (искажение

файлов, вымогание денег, нарушение работоспособности ПК) несет и массу элементарных неудобств: сокрытие файлов и папок, частичную блокировку функций операционной системы, блокировку вебсайтов, засорение жестких дисков и съемных носителей, снижение быстродействия ПК за счет потребления ресурсов ЦП и оперативной памяти [2].

В настоящее время существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учетными записями (например, «Администратор») без крайней необходимости.

2. Не запускать незнакомые программы из сомнительных источников, обращать внимание на расширение файлов.

3. Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).

4. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.

5. Пользоваться только доверенными дистрибутивами.

6. Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развертывания.

Рассмотрим перечисленное на примерах.

Особенностью иерархии прав в ОС Windows является наследование прав от родительского процесса дочернему. Запуская вредоносное ПО под привилегированной учетной записью, т.е. обладая правами администратора, пользователь передает ему свои привилегии. В результате вредоносное ПО получает возможность доступа к системным файлам и папкам, к реестру ОС, что позволяет ему заменять, модифицировать или удалять файлы ОС, копировать себя и добавлять вредоносный код в автозагрузку, нарушая работоспособность ОС.

2. Разработчики вредоносного ПО отслеживают популярность других программных продуктов и маскируют под них свои изделия. Такое ПО может быть визуально похожим на «настоящее» либо иметь лишь схожее название. Отдельно стоит обращать внимание на расширение файлов – исполняемый файл вредоносной программы может иметь иконку, характерную для изображения, текстового документа, видеофайла, архива или файла другого формата.

3. Для распространения вредоносного ПО часто используется механизм автозапуска со сменных носителей (жесткие диски, флеш-накопители, дискеты). Вредоносная программа копирует себя на носитель и записывает в его корень специально сконфигурированный файл – Autorun.inf, который обеспечивает ее автоматический запуск. При подключении зараженного носителя к другому компьютеру, ОС Windows сама считывает файл Autorun.inf и выполняет указанные в нем вредоносные инструкции. Опции сокрытия файлов и расширений также помогают им оставаться незамеченными в системе долгое время.

4. Вредоносные сайты – еще один способ доставки вредоносного ПО на компьютеры пользователей под видом легитимных программ. Принципиальное отличие в том, что пользователь сам загружает и устанавливает предлагаемое ПО на свой ПК.

5. Загрузка дистрибутивов с официальных сайтов минимизирует риски заражения и гарантирует отсутствие нежелательных компонентов.

6. Регулярное создание резервных копий важных файлов обеспечивает их сохранность и возможность восстановления как в случае вредоносной атаки, так и в случае программных и аппаратных сбоев ПК.

Знание механизмов работы вирусов позволяет обычным пользователям применять простые и эффективные методы для противодействия этим угрозам. Отличительной чертой большинства современных вредоносных программ является скрытое проникновение, закрепление в зараженной системе и сокрытие своей деятельности. Несмотря на разнообразие вирусов, прослеживаются общие методы решения названных задач.

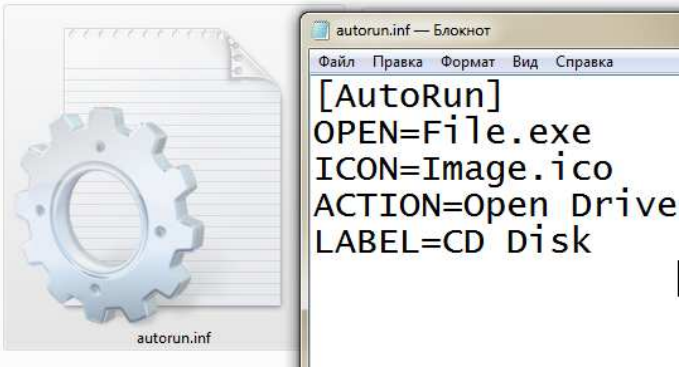


Рис. 1. Структура файла Autorun.inf.

Проникновение – самая важная стадия, без которой невозможны все дальнейшие. В последнее время большое распространение получили Autorun-вирусы, использующие файл автозапуска на съемных носителях для автоматического выполнения своего кода. При подключении устройства с подобным вирусом ОС Windows автоматически запускает файл вируса и вирус поражает систему. Рассмотрим структуру файла Autorun.inf (рис. 1).

Файл содержит 1 заголовок – блок [autorun] и 8 необязательных параметров. Наиболее часто используемые – это Open, Icon, Action и Label.

Параметр OPEN содержит путь к файлу, который будет запускаться при подключении носителя или попытке доступа к нему через Проводник Windows.

Параметр ICON содержит путь к файлу иконки-значка для носителя.

Параметр ACTION задает текст контекстного меню автозапуска.

Параметр LABEL задает название носителя.

В случае с вредоносным ПО вредоносный файл копирует себя на носитель, а также на носителе создается файл Autorun.inf (рис. 2). В параметр OPEN подставляется путь к вредоносному файлу, а в остальные параметры может помещаться ложная информация, сбивающая с толку пользователя. Например, в ICON – путь к иконке антивирусной программы, в ACTION – предложение «Обновить драйвера», а в LABEL – название известной компании.

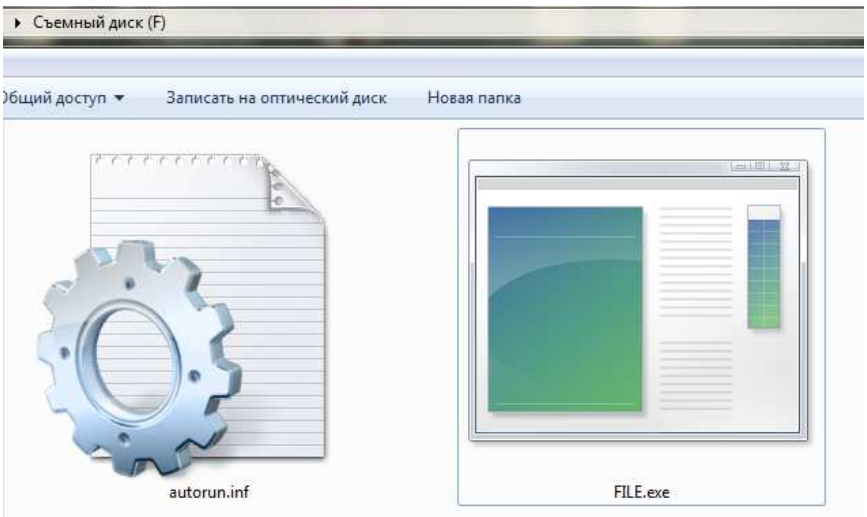


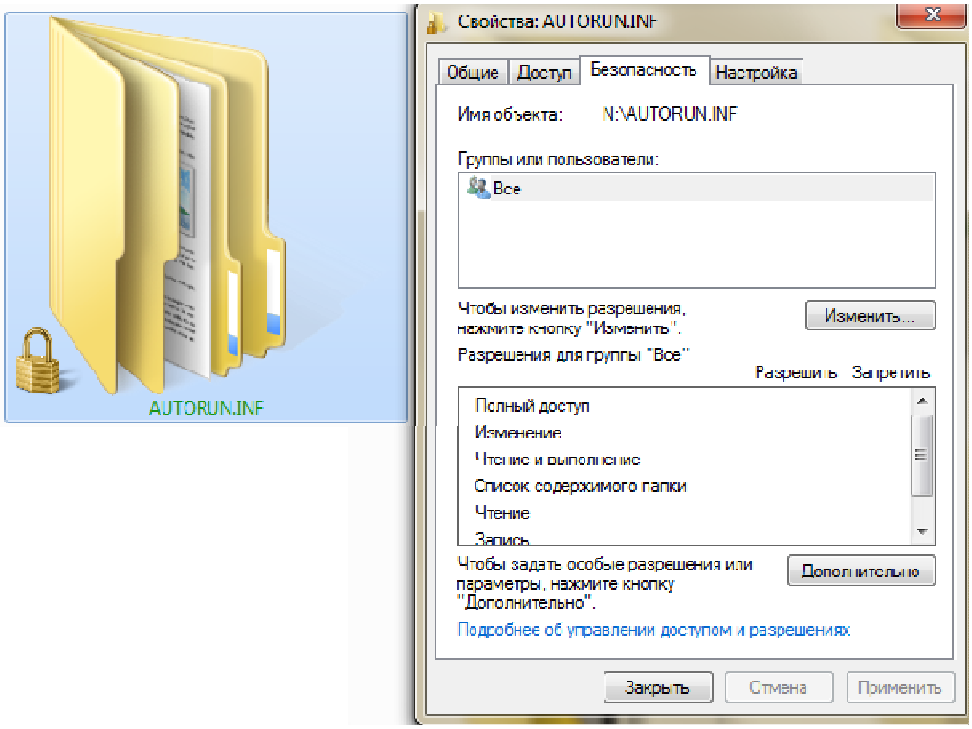
Рис. 2. Вредоносный файл и его Autorun.inf.

При первом рассмотрении проблемы находится очевидное решение: чтобы воспрепятствовать самостоятельному запуску вируса, достаточно отключить в ОС обработку файла автозапуска, которая по умолчанию включена. Этот способ защищает отдельную рабочую станцию от зараженного носителя – такого как дискета, жесткий диск или flash-накопитель. Недостатком этого способа является необходимостью производить отключение автозапуска на всех рабочих станциях. Также он не защищает от заражения сам носитель. Зараженный носитель, содержащий тело вируса и файл его автозапуска, продолжает представлять опасность для тех систем, в ко-

торых автозапуск не отключен. Существуют специальные программы, которые резидентно находятся в оперативной памяти системы и при подключении съемных носителей перехватывают обращение к ним, ищут файл автозапуска и удаляют его, делая дальнейшую работу с носителем более безопасной. Но не всегда такие программы успевают первыми перехватить доступ к подключенному устройству, и это их главный недостаток. Таким образом, вероятность заражения системы при подключении к нее зараженного носителя остается высокой.

Другой способ базируется в полной или частичной защите носителя от вредоносного ПО, – в частности, блокировка механизма или невозможность использования вирусом функции автозапуска. Например, копирование любого файла окончится неудачей, если в пункте назначения имеется файл с таким же именем и расширением. Следовательно, создание на носителе своего файла автозапуска Autorun.inf воспрепятствует записи вредоносного файла автозапуска на это устройство. В результате вредоносная программа сможет скопироваться на съемный диск, но не сможет обеспечить себе автозапуск, что позволит подключать такой диск к рабочим станциям, без риска автоматического заражения. Предлагаемый метод очень прост и эффективен и позволяет использовать накопители информации в «опасной среде», не опасаясь дальнейшего их использования в незараженных системах.

Все последующие действия должны быть направлены лишь на закрепление собственного Autorun.inf – защиту от случайного или преднамеренного переименования и удаления. Стоит отметить, что операции удаления файла и удаления папки имеют существенное отличие – удаление папки возможно лишь в том случае, если она пуста. Следовательно, в качестве собственного файла Autorun.inf выгоднее использовать папку с одноименным названием, содержащую как минимум один любой файл. Таким образом, созданная нами папка Autorun.inf на съемном носителе, внутри которой расположен пустой текстовый документ, уже не может быть удалена командой удаления папки. Помимо того, в качестве дополнительной защиты можно использовать возможности файловой системы



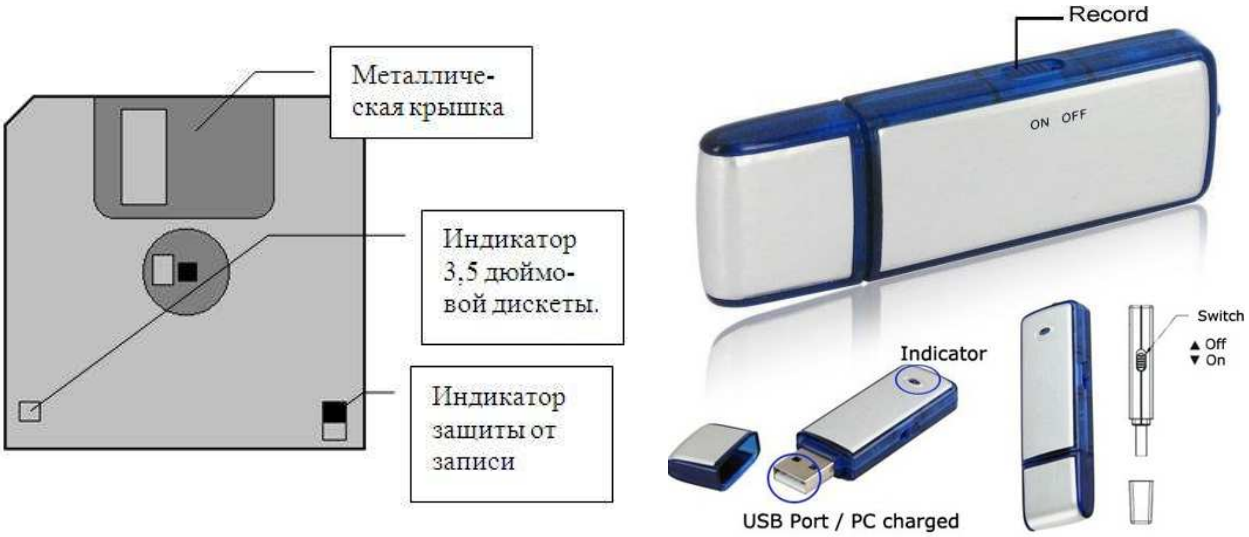
NTFS, ограничив права на доступ к папке Autorun.inf (рис. 3).

Рис. 3. Ограничение прав на доступ к папке Autorun.inf.

В результате этих нехитрых манипуляций носитель получает защиту от вредоносных файлов автозапуска. Вредоносная программа, попадая на такой носитель, не в состоянии записать свой Auto-

run.inf на место уже имеющейся папки.

Стоит упомянуть и другие способы защиты носителя. Первый заключается в аппаратном запрете записи новой информации на устройство и реализуется переключателем, который располагается на корпусе устройства (рис. 4). К сожалению, производители съемных жестких дисков и flash устройств не всегда оснащают свою продукцию подобными переключателями, а дискеты, хоть и имеют такой переключатель, практически вышли из обихода. Кроме того, аппаратная защита создает неудобство в работе с устройством – блокируется копирование не только вредоносной программы, но и



любой другой информации.

Рис. 4. Аппаратная защита от записи на съемный носитель.

Второй способ доступен для устройств, поддерживающих файловую систему NTFS. Устройство форматируется, затем в корне диска создается структура папок, после чего через управление правами доступа запрещается любая запись в корень устройства. Такой запрет лишает вредоносные программы возможности записывать что-либо в корневой каталог устройства. Пользователь также лишается этой возможности, но имеет возможность записи в заранее созданную им структуру папок.

Если же вирус уже проник в систему, то исправить ситуацию может опытный пользователь ПК, зная типичные места локализации вредоносных программ. Раньше для автозапуска вирусов использовалась системная папка «Автозагрузка».

Современное вредоносное ПО все чаще для автозапуска при загрузке системы использует ключи реестра, например:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.

Для своего копирования вредоносное ПО наиболее часто использует следующие каталоги:

в Windows XP

C:\Documents and Settings\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\Local Settings\Application Data
C:\Documents and Settings\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\Local Settings\Temp
C:\Documents and Settings\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\Local Settings\Temporary Internet Files

в Windows Vista/Windows 7

C:\Users\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\AppData\Roaming
C:\Users\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\AppData\Local\Temp

C:\Users\ИМЯ_УЧЕТНОЙ_ЗАПИСИ\AppData\Local\Microsoft\Windows\Temporary Internet Files

Для сокрытия своего физического присутствия на диске вредоносное ПО применяет различные механизмы маскировки. Файл вируса может иметь иконку полезной программы или, наоборот, не иметь иконки, что позволяет ему легко затеряться в системной папке наряду с консольными приложениями. Зачастую исполняемый файл вируса устанавливает себе атрибуты «Скрытый» и «Системный» и блокирует отображение скрытых файлов в Проводнике Windows. что также служит дополнительной защитой. Однако у пользователей, использующих альтернативные файловые менеджеры (например, Total Commander), наличие скрытых файлов, напротив, вызовет подозрение.

Другими косвенными признаками вредоносного файла могут являться его имя и дата создания. Например, файл с трудночитаемым именем abcde12345.exe, располагающийся в системной папке, с относительно недавней датой создания с большей долей вероятности является вирусом. Но необходимо быть внимательным, так как не все вирусы имеют в качестве имен беспорядочный набор символов. Многие вирусы специально называют свои файлы именами, схожими с именами важных системных файлов, корректируют дату своего создания, используют в названии различные языки. В то же время подозрительный на первый взгляд файл может оказаться частью какой-либо программы.

Для восстановления отображения скрытых файлов и папок в Проводнике Windows необходимо открыть меню «Сервис» – «Свойства папки» – «Вид», установить флажок «Отображать скрытые системные файлы» и переключатель «Отображать скрытые файлы». Некоторые вредоносные программы удаляют пункт «Свойства папки» из меню «Сервис». Для возвращения этого пункта достаточно открыть системную утилиту «Групповые политики», последовательно выбрать пункты «Конфигурация пользователя» – «Административные шаблоны» – «Компоненты Windows» – «Проводник». Параметру «Удалить команду "Свойства папки" из меню "Сервис"» установить значение «Отключен». Либо установить следующие значения реестра:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoFolderOptions"=dword:0000000
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions]
"NoBrowserOptions"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoFolderOptions"=dword:0000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions]
"NoBrowserOptions"=dword:00000000
```

Это позволит отображать скрытые файлы, локализовать вирусную программу и устранить угрозу.

Таким образом, в статье рассмотрены распространенные виды компьютерных угроз, а также простые, но эффективные способы предупреждения и отражения вирусной активности.

---

1. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Трикста; Акад. проект, 2005. – 542 с.

2. Дудоров, Е.Н. Возможные подходы к выявлению подозрительной активности программного обеспечения // Проблемы информационной безопасности. Компьютерные системы. – 2005. – № 2. – С. 31–37.