Федеральное агентство связи

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский технический университет связи и информатики»

(МТУСИ)

Кафедра: «Информационная безопасность»

КУРСОВАЯЯЯ РАБОТА

по дисциплине

Комплексные системы защиты информации

на тему:

«Тенденции развития компьютерных вирусов и борьбы с ними»

Выполнил:

Студент Канаев С. Д.

Группа М111501(73)

Проверил:

Звежинский С.С., профессор

Оценка\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва, 2016 г.

Содержание

Введение3

1. Классификация компьютерных вирусов 4

2. Примеры известных вирусов 10

3. Троянская программа 12

3.1 Распространение троянских программ12

3.2 Цели троянских программ13

3.3 Классификация троянских программ по внедрению в систему13

3.4 Типы троянских программ14

3.5 Примеры работы некоторых троянов15

4. Методы борьбы с компьютерными вирусами 19

4.1 Методы поиска вирусов 20

4.2 Технология эвристического сканирования24

4.2.1 Недостатки эвристического сканирования 25

4.3 Лицензионные антивирусные программы 25

4.4 Альтернатива платным программам26

5. Статистика вредоносных объектов от Касперского 28

Заключение30

Список использованной литературы 31

**Введение**

Работа с программным обеспечением на компьютере часто требует умения хранить в целостности информацию, защищать ее от возможных нарушений, сбоев в работе компьютера, вызванных воздействиями вредоносных программ или же нашими ошибками. Использование всемирной сети Интернет связано с возникновением вредоносного ПО, препятствующего нормальной работе компьютера, деформирующее файловую структуру дисков и наносящее ущерб хранимой в компьютере информации.

Среди набора программ, используемого большинством пользователей персональных компьютеров каждый день, антивирусные программы традиционно занимают особое место. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как превентивные, профилактические средства, так и средства лечения вирусов и восстановления данных.

Требования к антивирусным программам достаточно противоречивы. С одной стороны, пользователи хотят иметь надежную, мощную антивирусную защиту. С другой стороны, они хотят, чтобы эта защита не требовала от пользователя много времени и сил. И это вполне естественные требования.

Несмотря на большое количество принятых во многих странах законов о борьбе с компьютерными преступлениями и разработку антивирусов, количество нового вирусного ПО постоянно растет. Это требует от пользователя компьютера, знаний о сущности вирусов, способов их распространения и защиты от них.

**1 . Классификация компьютерных вирусов**

**Компьютерный вирус** - вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи [1].

Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, становится неработоспособной или же окажется под полным контролем злоумышленника.

Даже если автор вируса не программировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы обычно занимают некоторое место, иногда довольно значительное, в оперативной памяти или на накопителях информации и отбирают некоторые другие ресурсы системы.

Вирусы обычно разделяют по семи признакам:

**1) По среде обитания:**

а) Сетевые вирусы – это такой тип вирусов, который “проживает” в локальной сети. Данные вирусы, когда попадают на компьютер пользователя, копируют сами себя и распространяются по остальным компьютерам, которые подключены к сети. В основе источника распространения они используют электронный почтовый ящик, средства моментальной отсылки сообщений (например, skype), недостатки в расположении сети и неисправности в работе сетевых протоколов, а также сети обмена данными.

б) Файловые вирусы - это такие вирусы, которые записывают свой код в код программы. Они “просыпаются” при запускании инфицированной программы. Эти вирусы обычно заражают исполняемые файлы (.com, .exe), командные файлы (.bat), драйвера (.sys), динамические библиотеки (.dll).

 В настоящее время такие вирусы, как правило, представляют собой скрипты, написаны с использованием скриптового языка программирования (JavaScript, к примеру) и могут входить в состав веб-страниц. Они внедряются в исполняемые файлы, создают дубликаты файлов или используют особенности организации файловой системы для выполнения несанкционированных действий.

в) Загрузочные вирусы – это такие вирусы, которые располагают себя в загрузочном секторе жесткого диска, или же в секторе с системным загрузчиком жесткого диска, а также изменяют индикатор активного загрузочного сектора.

г) **Макровирусы -** поражают документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения макрокоманд. К таким документам относятся файлы, созданные с помощью пакета программ Microsoft Office, который поддерживает создание макросов на языке программирования Visual Basic for Application. Весьма полезно перед открытием незнакомого файла, созданного в таких программах, как Word или Excel, удостовериться, что поддержка макросов отключена (Сервис – Параметры – Безопасность макросов). Либо, для версии Microsoft Word 2010, в разделе "Безопасность программы" проверить, включен ли режим защищенного просмотра файлов и предотвращения выполнения данных [2].

Однако можно сказать, что современный вирус зачастую можно отнести сразу к нескольким группам вирусов. Такими сочетаниями являются, например, файловые загрузочные вирусы или файловые сетевые черви. Пример последнего: сетевой макро- вирус, который не только заражает документы, созданные в программах Word или Excel, но и рассылает свои копии по электронной почте.

 Еще одним классификационным признаком является **вид операционной системы**, так как любой вирус ориентирован на заражение файлов или выполнение несанкционированных действий в определенной операционной системе.

**2) По алгоритмам работы:**

а) Резидентные – это такой тип вирусов, которые при поражении компьютера заносят свою резидентную часть в оперативную память, а также считывают обращения операционной системы к объектам подвергшимся заражению, с целью имплантации в них. Такие вирусы обычно расположены в памяти компьютера и выражают работу до перезагрузки компьютера или отключения его от сети.

б) **Вирусы, использующие стелс-алгоритмы – это такие вирусы, которые выборочно или окончательно маскируют свое присутствие в программе. Преобладающим** стелс-алгоритмом является перехватывание запросов операционной системы на запись или чтение подвергшихся заражению объектов [3]. Стелс-вирусы временно лечат их или же вместо себя «подставляют» незараженные участки данных. Ярким примеров использования этих алгоритмов в случае с макро-вирусами является отсутствие возможности вызова меню просмотра макросов.

в) Вирусы, использующие полиморфность – это такие вирусы, которые используют алгоритм полиморфичности. Обнаружить их очень проблематично, так как данные вирусы не имеют неизменного участка кода. Проще говоря, два вида вируса не имеют совпадений. Данная технология реализуется шифрованием главного тела вируса и изменения программы-расшифровщика.

**г) Вирусы, использующие нестандартные приемы.** Применение нестандартных приемов обусловлено необходимостью спрятать тело вируса как можно глубже в ядре операционной системе, защиты от обнаружения резидентсткой копии, затруднения лечения от вируса.

**3) По разрушительным воздействиям:**

а) Неопасные – данные вирусы уменьшают свободную память на жестком диске, вследствие этого замедляется работа компьютера.

б) Опасные – эти вирусы приводят к повреждениям в конфигурации файлов и нарушении работы компьютера.

в) Очень опасные – данные вирусы повреждают ОС, губят или удаляют данные, хранящиеся на жестком диске.

**4) По способам заражения файлов:**

а) Перезаписывающие – такие вирусы вносят свой код вместо кода выбранного целью файла, удаляя его содержимое.

б) Паразитические – эти вирусы, когда распространяют копии самих себя, всегда меняют содержимое файлов, сохраняя файлы в полной или неполной работоспособности [4].

**5) Вирусы-компаньоны:**

К категории вирусов-компаньонов относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD.

**6) Вирусы-ссылки:**

Вирусы-ссылки также известные как link-вирусы не меняют физическое содержимое файлов, но когда запускается зараженный файл они заставляют операционную систему выполнять их код. Данной задачи эти вирусы достигают с помощью изменения нужных полей файловой системы [5].

### 7) Файловые черви

Файловые черви никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии — например, INSTALL.EXE или WINSTART.BAT.

Некоторые файловые черви могут записывать свои копии в архивы (ARJ, ZIP, RAR).

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Как видно, способов распространения компьютерных вирусов немало. Для предотвращения заражения необходимо соблюдать элементарные меры предосторожности:

* стараться использовать только проверенные ресурсы в сети Интернет;
* не скачивать сомнительные программы, а также не нажимать сомнительных картинок;
* при получении писем от неизвестного адресата, обращать внимание на расширение приложенных файлов. Если они имеют такие типы как:\*.bat,\*.vbs,\*.scr,\*.exe, то не стоит скачивать эти приложения, они могут быть заражены или попросту являются вирусом трояном;

### 8) Эксплоиты

Эксплоит, exploit - (от эксплуатировать) — простейший, несаморазмножающийся вредоносный код или просто нестандартный набор данных, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

В зависимости от метода получения доступа к уязвимому программному обеспечению, эксплоиты подразделяются на удалённые (remote) и локальные (local):

Удалённый эксплоит работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;

Локальный эксплоит запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав суперпользователя.

Атака эксплоита может быть нацелена на различные компоненты вычислительной системы — серверные приложения, клиентские приложения или модули операционной системы. Для использования серверной уязвимости эксплоиту достаточно сформировать и послать серверу запрос, содержащий вредоносный код. Использовать уязвимость клиента немного сложнее — требуется убедить пользователя в необходимости подключения к поддельному серверу (перехода по ссылке в случае если уязвимый клиент является браузером).

Эксплоиты фактически предназначены для выполнения сторонних действий на уязвимой системе и могут быть разделены между собой следующим образом:

1) Эксплоиты для операционных систем

2) Эксплоиты для прикладного ПО (музыкальные проигрыватели, офисные пакеты и т. д.)

3) Эксплоиты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие)

4) Эксплоиты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB)

5) Эксплоиты для интернет-сайтов (facebook.com, hi5.com, livejournal.com)

6) Другие эксплоиты

Эксплоит может распространяться в виде исходных текстов, исполняемых модулей, или словесного описания использования уязвимости. Он может быть написан на любом компилируемом или интерпретируемом языке программирования (наиболее частые: C/C++, Perl, PHP, HTML+JavaScript, XML).

Эксплоиты могут быть классифицированы также по типу используемой ими уязвимости, такой как: переполнение буфера, внедрение SQL-кода, межсайтовый скриптинг, подделка межсайтовых запросов и так далее.

### 9) Боты

"Бот" - производное от слова "робот" и представляет собой автоматизированный процесс, который взаимодействует с другими сетевыми службами. Боты часто автоматизируют задачи и предоставления информации и услуг, которые могли бы производиться человеком. Типичным использованием ботов является сбор информации (например, сканер поисковой системы, ищущий новые сайты), а так же автоматизированное взаимодействие с человеком (например, автоответчик в чате).

Боты могут использоваться как в хороших, так и в плохих целях. Примером незаконных действий может служить бот-нет (сеть ботов). Вредоносный бот распространяет вредоносное ПО, которое заражает компьютеры и подключает их через бэкдоры к центральному серверу управления, который может управлять всей сетью взломанных устройств. Используя бот-нет злоумышленник может совершать DDOS-атаки на сайты или сервера конкурентов. DDOS-атаки представляют собой одновременное огромное количеству бессмысленных запросов на сервер, исходящих от множества устройств (зараженных компьютеров), что приводит к перегрузке и зависанию сервера и невозможности нормальной работы и передачи информации (например, сайт перестает работать).

В дополнение к червеобразной способности самораспространяться, боты могут записывать нажатия клавиш, красть пароли, собирать финансовую информацию, совершать DDOS-атаки, рассылать спам. Боты имеют все преимущества червей, однако более универсальны и кроме того, объединены в сеть, которая позволяет контролировать зараженные компьютеры и совершать определенные действия по команде с контрольного центра. Создавая бэкдоры боты могут загружать на компьютер другие вредоносные программы, как вирусы или черви.

Боты в большинстве случаев стараются никак не проявлять себя для пользователя, поэтому опознать, что компьютер заражен бывает непросто.

Таким образом вредоносные боты являются наиболее опасными с точки зрения защиты информации, так как они не только сами распространяются и распространяют другое вредоносное ПО, но и способны совершать свои действия по команде из вне.

**2. Примеры известных вирусов**

**Вирус VIENNA (Вена), также имеет иные названия: 648, restart, Time Bomb.**

Является одним из первых самых простых вирусов. Впервые был обнаружен в Вене, далее и во всем мире. При попадании в память компьютера считывает com-программы в текущем. Изначальная версия данного вируса увеличивала размер зараженной программы на 648 байт. Первоначально обнаруженную еще не подвергшуюся заражению программу данный вирус заражает или с вероятностью 1/8 портит так, что при запускании происходит перезагрузка компьютера. При последнем варианте в тело зараженной программы заносится код EAF0FF00F0, означающий перезагрузку. Если испорченная таким действием программа вызывается из autoexec.bat, то происходит зацикливание перезагрузки ОС. В последствие было обнаружено более 20 модификаций этого вируса [6].

**Вирус BlackFriday, также известен как Israel Virus, BlackHole, Ierusalеm.**

Данный вирус впервые был найден в Израильском университете. Этот вирус инфицирует com и exe файлы, укрупняя их размер на 1813 байт, и остается резидентным в памяти компьютера. Вдобавок заражение происходит не единожды, что приводит к огромному разрастанию файла в размерах. Зараженный этим вирусом компьютер замедляет свою работу в пару тысяч раз. В нижнем левом углу экрана выскакивает черный прямоугольник. Помимо этого если заражение происходит в пятницу 13-го, то подвергшиеся заражению файлы удаляются.

**Вирус Dark Avenger, также известен как Sofia, Eddie.**

Данный вирус получил свои иные названия за текстовую строку содержащейся в его коде “ Eddie lives. Somewhere in time. This program was written in the city of Sofia”. Вирус инфицируется com и exe файлы, его размер 1800 байт. Этот вирус очень опасен, потому что на зараженном компьютере файлы заражаются не только при запуске, но и при переименовании и копировании. Вдобавок он удаляет файлы, размер который в пределах от 1800 байт до 64 кб. Также удаляет информацию из секторов винчестера [7].

**Вирус Ping Pong, также известен как Ball.**

Данный вирус инфицирует boot-сектор диска и заносит свой код как в свободные, так и в занятые кластеры. Проявляется данный вирус появлением ромбика на экране, который перемещается по экрану, отражаясь от его углов [8].

**Conficker 2008 года**

Самый, пожалуй, опасный представитель  из всех вирусов. Вредитель, который гордо носит название Conficker. Он один из самых последних и известных вирусов, который наносит непоправимый ущерб компьютерам. Данный вирус проникает в такие операционные системы, как Майкрософт Windows, причем охватывает года, начиная с двухтысячного и заканчивая Windows 7 и Windows Server 2008 года. Conficker привел в негодность около двенадцати миллионов компьютеров на всей Земле.

Его активное действие заключается в том, что вредитель находит всевозможные слабые места Windows, которые напрямую связаны с избытком информации в буфере и с помощью обманных путей, а именно, через RPС, который имеет функции запроса, создает и активирует специальный код, за счет чего делает все службы сервиса не активными и дает команду обновления Windows. В итоге, полностью ограничивает доступ, практически ко всем сайтам, где размещены антивирусные программы [9].

**Троянский Конь**

Данный вирус растекается по сети человеком. Это один из самых несложных разновидностей вредящих программ, которые до сих пор пользуются большой популярностью среди злоумышленников, поэтому данный вирус будет рассмотрен отдельно в следующем пункте.

**3. Троянская программа**

Троянская программа (троян, троянский конь) — вредоносная программа, которая используется злоумышленником для применения ресурсов компьютера в подозрительных целях, нарушения его работоспособности, или же для разрушения информации, её сбора или изменения [10].

Некоторые виды троянских программ вредят компьютерам и сетям, не нарушая при этом работоспособность зараженного компьютера (например, троянские программы, написанные для распределенных DoS-атак и DDoS-атак на удаленные ресурсы сети). Действие троянской программы, может и не быть вредоносным, но троянцы завоевали свою плохую славу за их использование в установке Backdoor программ [11]. Backdoor – это программа, основным назначением которой является скрытное управление компьютером.

Троян может в той или иной мере копировать (или даже полноценно заменять) программу или файл, под который он маскируется (программы инсталляторы, игры, документы, изображения и т.д.). В том числе, злоумышленник может получить код уже существующей программы и добавить туда троянские компоненты, а потом выдавать за оригинал [12].

Похожие маскировочные функции также используются компьютерными вирусами, но они имеют различие с троянскими программами, так как трояны не могут распространяться саморазмножением.

**3.1 Распространение троянских программ**

Троянские программы, как и загружаются в компьютерные системы злоумышленниками, так и побуждают пользователей загружать и/или запускать их на своих системах.

Для свершения последнего, троянские программы размещаются злоумышленниками на открытые ресурсы (файл-серверы и системы файло-обмена), носители информации, присылаются с помощью служб обмена сообщениями, попадают на компьютер через дыры безопасности или загружаются самим пользователем с адресов полученных одним из выше перечисленных способов[13].

Чаще всего заражение происходит, когда пользователь запускает какую-то программу, полученную из "сомнительного источника". Поэтому основной задачей злоумышленника является провоцирование пользователя на запуск вредоносного кода на своем компьютере [14].

**3.2 Цели троянских программ**

Троянские программы различаются по тем действиям, которые они осуществляют на компьютере. Каждая категория троянов преследует разные цели [15].

Целью трояна может быть [16]:

1) Cкачивание файлов;

2) Подделка ссылок, ведущих на пиратские веб-сайты;

3) Создание затруднений работы пользователя;

4) Кража данных, представляющих ценность, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам, получение информации касательно банковских счетов, которые могут быть использованы в незаконных целях;

5) Распространение вирусов;

6) Разрушение данных (удаление или переписывание, трудно замечаемые повреждения данных), выведения из строя или остановку обслуживания компьютерных сетей, систем;

7) Использование адресов электронной почты, для рассылки спама;

8) Слежка за пользователем и скрытое сообщение третьим лицам сведений, таких как, история посещения сайтов;

9) Регистрация нажатий клавиш, с целью кражи паролей и номеров кредитных карточек;

10) Дезактивация или создание затруднений в работе антивирусных программ;

**3.3 Классификация троянских программ по внедрению в систему**

Существует классификация, где троянские программы разбиваются на категории, базированные на том, как трояны получают доступ к системе и наносят ей ущерб. Существует 5 основных категорий[15]:

1) Удалённый доступ, это программы, которые позволяют получить доступ к удаленному компьютеру. Такие программы состоят из двух частей. 1-ая часть - сервер, вторая – клиент[16];

2) Удаление данных;

3) Загрузчик, вредоносные программы, предназначенные для загрузки и инсталляции на компьютер жертвы новых версий вредоносного ПО, установки троянов или рекламных баннеров. Затем загруженные программы запускаются на выполнение, или регистрируются троянцем на автозагрузку в соответствии с возможностями ОС. Информация об именах и расположении загружаемого ПО содержится в коде и данных троянца, или загружается трояном с "управляющего" Интернет-ресурса (обычно, с веб-сайта)[17];

4) DoS-атаки, программы, предназначенные для осуществления DoS-атаки (Denial of Service) с зараженного компьютера на компьютер жертвы, по назначенному заранее адресу. Смысл атаки заключается в отправке жертве большого числа запросов, что будет приводить к остановке в обслуживании, в случае если ресурсов удаленного компьютера жертвы не хватает для обработки всех поступивших запросов[18];

5) Деактивация программ безопасности;

**3.4 Типы троянских программ**

**Trojan-ArcBomb** – данные трояны являются архивами, созданные так, чтобы вызывать нестандартное поведение работы архиваторов при попытке разархивации (зависание или значительное замедление работы компьютера или заполнение диска «пустыми» данными). Архивные бомбы больше всего опасны для файловых и почтовых серверов. Если на сервере используется какая-либо система автоматической обработки входящей информации — то этот троян может прекратить работу сервера[19];

**Trojan-Banker** - троян, используемый для кражи пользовательской информации, относящейся к системам электронных денег, банковским системам и кредитным картам. Полученная информация передается злоумышленнику. Для передачи полученных данных может использоваться электронная почта, FTP, HTTP и другие способы[19];

**Trojan-Proxy** - вредоносная программа, предназначена для осуществления несанкционированного анонимного доступа пользователем к разным Интернет-ресурсам с помощью компьютера-жертвы[19]. Proxy Trojan копирует свои файл(ы) на ваш жёсткий диск. Типичное имя файла **wkfxi.js**. Потом он создаёт ключ автозагрузки в реестре с именем **Proxy Trojan** и значением **wkfxi.js**. Вы также можете найти его в списке процессов с именем **wkfxi.js** или **Proxy Trojan**.

**Trojan-Ransom** – троян предназначен для несанкционированной модификации данных на компьютере-жертве так, чтобы сделать невозможным работу с ним, либо создать помехи для неправильной работы компьютера. После захвата данных (блокировки данных), пользователю выдвигается требование выкупа. Указанную сумму жертва должна переслать злоумышленнику, после этого злоумышленник обещает выслать программу для восстановления данных или нормальной работы компьютера;

**Backdoor – троян**, предназначенный для доступа злоумышленнику к удалённому компьютеры жертвы. По функциональности бэкдор-трояны напоминают системы администрирования, разрабатываемые и распространяемые фирмами-производителями ПО. Эти вредоносные программы дают возможность злоумышленнику делать с компьютером всё, что заложил туда автор: принимать или отправлять файлы, запускать и удалять их, уничтожать информацию, выключать и перезагружать компьютер и так далее.

**Trojan.Winlock (Винлокер)** — семейство троянов, блокирующих или затрудняющих работу с ОС, и требующих перечисления денег за восстановление нормальной работоспособности ПК, частный случай Ransomware (троянов-вымогателей). Появились в конце 2007 года. Широко распространились зимой 2009—2010 годов, по некоторым данным были заражены миллионы компьютеров, В основном среди пользователей рунета. Вторую волну активности, это вредоносное программное обеспечение, получило в мае 2010 года. Блокирующее окно представлено на рисунке 1.

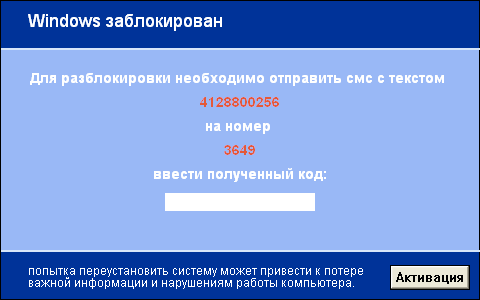


Рис. 1 Окно Trojan.Winlock

**Rootkit - троян**, предназначенный для скрытия в системе определенных объектов, либо активности. Скрытию, обычно, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти компьютера-жертвы, вредоносная сетевая активность.

**3.5 Примеры работы некоторых троянов**

**Back Orifice, Backdoor.BO** — троянская программа удаленного доступа. Была разработана в 1998 году. Программа предназначена для удаленного контроля над компьютером с ОС Windows 95/Windows 98. Архитектурой программы явлется клиент-сервер. BOSERV – небольшой серверный компонет, который устанавливается на компьютере-жертве, компонент представляет собой exe-файл. С помощью специальной утилиты BOCONFIG его можно присоединить к любому exe файлу. Клиентская часть реализуется программой BOGUI. Для обмена данных между BOGUI и BOSERV используется TCP/IP через порт 31337.

Возможности Back Orifice достаточно велики. Программа позволяет получать доступ к файлам на компьютере жертвы, останавливать и запускать процессы, перехватывать символы, вводимые с клавиатуры, просматривать образ экрана и т.д. Все действия происходят совершенно скрытно. Как утверждают разработчики: «Back Orifice даёт Вам гораздо больше возможностей на удалённом компьютере, чем у его локального пользователя». Интерфейс программы представлен на рисунке 2.

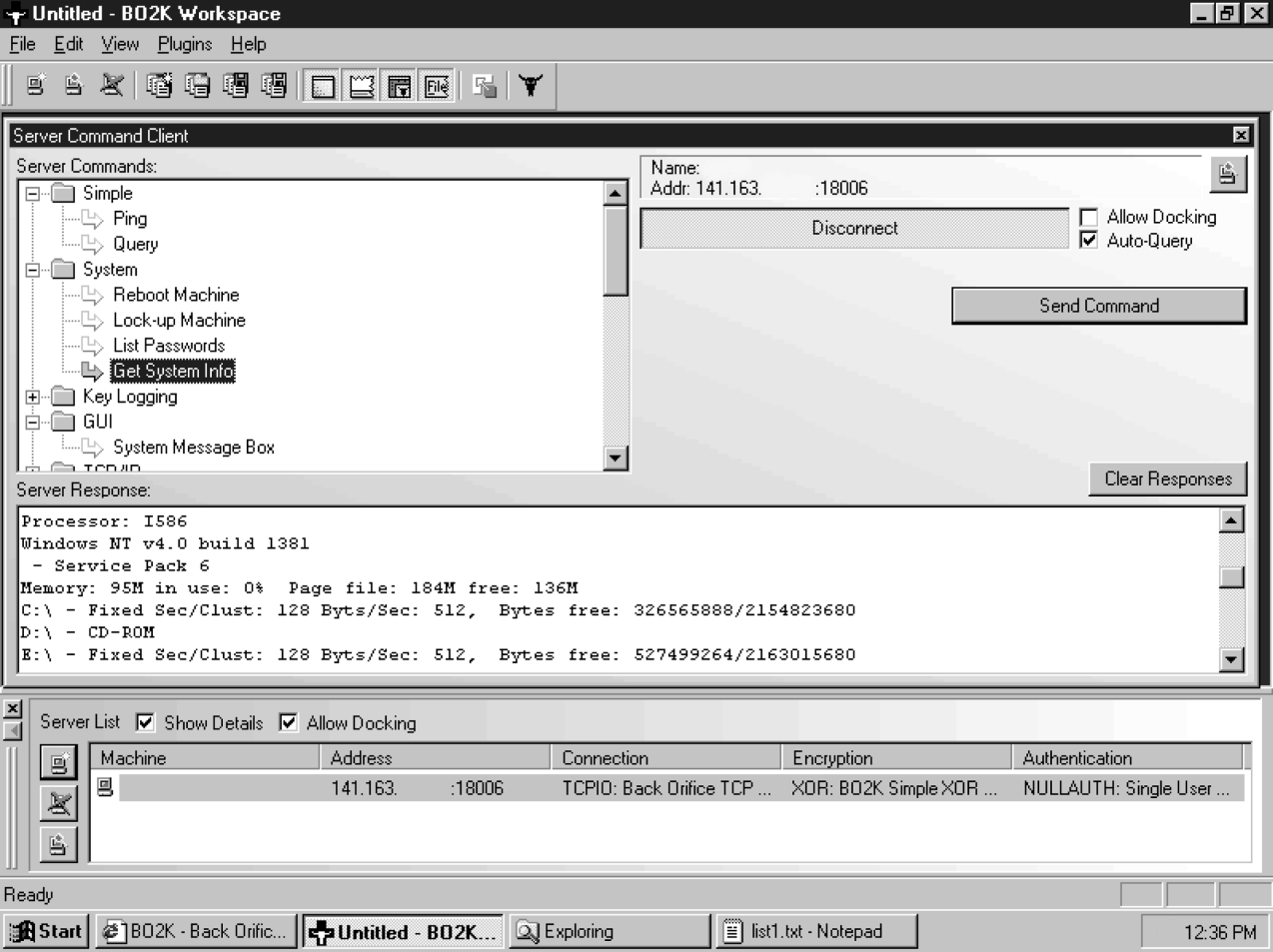


Рис. 2 Интерфейс Back Orifice

**Pinch** — один из наиболее активно используемых троянов в русскоязычном интернете, написанный программистом Александром Демченко в 2003 году [20]. Программа распространялась с открытым кодом, что привело к его усовершенствованиям, доработкам и изменениям сторонними разработчиками. Интерфейс программы приведен на рисунке 3.

Pinch построена на основе клиент-серверной архитектуры. Серверная часть написана на языке ассемблера (MASM) и после компиляции и упаковки обладает небольшим размером — около 20 кб. При попадании на компьютер, сервер, в наиболее распространенной своей модификации, собирает все сохранённые пароли из таких программ как: FTP-клиенты, браузеры, программы мгновенного обмена сообщениями, почтовые клиенты, менеджеры закачек.

Кроме того, Pinch собирает сведения об ОС и конфигурации ПК (маркировка и частота процессора, объем оперативной памяти, количество и размер жестких дисков и т.д.). В более новых версиях трояна появились функции удаленного контроля и доступа к файловой системе зараженного компьютера и множество других возможностей. Стоит отметить, что возможности Pinch могут сильно варьироваться в зависимости от модификации.

После того, как данные на зараженном компьютере были собраны, создается временный файл — C:\out.bin, в который упаковывается и зашифровывается вся необходимая информация. Данный файл может быть отправлен злоумышленнику по электронной почте, через протоколы HTTP (посредством указания данных в POST-запросе) или FTP. Всё происходит скрытно. Полученные данные расшифровываются с помощью специальной программы Parser.

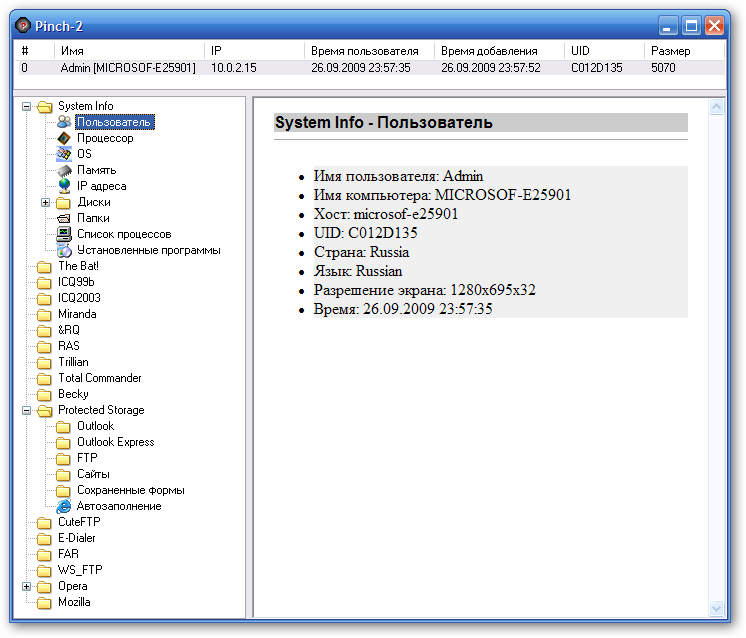


Рис. 3 Интерфейс программы Pinch

Здесь описаны лишь некоторые типы троянских программ, которые поддаются обобщению и систематизации. Однако есть трояны, в которых скомбинировано много из перечисленных в статье проявлений. Существуют троянские программы, написанные специально для инсталляции на конкретный компьютер, и выполняемые ими задачи могут быть очень специфическими [21]. В принципе, антивирусные программы способны обнаруживать и удалять трояны автоматически. Чрезвычайно важно для обеспечения большей точности обнаружения регулярное обновление антивирусной базы данных.

**4. Методы борьбы с компьютерными вирусами**

Способы противодействия компьютерным вирусам можно разделить на несколько групп [22]:

а) профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения;

б) методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;

в) способы обнаружения и удаления неизвестного вируса.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус). Более того, невозможность существования абсолютного антивируса была доказана математически на основе теории конечных автоматов, автор доказательства — Фред Коэн. Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

* «Ложное срабатывание» (False positive) — детектирование вируса в незараженном объекте (файле, секторе или системной памяти). Обратный термин — «False negative», т.е. недетектирование вируса в зараженном объекте.
* «Сканирование по запросу» («on-demand») — поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания (system scheduler).
* «Сканирование на-лету» («real-time», «on-the-fly») — постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна. Дело в том, что антивирус - это тоже программа, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Но существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов.

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем, на процессорах различных типов.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

**4.1. Методы поиска вирусов**

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами. Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов антивирусных программ:

**Программы-детекторы**

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

**Программы-доктора**

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

**Программы-ревизоры (инспектора)**

Программы-ревизоры (инспектора) относятся к самым надежным средствам защиты от вирусов. Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок, изучают, не забрался ли вирус в файлы, нет ли посторонних в загрузочном секторе жесткого диска, нет ли несанкционированных изменений реестра Windows. Причем инспектор может не пользоваться средствами операционной системы для обращения к дискам (а значит, активный вирус не сможет это обращение перехватить).

**Программы - фильтры (мониторы)**

Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

1. попытки коррекции файлов с расширениями COM, EXE

2. изменение атрибутов файла

3. прямая запись на диск по абсолютному адресу

4. запись в загрузочные сектора диска

5. загрузка резидентной программы.

**Вакцины или иммунизаторы**

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

**Иммунизаторы**

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса [23]. Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время.

Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натыкается на нее и считает, что система уже заражена.

Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов: одни вирусы считают уже зараженными файлы, если время создания файла содержит метку 62 секунды, а другие — 60 секунд. Однако несмотря на это, подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

**Сканеры**

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования вирусов-полиморфов.

Во многих сканерах используются также алгоритмы «эвристического сканирования», т.е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения («возможно заражен» или «не заражен») для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей.

Сканеры также можно разделить на две категории — «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на-лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам — размеры антивирусных баз, которые сканерам приходится «таскать за собой», и относительно небольшую скорость поиска вирусов.

**CRC-сканеры**

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов [24]. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

В настоящий момент существует множество антивирусных программ, однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости.

2. Не запускать незнакомые программы из сомнительных источников.

3. Стараться блокировать возможность несанкционированного изменения системных файлов.

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

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

6. Пользоваться только доверенными дистрибутивами.

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

8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Особый интерес в настоящее время представляют методы эвристического сканирования, которые рассмотрены ниже.

**4.2. Технология эвристического сканирования**

Методы эвристического сканирования не обеспечивают какой-либо гарантированной защиты от новых, отсутствующих в сигнатурном наборе компьютерных вирусов, что обусловлено использованием в качестве объекта анализа сигнатур ранее известных вирусов, а в качестве правил эвристической верификации — знаний о механизме полиморфизма сигнатур. В то же время, этот метод поиска базируется на эмпирических предположениях, полностью исключить ложные срабатывания нельзя.

В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода эмулирует работу данного вируса по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет ее с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала — программа идентифицирована [25].

Другим распространённым методом эвристического анализа, применяемым большой группой антивирусов, является декомпиляция подозрительной программы и анализ её исходного кода. Исходный код подозрительного файла проходит сверку и сравнение с исходным кодом известных вирусов и образчиков вирусной активности. В случае, если определённый процент исходного кода идентичен коду известного вируса или вирусной активности, файл отмечается как подозрительный, о чем оповещается пользователь.

**4.2.1 Недостатки эвристического сканирования**

Чрезмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фрагментов кода, выполняющего действия и/или последовательности, в том числе и свойственные некоторым вирусам. В частности, распаковщик в файлах, запакованных PE-упаковщиком (Win)Upack вызывает ложные срабатывания целого ряда антивирусных средств.

Наличие простых методик обмана эвристического анализатора. Как правило, прежде чем распространять вредоносную программу (вирус), ее разработчики исследуют существующие распространенные антивирусные продукты, различными методами избегая ее детектирование при эвристическом сканировании. К примеру, видоизменяя код, используя элементы, выполнение которых не поддерживается эмулятором кода данных антивирусов, используя шифрование части кода и др.

Несмотря на заявления и рекламные проспекты разработчиков антивирусных средств относительно совершенствования эвристических механизмов, эффективность эвристического сканирования на данный момент далека от ожидаемой. Независимые тесты компонентов эвристического анализа показывают, что уровень обнаружения новых вредоносных программ составляет не более чем 40-50 % от их числа.

Даже при успешном определении, лечение неизвестного вируса практически всегда является невозможным. Как исключение, некоторыми продуктами возможно лечение однотипных и ряда полиморфных, шифрующихся вирусов, не имеющих постоянного вирусного тела, но использующих единую методику внедрения. В таком случае, для лечения десятков и сотен вирусов может существовать одна запись в вирусной базе [25].

**4.3 Лицензионные антивирусные программы**

Выбор антивируса для домашнего пользования - актуальный вопрос, особенно для начинающих пользователей. Рано или поздно у любого возникает необходимость установки антивируса. Интересный факт, но многие пользователи вообще не устанавливают программ для защиты своего компьютера. Не устанавливают, пока не возникают различные сбои в работе системы. И действительно, при заражении компьютера вирусами замедляется работа системы, компьютер "тормозит" или "подвисает". В худшем же случае троянские программы могут похитить пароли и личную информацию. Как выбрать домашний антивирус, чтобы обезопасить себя от неприятностей попробуем разобраться.

Различные фирмы-производители программных продуктов, целенаправленно занимающиеся компьютерной и информационной безопасностью, предлагают сегодня большой выбор антивирусных программ.

Приобретение лицензионной антивирусной программы обеспечит относительно надежную защиту данных от несанкционированного доступа и использования компьютера во вредоносных целях.

Ниже представлены наиболее популярные лицензионные антивирусные программы, которые можно приобрести, в т.ч и через Интернет.

**Антивирус Касперского -**обеспечивает защиту в реальном времени от вирусов, червей, троянских коней, руткитов, adware, шпионских программ в том числе и неизвестных угроз используя проактивную защиту, которая включает HIPS-компоненты, в том числе, имеются версии для мобильных устройств (18 версий).

**Eset NOD32 -**представляет полную защиту компьютера. Комплексная защита компьютера функционирует в реальном времени и обеспечивает надежную защиту от вирусов и вредоносных программ, а так же других угроз, таких как фишинг-атаки, черви, spyware, adware и другие.Отличительной особенностью является экономичное использование ресурсов и высокая скорость исполнения (31 версия)

**Доктор Веб -**базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией (45 различных версий).

**McAfee -** эффективная защита от вирусов, шпионских и вредоносных программ. Защитное ПО постоянно сканирует и блокирует опасные электронные сообщения, содержимое опасных веб-страниц.

**4.4 Альтернатива платным программам**

Нередко встречается сегодня практика, когда производители антивирусных программ предлагают версии своих продуктов без оплаты, которые менее функциональны, чем их платные аналоги. Это делается по многим причинам, одна из главных это продвижение и популяризация своего бренда среди пользователей.

Как правило, для того чтобы продукт без оплаты полноценно работал, необходима его регистрация. Обычно она заключается в заполнении регистрационной формы, с внесением своих контактных данных.

Также в некоторых антивирусах встречается назойливая реклама, которая постоянно напоминает о необходимости купить платную версию программы. Помимо всего этого антивирус без оплаты имеет урезанный функционал. Все это можно получить, если скачать бесплатный антивирус.

Нужно отметить, что некоторые программы подобного рода смогут защитить систему не хуже коммерческих антивирусов от неизвестных или малоизвестных производителей**.**Так что скачать антивирус бесплатно или использовать пробную версию антивируса за оплату это решать уже пользователю.

Примеры бесплатных программ-антивирусов:

A**VG Anti-Virus Free Edition 2013** из раздела бесплатных антивирусов позволит обеспечить базовую защиту компьютера. Хороший вариант для домашнего пользователя, который много времени проводит в социальных сетях благодаря встроенной функции защиты AVG Social Networking Protection.

Антивирус **Аvast! Free Antivirus -**это один из лучших антивирусов среди бесплатных программ для защиты. Новое эвристическое ядро и высокая эффективность обнаружения сделали популярным avast среди пользователей всего мира.

Антивирус от **Microsoft**под названием **Security Essentials** предоставит защиту от вирусов, шпионов и других вредоносных программ. Наличие журнала проверки, планировщика, а также интуитивно понятный интерфейс для пользователей сделали этот антивирус, который распространяется бесплатно, популярным среди многих пользователей.

**5. Статистика вредоносных объектов от Касперского**

На эти вредоносные объекты пришлось 96,6% атак вредоносных программ (рис. 4) [26].

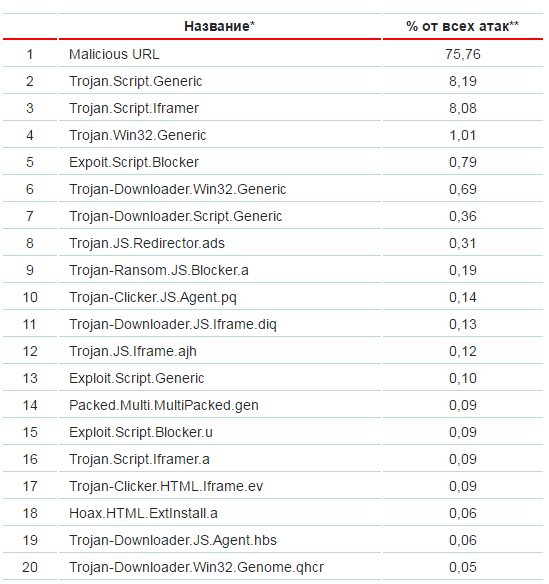
****

Рис. 4 **TOP 20 вредоносных объектов в интернете**

В TOP 20 представлены по большей части вердикты, которые присваиваются объектам, использующимся, как правило, в drive-by атаках. Они детектируются эвристически как Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic и другие. Такие объекты занимают семь позиций в рейтинге.

Malicious URL – вердикт для ссылок из нашего черного списка (ссылки на веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами, сайты-вымогатели и т.д.).

Под вердиктом Trojan.JS.Redirector.ads (8-е место) детектируется скрипт, который злоумышленники размещают на зараженных веб-ресурсах. Он перенаправляет пользователей на другие веб-сайты, например, на сайты онлайн-казино. Попадание данного вердикта в рейтинг должно служить напоминанием администраторам веб-ресурсов о легкости автоматического заражения их сайтов даже не самыми сложными программами.

**Заключение**

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

Антивирусное обеспечение и проблема удаления вирусов играет всё большую роль, т.к. количество вирусов и вирусописателей постоянно увеличивается, а вследствие этого возрастает процент вероятности заражения вирусом, т.е. возникает постоянная необходимость в профилактике компьютера от вирусов, удаления вирусов. От того как вирус внесен и что он сделает в компьютере и будут предприняты все дальнейшие шаги по удалению вирусов. Естественно он может быть внесен вне зависимости от желания владельца компьютера, через те или иные уязвимости браузеров, уязвимостей операционной системы, для подобных вещей существуют фаерволы, которые судя по названию, являются нечто вроде блокирующей стены, отслеживающие исходящие и входящие потоки данных. Но для удаления вирусов фаервол не подходит.

Имея в своем наличие наиболее удобный и четко настроенный антивирус, возможность заражения всегда остается, т.к. антивирусы, обладают лишь базой вирусов, и если кто-то напишет вирус, только под Вас, то антивирус его не определит и даст спокойно запустить, поэтому вопрос ручного удаления вирусов всегда актуален. Антивирусы нужны лишь для отсечения большого количества вирусов, гуляющих по сети, опасность потери данных с такими вирусами невелика, однако велика вероятность испортить операционную систему, сильно её затормозить и вывести её из строя и простое удаление вируса уже не поможет, необходимо будет реанимировать пострадавшую машину. Вирусов огромное количество видов, и сказать точно, что делает тот или иной невозможно, шаги по удалению вирусов принимаются по каждому индивидуально.

**Список использованной литературы**

1. https://ru.wikipedia.org/wiki/Компьютерный\_вирус

2. http://programmistan.narod.ru/useful/4.html

3. http://www.spravkapc.ru/articles/klassifikatsiya-kompyuternykh-virusov.html

4. http://www.tadviser.ru/index.php/Статья:Компьютерный\_вирус

5. http://besthuck.0pk.ru/viewtopic.php?id=29

6. http://virus-info.3dn.ru/publ/

7. http://stfw.ru/page.php?id=9120

8. http://en.wikipedia.org/wiki/Ping-Pong\_virus

9. http://moydrugpc.ru/pogovorim-o-virusah-samye-pervye-i-uzhasnye

10. http://www.anvir.net/troyanskie-programmyi.htm

11 http://mediacentr7.narod.ru/zashita/zashita.files/Page293.html

12 http://www.bezopasnik.org/dok/47.htm

14. http://kunegin.narod.ru/ref7/troya/sposob.htm

13. http://forum.kasperskyclub.ru/wiki/Троянская\_программа

15. http://www.belvit.com/publ/10-1-0-143

16. http://ru.wikipedia.org/wiki/Троянская\_программа

17. https://www.securelist.com/ru/threats/detect/trojan-programs

18. http://www.securrity.ru/terms/page\_nr4.html

19. http://it-sektor.ru/troyan-ili-troyanskiyi-kon.html

20. http://ru.wikipedia.org/wiki/Pinch

21. <http://compress.ru/article.aspx?id=10521&iid=430>

22. http://www.faqpk.ru/forum/99-208-1

23.http://www.studmed.ru/docs/document30350/власова-ла-защита-информации?page=8

24. <http://www.studfiles.ru/preview/2204125/page:6/>

25.http://www.studfiles.ru/preview/4599612/page:2/

26.https://securelist.ru/analysis/ksb/27543/kaspersky-security-bulletin-2015-osnovnaya-statistika-za-2015-god/