Содержание

...Голыми руками, хитрость против хитрости, разум против инстинкта, сила против силы, трое суток не останавливаясь, гнать оленя через бурелом, настигнуть и повалить на землю, схватив за рога...

А. и Б. Стругацкие. «Обитаемый остров»

Введение

Тема защиты компьютерной информации стала очень популярной в последние десятилетия. Связано это прежде всего с повсеместным распространением вычислительной техники, внедрением ее практически во все сферы человеческой деятельности. Любые нарушения в работе вычислительных систем с каждым годом становятся для человека все болезненнее и опаснее.

Одной из актуальнейших проблем, связанных со «здоровьем» компьютеров, является проблема защиты их от компьютерных вирусов. После 26 апреля 1999 года, когда сотни тысяч ПЭВМ в мире были выведены из строя в результате активации вируса **Win32.CIH** («Чернобыльского»), в этом уже никто не сомневается.

Но достоверной и, главное, полезной информации по вирусологической тематике немного. Существующие же публикации можно условно разделить на две группы.

Первую составляют книги и статьи, написанные «ортодоксами» – авторами известных антивирусных программ и сотрудниками организаций, занимающихся защитой компьютерной информации. Как правило, эти публикации рассчитаны на массового читателя и направлены на формирование у него лишь минимально необходимого уровня антивирусной грамотности. Технических деталей в таких публикациях мало, а конкретная информация сводится к описанию внешних проявлений различных вирусов и правил работы с теми или иными антивирусами.

Другая группа публикаций принадлежит перу «экстремистов». Эти работы содержат достаточно подробные описания конкретных алгоритмов, исходные тексты вирусов, советы по их распространению. Как правило, авторами являются люди, написавшие несколько простых вирусов и горящие желанием донести свое «умение» до всех желающих. Книги и статьи подобного сорта рассчитаны преимущественно на невзыскательных любителей «жареного». Соответ-

ственно, в них содержится слишком много эмоций и слишком мало действительно полезной информации.

Книга, которая лежит перед вами, не относится ни к первой, ни ко второй группе. Автор постарался пройти по узкой грани между «безответственным подстрекательством к написанию вирусов» и «ханжеским умолчанием необходимых подробностей». В книге рассматриваются основные принципы организации компьютерных вирусов, методики их обнаружения, изучения и обезвреживания.

Нужна ли такая книга? Представляется, что просто необходима.

Прежде всего, знание технических подробностей устройства вирусов и принципов их обнаружения поможет пользователю грамотно построить и использовать антивирусную защиту.

Во-вторых, нельзя исключить ситуацию, когда вирусолог-профессионал просто физически не успеет прийти на помощь, и рассчитывать в условиях дефицита времени придется только на свои силы, знания и умения. Такая книга может послужить в качестве учебника и справочника по самостоятельному решению проблемы.

В-третьих, компьютерная вирусология широко применяет методы самых различных областей человеческого знания: техники, информатики и математики. Изучение устройства вирусов и принципов их распознавания поможет существенно повысить свою квалификацию.

В-четвертых, в настоящее время назрела острая необходимость в специалистах, компетентных в области компьютерной вирусологии, но производители коммерческих антивирусов делятся своими знаниями и умениями лишь с узким кругом «посвященных». Не настала ли пора раскрыть некоторые их секреты?

Наконец, изучать мир компьютерных вирусов просто очень интересно!

Итак, в книге рассмотрены все типы саморазмножающихся программ, получивших распространение в последнюю четверть века:

- загрузочные вирусы;
- файловые вирусы для MS-DOS, Windows всех версий и UNIX-подобных операционных систем;
- макровирусы для MS Office;
- сетевые, почтовые и «мобильные» черви;
- «экзотические» типы вирусов.

Так называемые «троянские программы», не способные к самостоятельному размножению, в книге не рассматриваются.

Приведены необходимые сведения по системной организации различных сред, пригодных для существования компьютерных ви-

русов, – носителей информации, операционных систем, пакетов прикладных программ. Также значительная часть книги посвящена рассмотрению математических принципов и конкретных алгоритмов, лежащих в основе поиска, распознавания и удаления вредоносных программ.

Конечно, книга рассчитана на достаточно квалифицированного читателя. Необходимо владение программированием на языках Си и Ассемблер для i80x86/Pentium хотя бы на уровне институтских курсов. Для адекватного восприятия математических аспектов нелишними будут знания в рамках дисциплин «Дискретная математика» и «Дифференциальные уравнения», изучаемых на младших курсах технических вузов. Но автор надеется, что это не станет препятствием для пытливого читателя, желающего заняться увлекательнейшим занятием – охотой за компьютерными вирусами.

ГЛАВА 1

Общие сведения о компьютерных вирусах

В среде компьютерной и околокомпьютерной общественности сложилось представление о компьютерном вирусе как о некоем неуловимом электронном микроорганизме, путешествующем с машины на машину и необратимо разрушающем все, до чего способен дотянуться своими отравленными виртуальными когтями. А по страницам малонаучно-фантастических произведений и бульварных журналов кочуют «боевые вирусы» и «вирусы-убийцы», якобы разводимые и используемые нехорошими хакерами для своих зловещих целей.

Что же представляют собой компьютерные вирусы на самом деле?

1.1. Что такое «компьютерный вирус»

Пожалуйста, тогда еще одно определение, очень возвышенное и благородное.

А. и Б. Стругацкие. «Пикник на обочине»

Если углубиться в историю происхождения слова «вирус», то можно отметить, что «настоящие» болезнетворные вирусы, то есть сложные молекулы, паразитирующие на живых клетках растений и организмов, получили свое наименование в соответствии с латинским словом *virus*, которое дословно переводится как «яд». Этот термин принадлежит голландцу Мартину Бейерингу, который в самом конце XIX века в научной дискуссии с первооткрывателем вирусов русским ученым Д. И. Ивановским отстаивал гипотезу, что обнаруженные незадолго до этого странные микроскопические объекты являются ядовиты-

ми веществами. Ивановский же считал, что они «живые» и поэтому представляют собой не «вещества», но «существа». В настоящее время признано, что вирусы и не «вещества», и не «существа». Это автономные «обломки» и «испорченные детали» наследственного аппарата клеток, способные внедряться в живую клетку и «перепрограммировать» ее таким образом, чтобы она воспроизводила не себя, а все новые и новые «обломки» и «детали».

Рис. 1.1 ❖ «Настоящий» вирус и его первооткрыватели:
а) вирус «табачной мозаики»; б) Д. И. Ивановский; в) М. Бейеринг

Таким образом, в понятии «вирус» главным сейчас считается не ядовитость и вредоносность, а способность к самовоспроизведению.

Итак, компьютерный вирус – это:

программа, способная к несанкционированному созданию своих функционально идентичных копий.

В данном определении рассмотрим подробнее три ключевых понятия.

Во-первых, основным определяющим признаком вируса является умение воспроизводиться, генерировать себе подобные объекты. Именно эту часть определения имел в виду в середине 80-х годов американский математик Ф. Коэн, впервые в истории произнеся слова «компьютерный вирус» (хотя сам он уверяет, что авторство термина принадлежит его коллеге Л. Адлеману). В те годы возможность существования вирусов рассматривалась в основном только теоретически, и алгоритмы их функционирования описывались не на языках про-

граммирования, а в терминах системы команд математических формализмов типа «машины Тьюринга» или «нормальных алгоритмов Маркова».

Во-вторых, понятие «функциональной идентичности» копий вируса введено в определение ввиду того, что существует класс так называемых *полиморфных* вирусов, два различных экземпляра которых внешне могут не иметь ничего общего, но выполняют одни и те же действия в соответствии с одним и тем же алгоритмом. Таким образом, полиморфные вирусы идентичны только с точки зрения выполняемых ими функций.

Наконец, понятие «несанкционированный» означает, что вышеупомянутое создание своих копий происходит вне зависимости от желания пользователя. Любая уважающая себя операционная система (например, MS-DOS) тоже способна копировать самое себя, но вирусом не является, поскольку процесс этот происходит с ведома человека.

От компьютерных вирусов необходимо отличать так называемые *троянские программы*, не обладающие способностью к саморазмножению и предназначенные исключительно для выполнения несанкционированных (как правило, деструктивных) действий. Журналисты и малоквалифицированные пользователи часто смешивают понятия вируса и троянской программы. А ведь между «вирусами» и «троянами» такая же разница, как между «заразой» и «отравой». Мы же не говорим «отравился гриппом» или «заразился цианистым калием», верно? Вот и не надо путать!

Класс троянских программ нами рассматриваться не будет.

1.2. Несколько исторических замечаний

Это длинная история, которую к тому же изложить в общепринятых терминах очень трудно.

А. и Б. Стругацкие. «Хромая судьба»

Существует множество взглядов на историю возникновения и развития проблемы компьютерных вирусов, довольно сильно различающихся в отношении того, какие события следует считать действительно важными, в какой последовательности и когда они происходили, да и происходили ли вообще. Попытаемся и мы дать краткий очерк этой истории, основанный на синтезе различных мнений.

Прежде всего следует отметить, что идея квазиживых компьютерных организмов бытовала в художественной литературе и в массовом сознании задолго до того, как появился первый «настоящий» компьютерный вирус. Н. Н. Безруков для доказательства этого тезиса ссылается на иностранные источники [3], но можно найти и отечественные примеры. Например, в фантастическом рассказе Д. Биленкина «Философия имени», написанном в конце 70-х годов XX века, системы управления звездолета подвергаются атаке со стороны кибернетических микроорганизмов, возникших в результате «мутаций» защитно-ремонтных микроустройств корабля.

Кроме того, к моменту создания первого «настоящего» вируса уже существовало множество аналитических (например, работы фон Неймана) и программных (например, черви **Creeper** и **Xerox**) моделей, содержащих идеи самокопирования компьютерного кода. Огромную роль в разработке и изучении таких моделей сыграл американский математик Ф. Коэн. Он в первой половине 80-х годов XX века активно изучал саморазмножающиеся компьютерные механизмы с теоретических позиций, опубликовал несколько научных работ и защитил в 1986 г. на базе университета Южной Калифорнии докторскую диссертацию на вирусологическую тему.

Направление работ Ф. Коэна не было ни для кого секретом, он активно публиковался в различных научных изданиях. Поэтому некоторые эксперименты по созданию компьютерных вирусов, скорее всего, были выполнены людьми, знакомыми с его работами, – студентами и аспирантами учебных заведений. Считается, например, что вирус **Lehigh** был написан в 1986–1987 гг. студентом Лехайского университета по имени Ken van Wyk с целью практической иллюстрации теоретических разработок Ф. Коэна.

Впрочем, несколько ранее (вероятно, еще в начале 1986 г.) двумя пакистанцами, братьями Басидом и Амжадом Алви, был создан и распространился по миру в загрузочных секторах дискет вирус **Brain**, который лишь спустя несколько месяцев был обнаружен, опознан именно как «компьютерный вирус» и подробно изучен в университете штата Делавэр, США.

Известный российский программист Антон Чижов утверждал, что примерно в то же время им в исследовательских целях был написан и распространен по компьютерам московских организаций безымянный и безвредный вирус, который прожил до конца года и мирно самоуничтожился. Ни подтвердить, ни опровергнуть этого факта ни-

кто, кроме самого Чижова, не способен – в те времена вирусология еще не существовала ни как наука, ни как профессия.

1987 год принес еще ряд знаменательных событий. Ральф Бюргер (Германия) опубликовал в своей книге [36] метод заражения COM-программ и привел в качестве примера исходный текст вируса **Vienna.648**, якобы написанного кем-то другим. В Израиле были созданы вирусы семейства **Jerusalem** (Черная пятница), в Новой Зеландии – вирус **Stoned (Marijuana)**, а в Германии – вирусы семейства **Cascade**. Большинство упомянутых вирусов очень быстро распространились по миру, а некоторые из них (например, вирусы многочисленного семейства **Stoned**) встречаются изредка в загрузочных секторах дискет даже сейчас.

Авторов первых вирусов по праву можно считать очень талантливыми программистами, поскольку они самостоятельно открывали доселе неизвестные особенности операционной системы и учились пользоваться ими. Но примерно к 1988 г. начала складываться ситуация, когда в «дикой природе» оказывались не только сами вирусы, но и их тщательно прокомментированные исходные тексты. И, как следствие, наряду с оригинальными разработками стали появляться вирусы, созданные по чужому образу и подобию, например клоны вируса **Vienna**. По этому поводу хочется процитировать В. В. Маяковского:

Человек, впервые формулировавший, что «дважды два четыре», – великий математик, если даже он получил эту истину из складывания двух окурков с двумя окурками. Все дальнейшие люди, хотя бы они складывали неизмеримо большие вещи, например паровоз с паровозом, – все эти люди – не математики... Но не надо отчетность по ремонту паровозов посылать в математическое общество и требовать, чтобы она рассматривалась наряду с геометрией Лобачевского.

Видимо, вирусописатели не были знакомы с мнением великого советского поэта, поэтому количество вирусов, написанных по мотивам чужих разработок, стало увеличиваться в геометрической прогрессии.

Впрочем, далеко не все вирусописатели занимались плагиатом. Важнейшим событием 1988 г. можно считать эпидемию оригинального, намного опередившего свое время «сетевого червя», написанного Р. Моррисом, аспирантом Корнелльского университета (США). Этот вирус в течение нескольких ноябрьских дней сумел распространить-

ся по университетским и коммерческим сетям США, Канады и некоторых других стран, заразив более 6000 компьютеров.

Также к 1988 г. (по мнению Н. Н. Безрукова, [3]) следует отнести первые случаи проникновения «импортных» компьютерных вирусов на территорию СССР. Широкий общественный резонанс получили эксперименты по обнаружению и изучению вирусов, проводившиеся в 1989 г. во время работы «летней международной компьютерной школы» (г. Переславль-Залесский). Именно в эти годы появились первые удачные антивирусные программы и начали складываться коллективы людей, до настоящего времени профессионально занимающихся разработкой средств антивирусной защиты. Среди отечественных «ветеранов антивирусного фронта», которые начали серьезно заниматься проблемой защиты от компьютерных вирусов именно в те годы, можно отметить как Д. Н. Лозинского, Е. В. Касперского, Д. О. Грязнова, В. В. Богданова, так и еще несколько не менее ярких имен.

К 1990 г. во всем мире было создано всего около сотни вирусов, причем каждый новый распространялся практически беспрепятственно, вызывая более или менее широкую эпидемию. Связано это было прежде всего с недостаточной информированностью пользователей и неразвитостью средств антивирусной защиты. Но вскоре ситуация изменилась. С одной стороны, пользователи наконец-то поняли опасность бесконтрольного распространения вирусов, многие из которых содержали вредоносные фрагменты. С другой – начала набирать обороты индустрия антивирусного программного обеспечения. В нашей стране активно использовалась условно-бесплатная антивирусная программа AidsTest Д. Н. Лозинского, несколько менее популярен был пакет «Доктор Касперский» Е. В. Касперского. За рубежом лидировали комплект Scan/Clean от John McAfee, Findvirus от Alan Solomon и Norton Antivirus от Peter Norton Computing (впоследствии эта торговая марка стала собственностью фирмы Symantec). Впрочем, последний антивирус мог и «не родиться», поскольку буквально парой лет ранее, в конце 1980-х годов, Питер Нортон публично и громогласно заявлял о мифичности вирусной угрозы и сравнивал ее с угрозой крокодилов, живущих в нью-йоркской канализации. Но, к счастью, быстро сообразил «что почем» и благословил развитие антивируса, названного его именем[1].

---

[1] Кстати, спустя 15 лет появились и реальные сообщения о поимке аллигаторов в канализациях американских городов.

Разумеется, более широкое распространение получали вирусы, использующие свежие и оригинальные способы распространения и заражения. Среди «лауреатов» 1989–1991 гг. можно отметить прежде всего вирусы «болгарской сборки», связанные с разработками талантливого и плодовитого программиста по прозвищу Dark Avenger и его «сподвижников», а именно **Eddie**, **Vacsine**, **Doodle** (в том числе и знаменитый «музыкальный» **Doodle-2C.2885**) и др. Кроме того, активно подключились к процессу написания вирусов и отечественные программисты: вирусы семейств **XPEH**, **SVC**, **Voronezh** и многих других быстро распространялись по стране вместе с компьютерными играми, прикладными и системными программами, которыми обменивались между собой ничего не подозревающие пользователи. По воспоминаниям Д. Н. Лозинского, в 1990–1992 гг. ему приходилось выпускать новую версию своей антивирусной программы два раза в неделю. Не скучали и авторы других антивирусов, получивших хождение в те годы, например В. В. Богданов (AntiAPE), А. Борисов (AVSP), Alan Solomon (DrSolomon) и др.

А количество вирусов и вирусных семейств продолжало стремительно увеличиваться. И основную опасность несли не столько эпидемии профессионально написанных шедевров типа **Dir.1024** (**Driver.1024**) или «удачно» запущенных в живую природу достаточно рядовых вирусов типа **Michelangelo** (**March-6**), сколько всевозрастающая лавина простых, во многом повторяющих друг друга, короткоживущих подделок. Именно это обстоятельство в 1992–1993 гг. породило качественно новый виток в эскалации противостояния «вирус–антивирус». Авторы антивирусных программ начали использовать в своих продуктах механизм *эвристического анализа,* позволявший автоматически распознавать новые, еще не известные вирусологам экземпляры компьютерной инфекции по типичным, характерным именно для вирусов фрагментам кода и операциям. Их оппоненты ответили созданием *полиморфных вирусов*, два любых экземпляра которых хотя и работали по одному и тому же алгоритму, но не содержали внутри себя постоянных фрагментов кода. Более того, все тот же Dark Avenger сделал доступной для широких масс «заинтересованных личностей» технологию **MtE**, позволявшую достаточно просто подключать механизм полиморфности к любому вирусу, даже самому примитивному, многократно увеличивая тем самым его сопротивляемость к обнаружению.

Середина 90-х годов прошла под знаком борьбы именно с высокосложными, подчас *многоплатформенными* (то есть способными

заражать программы различных типов) вирусами. Шанс на распространение получали только очень изощренные вирусы, например принадлежащие к семействам **OneHalf**, **Natas**, **Zhenghi**, **Ukraine**, **NutCracker**, **RDA.Fighter**, **Kaczor** и др., написать которые мог далеко не каждый программист. В свою очередь, вирусологи взяли на вооружение крайне сложные механизмы *эмуляции кода*, позволявшие имитировать исполнение программ и реагировать уже не столько на подозрительные фрагменты программ, сколько на их подозрительные действия. На смену простым антивирусам типа AidsTest приходили более сложные разработки, например DrWeb питерца И. Данилова. Ситуация несколько стабилизировалась, но ненадолго.

Ко второй половине 90-х годов большинство пользователей уже перешло в своей работе на операционные системы семейства MS Windows. Изменились каналы распространения и содержание файлов, копируемых с компьютера на компьютер. На смену дискетам пришли компакт-диски и глобальные сети. Все чаще вместо игр и утилит с компьютера на компьютер передавались изображения, базы данных, документы. Вирусы, заражающие такие якобы «неисполнимые» файлы, просто обязаны были появиться, и они появились! Первой ласточкой стал так называемый *макровирус* **Macro.Word.Concept** (лето 1995 г.), заражавший специализированные программы на макроязыке WordBasic, которые содержались внутри документов текстового процессора MS Word. Потом количество макровирусов стало увеличиваться с такой же скоростью, с какой всего за несколько лет до этого множились MS-DOS-вирусы. Появились макровирусы для электронных таблиц MS Excel (например, знаменитый **Macro.Excel.Laroux**) и баз данных MS Access. Был освоен макроязык VBA, который фирмой Microsoft «поставлялся на вооружение» вместе с новыми версиями MS Office. Пик распространенности макровирусов пришелся на 1998–2000 годы, среди «лауреатов» можно назвать **Macro.Word.Cap**, **Macro.Word97.Class**, **Macro.Word97.Ethan**, **Macro.Word97.Marker**, **Macro.Word97.Thus** и прочих. В новом веке количество вновь создаваемых макровирусов заметно уменьшилось, а через несколько лет и вовсе сошло на нет.

Кроме того, к 1996 г. вирусописателями были наконец-то разработаны способы простого и надежного заражения Windows-программ. Конечно, написание Windows-вирусов – не такая простая задача и требует достаточно высокой квалификации, но в условиях неразвитости соответствующего антивирусного обеспечения и неверия пользователей в возможность распространения Windows-«заразы»

повторилась ситуация конца 80-х годов. Относительно немногочисленные Windows-вирусы сумели быстро распространиться по всему миру. Апофеозом стала активация вируса **Win9X.CIH** («Чернобыльского») в апреле 1999 г., которая привела к повреждению сотен тысяч компьютеров во всем мире. Годом позже «прогремел» чрезвычайно заразный вирус **Win32.FunLove**, источниками распространения которого неоднократно становились случайно инфицированные дистрибутивы, размещенные на интернет-сайтах крупнейших производителей программного обеспечения. А потом Windows-вирусы тоже отошли на второй план, хотя программно-аппаратные условия, содействующие их существованию и распространению, не изменились и остаются относительно благоприятными для этого вида «заразы» до сих пор.

Вместо этого вирусописатели принялись активно осваивать новые пути распространения «заразы» – через глобальную сеть Интернет. Очень простой по идее и реализации вирус-червь **Melissa** в том же апреле 1999 г. за несколько суток сумел многократно «обежать» всю планету, вызвав панику среди пользователей и системных администраторов. Следующая пятилетка запомнилась в основном молниеносными по скорости «расползания» и исключительно обширными по распространенности эпидемиями сетевых и почтовых вирусов и червей **VBS.LoveLetter**, **E-Worm.Win32.Swen**, **E-Worm.Win32.Klez**, **Net-Worm.Win32.LoveSan**, **E-Worm.Win32.MyDoom**, **Net-Worm.Win32.Sasser** и прочих. В 2005 году появились признаки того, что и эти эпидемии стали потихоньку стихать. На смену глобальным эпидемиям нескольких десятков различных червей пришли практически не прекращающиеся «микроэпидемии», вызываемые массами мелких модификаций нескольких «базовых разработок», – например, одних только разновидностей червя **Bagle** насчитывается несколько тысяч. Кроме того, сохранили умеренную актуальность и вирусы «старых» типов, просто про них стали меньше говорить. В мировых масштабах они «не делают погоды», но встречаются в «дикой природе» до сих пор.

Почему же поколения вирусов сменяют друг друга без, казалось бы, достаточно веских объективных причин? Дело в том, что сильное влияние на мировую вирусную «погоду» оказывает субъективный социальный фактор, известный под названием «мода». В условиях растущего противодействия, оказываемого вирусам со стороны вирусологов и пользователей, неорганизованное вирусописательское сообщество мечется, бросается из одной крайности в другую,

в любой момент готово изменить направление своей деятельности, если это изменение обещает возможность «прославиться» проще и быстрее. Кроме того, у значительной части киберандеграунда в последние годы изменилась мотивация, так что «слава» стала цениться куда меньше, чем «деньги» и «власть». Это привело к массовым миграциям бывших вирусописателей в стан «троянщиков», то есть в стан производителей самостоятельно не размножающегося, но крайне вредоносного (похищающего конфиденциальную информацию, рассылающего спам и т. п.) программного обеспечения. Наконец, созданием вредоносных программ профессионально занялись структуры (вероятно, спецслужбы и силовые ведомства различных стран), которые заинтересованы не в массовых эпидемиях, а в точечных атаках на ограниченный круг целей. Так, например, в создании и распространении «шпионских программ» **Magic Lantern** (2001 г.) и **R2D2** (2011 г.) подозревают ФБР США и полицию ФРГ соответственно, а авторство «боевого» червя **Stuxnet** (2010 г.) приписывают тем политическим структурам, которым не выгодно развитие ядерной программы Ирана.

Настоящее время характеризуется появлением все новых и новых типов вирусов, активно осваивающих многочисленные «дыры» в защитных механизмах информационных систем. Количество обнаруженных потенциальных целей для заражения вирусами увеличивается с каждым годом. Вирусы научились распространяться не только вместе с программами, документами, электронными таблицами и html-страницами, но и вместе с базами данных, изображениями, архивами, и даже освоили сотовую телефонную связь. Кроме того, старые «дыры» тоже еще полностью не залатаны, и традиционные типы вирусов по-прежнему в любой момент способны «осчастливить» мировое компьютерное сообщество своим присутствием.

Ближайшие несколько лет обещают немало ярких и интересных событий на фронте антивирусной борьбы.

1.3. Какие бывают вирусы

Азарт классификатора и коллекционера вдруг пробудился в нем.

А. и Б. Стругацкие. «Отягощенные злом»

Ранее мы уже использовали ряд терминов, относящихся к различным типам вирусов. Теперь рассмотрим эти классификации подробнее.

1.3.1. Классификация по способу использования ресурсов

В настоящее время целесообразно различать *вирусы-паразиты* (или просто *вирусы*) и *вирусы-черви* (или просто *черви*).

Первые размножаются с использованием ресурсов, принадлежащих другим программам. Например, они внедряются внутрь этих программ и активируются вместе с их запуском.

Вторые, как правило, используют только ресурсы вычислительных систем (оперативную и долговременную память, непрограммные файлы), рассылая свои копии по сетям, раскладывая их по носителям информации, буферам памяти, чужим архивам и т. п. Черви автономны, к другим программам они не прикрепляются.

1.3.2. Классификация по типу заражаемых объектов

В соответствии с этой классификацией вирусы можно разделить на *программные*, *загрузочные*, *макровирусы* и *многоплатформенные* вирусы.

Программные вирусы заражают файлы других программ. Пример: вирус **Win9X.CIH**, паразитирующий на Windows-программах.

Загрузочные вирусы заражают или подменяют маленькие программки, находящиеся в загрузочных секторах жестких дисков, дискет и флэшек. Примером может служить вирус **Michelangelo**.

Питательной средой для *макровирусов* служат «макросы» или «скрипты», то есть специализированные программные компоненты, написанные на *языках сценариев* и находящиеся внутри файлов различных офисных приложений – документов MS Word, электронных таблиц MS Excel, изображений Corel Draw и прочего. Примеры: вирус **Concept**, заражающий документы MS Word; вирус **Laroux**, заражающий Excel-таблицы.

Многоплатформенные вирусы паразитируют одновременно на объектах различных типов. Например, вирус **OneHalf.3544** заражает как программы MS-DOS, так и загрузочные сектора винчестеров. А вирусы семейства **Anarchy**, кроме программ MS-DOS и Windows, способны заражать также документы MS Word.

1.3.3. Классификация по принципам активации

По этому признаку вирусы целесообразно разделить на *резидентные* и *нерезидентные*.

Резидентные вирусы постоянно находятся в памяти компьютера в активном состоянии, отслеживают попытки обращения к жертвам со стороны других программ и операционной системы и только тогда заражают их. Например, исполнимые программы заражаются в момент запуска, завершения работы или копирования их файлов, а загрузочные сектора – в момент обращения к дискетам. Примерами подобных вирусов являются все те же **OneHalf.3544** (в среде MS-DOS) и **Win9X.CIH** (в среде Windows 95/98/ME).

Нерезидентные вирусы запускаются в момент старта зараженных носителей, время их активности ограничено. Например, вирус **Vienna.648** «бодрствует» только несколько мгновений сразу после запуска зараженной им программы, но за это время успевает найти на диске множество новых жертв и прикрепиться к ним, а потом передает управление своему носителю и «засыпает» до следующего запуска.

В многозадачных операционных системах возможны «*полурезидентные*» вирусы: они стартуют как нерезидентные, организуют себя в виде отдельного потока запущенной программы, весь срок работы этой программы ведут себя словно резидентные, а потом завершают работу вместе с программой-носителем. Пример – **Win32.Funlove.4070**.

1.3.4. Классификация по способу организации программного кода

Этот таксономический признак позволяет выделять *незашифрованные*, *зашифрованные* и *полиморфные* вирусы.

Незашифрованные вирусы представляют собой простые программы, код которых не подвергается никакой дополнительной обработке. Такие вирусы (например, **Vienna.648**) легко обнаруживать в программах, исследовать при помощи дизассемблеров и декомпиляторов и удалять.

Код *зашифрованных вирусов*, как правило, подвергается некоторым видоизменениям. Вирус заражает жертвы своей зашифрованной копией, а после старта расшифровывает ее в памяти ЭВМ. При обнаружении, изучении и удалении таких вирусов возникают трудности, так как вирусологу необходимо как минимум выполнить обратную операцию – расшифровку кода. Обычно зашифровка вирусов сопровождается использованием в коде специальных антиотладочных приемов. Пример такого вируса – **Sayha.Diehard**.

Наконец, *полиморфные вирусы* – это разновидность зашифрованных вирусов, которые меняют свой двоичный образ от экземпляра к экземпляру. Например, полиморфными являются все вирусы семейства **OneHalf**. Частным случаем полиморфных являются *метаморфные* вирусы, которые не шифруют двоичный образ своего тела, а просто переставляют местами его команды и заменяют их аналогами, выполняющими те же действия. Пример: **Win32.ZMyst**.

1.3.5. Классификация вирусов-червей

Чаще всего она выполняется по способу распространения. *Почтовые черви* (например, **E-Worm.Win32.Aliz**) распространяются по электронной почте, в виде вложений («аттачей») в электронные письма. *Сетевые черви* (их еще иногда называют «*интернет-червями*»), такие как, например, **Net-Worm.Win32.Lovesan**, используют для своего распространения непосредственно сетевые протоколы и рассылают себя внутри информационных пакетов. «*Телефонные*», или «*мобильные*», *черви* (например, **Cabir**), являющиеся разновидностью «сетевых», при самораспространении пользуются специфическими протоколами беспроводного информационного обмена, такими как BlueTooth. А известные еще с 1980-х годов *файловые черви* (например, **Mkworm.715**) самостоятельно не распространяются с компьютера на компьютер, вместо этого они раскладывают свои многочисленные копии по различным каталогам различных носителей информации и «засовывают» их в ZIP- и RAR-архивы.

1.3.6. Прочие классификации

Существует еще немало вирусных таксономий, порой довольно странных. Например, юристам выгодно делить все вирусы на «*вульгарные*» (состоящие из единого неделимого фрагмента) и «*раздробленные*» (состоящие из отдельных фрагментов, не являющихся вирусами, но способных объединяться в одну вирусную программу). А журналисты, не имеющие никакого представления о реальном устройстве и возможностях вирусов, обсуждают «четыре поколения деструктивности», причем вирусы, принадлежащие последнему поколению, якобы способны воздействовать аж на человеческий мозг.

Разумеется, нас подобная «ненаучная фантастика» интересовать не будет.