Февраль 1991 г. *Том 161, № 2*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

МЕТОДИЧЕСКИЕ ЗАМЕТКИ

От редакции. Компьютеры стали неотъемлемым орудием работы физиков. Редакция надеется, что публикуемая статья, написанная физиком, будет полезна широкому кругу читателей журнала.

621.142

КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕТОДЫ БОРЬБЫ С НИМИ

Г. Л. Ландсберг

(Институт физики высоких энергий, Протвино, Московская обл.)

СОДЕРЖАНИЕ

Преамбула. Компьютерные вирусы... Термин, который, благодаря тщаниям журналистов, знают теперь даже люди, далекие от ЭВМ. Атмосфера некой таинственности и суеверного ужаса окружает эти искусственно созданные программы, предназначенные для уничтожения данных на магнитных дисках, замедления работы компьютеров, создания помех действиям пользователей. Так ли страшны и загадочны вирусы? Как они действуют? Какой арсенал средств предлагает «компьютерная медицина» для борьбы с ними?

Настоящий обзор дает ответы на эти и некоторые другие вопросы. В основном он посвящен вирусам на IBM PC-совместимых компьютерах с распространенной операционной системой MS DOS [1], хотя содержит информацию и о вирусах на других персональных компьютерах, а также на больших ЭВМ. Обзор рассчитан как на «рядовых» пользователей IBM PC, так и на системных программистов. Для людей, слабо знакомых со структурой операционной системы MS DOS, приводятся все необходимые для понимания настоящей статьи сведения.

Введение содержит объяснение некоторых терминов, встречающихся в тексте, и краткое описание принципов работы MS DOS (в объеме, необходимом для объяснения механизмов действия вирусов). В первом разделе рассмотрена «анатомия» вирусных программ, приведена их классификация и описаны основные способы размножения. Второй раздел посвящен различным программам-антивирусам. В третьем разделе рассмотрены конкретные, наиболее распространенные в СССР вирусы и приведены рекомендации по их «лечению». Четвертый раздел содержит краткое описание универсальной антивирусной системы PHENIX, которой посвящен отдельный препринт [2].

Данный обзор представляет собой попытку собрать воедино и критически проанализировать многочисленные и часто противоречивые сведения, содержащиеся в различных публикациях на эту тему (статьи в специализированных и популярных журналах, препринты, книги, описания программ-антивирусов и др.).

Следует иметь в виду, что компьютерная вирусология — довольно новая область знания. В мире она фактически развивается с 1988 г., а в СССР — с 1989 г. В настоящее время организованы постоянно действующие семинары по вирусам в г. Киеве (руководитель Н. Н. Безруков), наиболее интересные результаты которого публикуются в бюллетене «СОФТПАНОРАМА», и в Москве (руководитель Л. Г. Бунич).

После первой, весьма пространной, отечественной статьи [3] А. А. Чижова, посвященной вирусам, появилось несколько довольно подробных работ, среди которых наиболее содержательными представляются препринт [4] Н. Н. Безрукова и ряд статей И. Ш. Карасика в журналах «Интеркомпьютер» [5, 6] и «Мир ПК» [7]. Имеются многочисленные зарубежные публикации, посвященные вирусам. Большая часть из них носит характер специальных сообщений в компьютерных журналах (например, [8—14]), однако, есть и книги, содержащие обзор ситуации с вирусами [15, 16]. К сожалению, число новых видов вирусов и «штаммов» уже известных вирусных программ постоянно растет, поэтому информация в подобных обзорах быстро устаревает. В настоящей статье основное внимание уделяется принципам действия вирусов и антивирусов, а конкретные их типы рассматриваются лишь в качестве иллюстраций (кроме раздела 3, посвященного современной ситуации с вирусами в СССР).

Введение. Начнем с терминологии.

Компьютерный вирус — искусственно созданная программа, обладающая способностью к скрытому саморазмножению в операционной среде компьютера посредством включения в исполняемый код (загружаемые программы, элементы операционной системы, компилируемый текст, командные файлы) своей, возможно, модифицированной копии, сохраняющей способность к самовоспроизведению. Обычно вирус служит для создания тех или иных помех в работе пользователей, уничтожения данных на магнитных носителях или разрушения элементов аппаратного обеспечения ЭВМ (дисководы, мониторы). Это — модифицированный вариант определения, данного Ф. Коуэном (F. Cohen) в статье [17], являющейся одной из первых серьезных работ в области математического исследования вирусов.

Антивирус — программа, предназначенная для локализации и уничтожения вируса на конкретном компьютере. Хорошие антивирусы способны ликвидировать также некоторые разрушения, создаваемые вирусами, например, восстанавливать зараженные файлы.

Командный интерпретатор — часть операционной системы, представляющая собой интерфейс с пользователем. В системе MS DOS стандартным интерпретатором является COMMAND. COM, однако, существуют и другие интерпретаторы, совместимые с этой операционной системой (например, 4DOS. COM фирмы «J. P. Software»).

Защита файлов и ядра операционной системы — специальные меры, препятствующие случайному стиранию файлов, а также изменению содержимого памяти, занимаемого операционной системой. На больших ЭВМ защите уделяется много внимания; обычно она весьма сложна и имеет несколько уровней. Операционная система MS DOS, концептуально рассчитанная на одного пользователя, вообще не имеет защиты памяти. Примитивные средства защиты файловой системы в ней существуют (так называемый атрибут Readonly, который не дает открывать файл для записи или стирать его), однако они очень просты и служат скорее для предупреждения, а не для собственно защиты, так как любая программа может изменить этот атрибут, после чего модифицировать файл по своему усмотрению.

Прерывание — специальная ситуация, возникающая при работе компьютера, в которой управление передается так называемой программе обработки прерывания. Различают hardware-прерывания, предназначенные для обслуживания устройств ввода — вывода, таймера и т. п. На конкретном компьютере они не зависят от операционной системы, так как выполняются аппаратно. Программы обработки этих прерываний обычно содержатся в ROM (read only memory). На компьютерах типа IBM PC они составляют часть BIOS (Basis Input-Output System). Кроме того, существуют и software-прерывания, поддерживаемые какой-либо операционной системой. Они фактически представляют собой интерфейс между программами пользователя и системой. Адреса точек входа в программы обработки прерываний на IBM PC хранятся в младших адресах оперативной памяти (таблица векторов прерываний).

Загрузочный сектор — нулевой сектор логического диска (партиции (partition) на жестком диске) или дискеты, предназначенные для хранения кода начальной загрузки операционной системы. Структура этого сектора подробно описана в [1, 6].

Главный загрузочный сектор (Master Boot Record, MBR) — первый абсолютный сектор жесткого диска на IBM PC-совместимых компьютерах. Содержит сведения о делении жесткого диска на партиции (таблица партиций), информацию о том, какая партиция является загружаемой (т. е. содержит операционную систему), а также программный код, помещающий в оперативную память содержимое загрузочного сектора такой партиции и передающий управление на начало находящейся там программы. Структура MBR детально рассмотрена в [1, 6].

Теперь коснемся принципов работы MS DOS на IBM PC-совместимых ЭВМ. При включении компьютера управление передается специальной программе POST (Power On Self Test), находящейся в ROMe и тестирующей память, контроллеры и другие элементы электроники. При удачном завершении тестов производится попытка загрузки операционной системы с гибкого диска в нулевом дисководе (логическое имя A:). При отсутствии в нем дискеты управление передается программе, находящейся в главном загрузочном секторе, которая, согласно таблице партиций, в свою очередь передает управление программе, расположенной в нулевом секторе загружаемой партиции. Этот boot-код загружает собственно операционную систему (что также происходит в несколько стадий, но их

описание выходит за рамки настоящей статьи). Командный интерпретатор COMMAND. COM, которому передается управление в случае успеха, загружается в оперативную память не целиком. Постоянно в памяти находится лишь малая его часть (около 4 Кбайт). При выполнении некоторых команд DOS интерпретатор подгружается с диска.

Осталось кратко описать формат исполняемых модулей системы MS DOS. Микропроцессоры Intel 8086/88 и 80286 (являющиеся базовыми для IBM PC/XT и IBM PC/AT соответственно) имеют 16-разрядное слово. Система команд этих процессоров позволяет использовать 16-битный адрес (операторы и операнды типа near), что соответствует 64 Кбайтам памяти или одному сегменту. Однако существует возможность использования 20-битного адреса, задаваемого парой 16-битных слов segment и offset[1] ●. При этом операторы и операнды имеют тип far, и объем адресуемой памяти возрастает до 1 Мбайта. Микропроцессор Intel 80386, базовый для IBM PC/AT-386 или IBM PC/SuperAT, имеет 32-битный адрес, однако, MS DOS использует его возможность эмуляции 16-битной моды работы, поэтому, с точки зрения этой операционной системы, все четыре процессора одинаковы и различаются лишь быстродействием [2] ●.

В связи с такой архитектурой микропроцессоров MS DOS поддерживает два типа исполняемых модулей. Одни, так называемые COM-программы (файлы, содержащие их код, обычно имеют расширение .COM), должны иметь размер, не превышающий 64 Кбайтов, и поэтому состоят обычно лишь из команд типа near. Способ загрузки их в память чрезвычайно прост: текст файла располагается в каком-либо ее сегменте, начиная с адреса l00h [3] ●. Программы, длина которых превышает 64 Кбайта, устроены несколько по-другому. Они могут содержать любые команды и операторы (как типа near, так и far) и состоять их нескольких относительных (relocatable) модулей. Такие файлы обычно имеют расширение .EXE и в начале содержат стандартный заголовок, в котором размещаются: таблица относительных модулей, начальные значения счетчика команд IP и указателя стека SP, а также некоторая другая служебная информация. При загрузке такого файла (он имеет первые два байта, содержащие символы 'MZ' (5Dh, 4Ah) — так называемая сигнатура EXE-модуля) операционная система прибавляет соответствующие смещения ко всем far адресам относительных модулей, хранящимся в таблице, после чего устанавливает начальные значения регистров SS, SP, CS и IP, тем самым передавая управление в точку входа исполняемой программы. Загрузка и выполнение EXE- и COM-модулей происходит при вызове DOSовского прерывания 21h (основное внутреннее прерывание MS DOS), точнее его подфункции 4Bh. Подробнее структура заголовка EXE-файла описана в [1].

Перед окончанием своей работы программа вызывает прерывание 20h, которое восстанавливает значение векторов некоторых прерываний (они могли быть изменены во время работы программы), освобождает занимаемую ею оперативную память, после чего передает управление той программе (программа-родитель), которая выдавала запрос на исполнение только что завершившего свое функционирование модуля (обычно это — командный интерпретатор, но может быть и другая программа, например, Norton Commander, PCShell и т. п.). Другой возможный способ окончания работы программы — оставление своего тела резидентным в памяти (Terminate but Stay Resident, TSR), что осуществляется при вызове прерывания 27h. В этом случае операционная система резервирует часть памяти, занимаемой исполняемым модулем, и не освобождает ее при пе-

редаче управления программе-родителю. Такой механизм завершения позволяет реализовывать процедуры обработки прерываний, отличные от стандартных DOSовских и BIOSовских, а также создавать программы, активизирующиеся при определенных условиях (нажатие какого-либо сочетания клавиш, заданное время суток и т. п.).

Вот и все, что нужно знать об операционной системе MS DOS для понимания механизма действия вирусов.

1. Что такое вирусы? Этот раздел целиком посвящен различным типам вирусов. Он содержит некоторые исторические сведения, описание механизмов размножения и активизации вирусов, типичные проявления их деятельности, признаки зараженности компьютеров, а также попытки классификации вирусных программ.

1.1. Немного истории.

> «...Таковым же образом утаено... из каковых дальних пределов чтойность ктойности нашей почерпнула свою причинность...».
>
> *Дж. Джойс* «Улисс»

История появления вирусов весьма запутана. Официальной версии об их возникновении не существует, и среди историографов ведется борьба за отодвигание момента создания первых вирусных программ все дальше в прошлое. В связи с этим представляется разумным избежать неоднозначных утверждений и остановиться лишь на основных исторических вехах, предшествующих появлению вирусов.

Впервые возможность существования вирусов была теоретически доказана знаменитым американским математиком Джоном фон Нейманом в 1949 г. в работе «Theory and Organization of Complicated Automata». Нейман показал, что достаточно сложный автомат может обладать способностью к размножению. Попытки практической реализации самовоспроизводящихся автоматов появились много позже.

В 1959 г. в журнале «Scientific American» появляется статья Л. С. Пенроуза (L. S. Penrose) о самовоспроизводящихся механизмах, на основе которой F. G. Stahl создает программу для IBM 650, моделирующую борьбу за выживание среди существ, «пожирающих» ненулевые слова в машинной памяти, в том числе и друг друга. После «съедания» определенного количества слов, организм порождает себе подобный (с возможностью мутаций). Если за достаточно большое количество «ходов» существо не «поедает» ни одного ненулевого слова, оно «умирает от голода». Однако низкое быстродействие и малый объем оперативной памяти компьютера не позволили получить интересных результатов. Подробности, связанные с этой программой, можно найти в обзоре [18].

Приблизительно в 1962 г. сотрудник фирмы «AT &TBell Laboratories» V. A. Vysotsky изобрел игру «Darvin», в которой программы-организмы боролись за жизненное пространство в оперативной памяти компьютера. Здесь тоже прослеживается связь с вирусной тематикой и биологической борьбой за существование. Статья об этой игре появилась лишь десятью годами позже в журнале «Software: Practice and Experience». Развитием идеи «Darvin» стала популярная игра «Бой в памяти» («Core war»), описанная в [19].

В 1982 г. сотрудники фирмы XEROX создают программу — «червь» [20], способную «переползать» на различные компьютеры (объединенные

в сеть) с целью оптимального использования машинных ресурсов. Предполагалось, что ночью такая программа может работать сразу на большом количестве ЭВМ, а днем, когда компьютеры загружены, она занимает лишь базовую машину, для того чтобы не мешать остальным пользователям.

В 1983 г. Ken Tompson получает премию Ассоциации по вычислительной технике (Association for Computer Machinery) за демонстрацию вирусного кода. В то время еще не знали, сколько вреда принесут вирусы всего через несколько лет!

С конца 1987 г. отмечается массовое распространение вирусов на персональных компьютерах типа IBM PC. К 1990 г. из число превышает 70 и имеет устойчивую тенденцию к росту. Первыми вирусами на IBM PC-совместимых компьютерах были Lehigh (обнаружен в Лехайском университете, США) и Jerusalem (обнаружен в Иерусалимском университете, Израиль), о которых сказано ниже, а также в работах [4, 6, 8, 9].

Совмещение функции размножения с вредительством наблюдается даже у первых MS DOS-вирусов. Надо сказать, что это неудивительно. Дело в том, что еще до появления вирусов существовали программы, направленные на уничтожение данных. Простейшие из них (так называемые «логические бомбы») создавались в качестве мести. Например, служащий, разрабатывающий систему банковского учета, помещал проверку на наличие своей фамилии в каталогах для получения заработной платы. В случае ее отсутствия (увольнение работника) происходила та или иная порча данных, устранение которой могло обойтись весьма дорого.

Позднее появляются так называемые «троянские программы», обычно маскирующие свою вредительскую деятельность какими-либо полезными функциями. Например, программа, находящая плохие кластеры на дисках, может в действительности медленно создавать их; программы, оптимизирующие диск,— приводить к постепенной потере файлов и т. п. Подробный список «троянских» программ для IBM PC-совместимых компьютеров, известных к моменту публикации, помещен в августовском номере журнала «PC World» за 1988 г. Более подробные сведения о «Троянской войне» можно найти в обзоре [21].

Однако только с появлением вирусов отдельные случаи порчи данных приобретают массовый характер. Однажды выпущенный из-под контроля вирус уже не может быть до конца уничтожен, так как хранится и появляется вновь и вновь из архивов, вирусных «коллекций» и т. п. По некоторым гипотезам, первые MS DOS-вирусы предполагались как наказание за незаконное копирование программного обеспечения. Но, как показала практика, чаще всего страдают не непосредственные виновники, а третьи лица. С появлением и распространением компьютерных сетей могут пострадать даже ни в чем не повинные пользователи.

Проблема защиты от вирусов приобрела столь серьезное значение, что многие страны приняли ряд законов, предусматривающих уголовную ответственность за умышленное создание и распространение вирусов. Так, в США на рассмотрение Конгресса внесены билли 55 (Virus Eradiation Act) и 287 (Computer Protection Act) [22], предусматривающие крупные денежные штрафы или тюремное заключение сроком до 15 лет за преднамеренную порчу программного обеспечения. Многие компьютерные фирмы и ассоциации пользователей персональных ЭВМ обращаются в свои правительства с целью установления высшего приоритета для исследований, связанных с защитой от вирусов [23].

К счастью для пользователей, существует эмпирическое правило, отмечаемое во многих публикациях (например, в [4]), согласно которому, чем грамотней и красивее написана вирусная программа, тем меньше вреда она обычно приносит. Чаще всего, действие подобных вирусов сводится к изощренным визуальным или звуковым эффектам («осыпание» букв на экране, исполнение мелодии и т. п.). Однако и самый безобидный вирус может быть легко модифицирован даже не очень квалифицированным программистом так, что он будет производить разрушения. Кстати, наибольшее количество «штаммов» известных вирусов возникло именно таким образом.

Обычно вирусы переносятся компьютерными играми и ...антивирусами. Игры являются наиболее часто несанкционированно обмениваемым программным продуктом, причем пользуются ими все, в том числе и пользователи, не знающие о том, как определить наличие вируса до наступления необратимых последствий его деятельности [1] ●. Антивирусы же предназначены для работы в опасной близости с вирусами, поэтому тоже часто оказываются зараженными.

Следует еще раз подчеркнуть сходство компьютерных вирусов с биологическими:

— и те и другие способны к размножению и мутациям;

— человек является переносчиком обоих типов вирусов;

— не от всех вирусов своевременно появляется противоядие;

— невозможно создать универсальное лекарство против всех вирусов, хотя для каждого конкретного вируса оно рано или поздно создается.

Если не предпринимать решительных мер по борьбе с компьютерными вирусами, очень скоро может наступить настоящая борьба за существование, но уже не между отдельными программами в памяти компьютера, а между *вирусами* и *пользователями персональных ЭВМ*. Чтобы победить в этой войне, нужно знать врага «в лицо». Для этого стоит прочитать следующий раздел.

1.2. Вирусы под микроскопом. Перед тем как перейти к рассмотрению вирусов для IBM PC-совместимых компьютеров, существование которых не вызывает сомнений, поговорим немного о вирусах на других ЭВМ.

1.2.1. *Бывают ли вирусы на больших ЭВМ?*

«На этот вопрос мы отвечаем положительно: Да, Бога нет!».

А. Зиновьев

На больших ЭВМ, т. е. на компьютерах с разделением времени и многопользовательскими операционными системами, настоящие вирусы проявляются крайне редко. Многочисленные публикации на эту тему в газетах и популярных журналах чаще всего являются «дутыми» сенсациями и свидетельством некомпетентности отдельных журналистов, пользователей и даже системных программистов. На это указывают многие специалисты по вирусам (см. [4, 24]).

Дело в том, что операционные системы, предназначенные для одновременного обслуживания большого числа пользователей, имеют довольно сложные системы защиты файлов и оперативной памяти, предназначенные для обеспечения независимой работы разных программистов. Чаще всего такая защита производится аппаратными методами и преодолеть ее крайне трудно. Вместе с тем, даже если квалифицированный программист сможет «взломать» операционную систему (подобрав, например, па-

роль) и внедрить в нее вирус, удалить его очень просто. Более того, относительно несложно «вычислить» человека, создавшего вирус (например, по содержимому backup-лент, терминалу, с которого производился подбор пароля и т. д.). Не стоит сомневаться, что такого хэкера [5] ●ждет серьезное уголовное наказание. Таким образом, «игра не стоит свеч».

Видимо, поэтому единственным достоверно известным случаем вирусного поражения больших компьютеров был прецедент заражения в США около 2000 ЭВМ типа SUN-3 и VAX, объединенных в сеть Internet, вирусом Морриса [4, 24] 2 ноября 1988 г. (кстати, до вступления в силу серьезных федеральных законов, препятствующих распространению вирусов). Вирус был создан Робертом Моррисом младшим (Robert Morris), аспирантом факультета информатики Корнельского университета (США). При написании вируса использовалась ошибка в стандартном программном обеспечении системы UNIX, которая функционировала на большинстве машин, объединенных в сеть. Под UNIXом существуют так называемые процессы-«демоны», не связанные ни с одним пользователем. Одним из таких «демонов» является программа fingerd, позволяющая получить информацию о других пользователях на данном компьютере. Вирус посылал по сети запрос к fingerd, однако, передавал «демону» слишком много информации, в результате чего она переполняла буфер и записывалась в ту область памяти, где находился код самого «демона». Таким образом, на место fingerd оказывалась записанной простая программа, выдающая запрос на передачу ей с того компьютера, который обращался к «демону», короткого (99 строк) модуля, написанного на языке С,— стандартном для UNIX. Затем модифицированный fingerd обращался к операционной системе с командой на трансляцию этой программы, после чего запускал ее. Программа уничтожала все следы, «пряталась» в операционной системе, а затем по очереди запрашивала и запускала специальные модули, предназначенные для определения следующих кандидатов для заражения. При этом использовались тонкие процедуры для определения паролей пользователей. При получении имени следующего узла в сети модуль распространения посылал запрос «демону» на этой машине, тем самым обеспечивая размножение вируса. Общая длина всех элементов вирусной программы достигала 68 Кбайт. Это — самый длинный из известных к 1990 г. вирусных кодов.

Из-за ошибки в программе, однако, вирус распространялся слишком быстро, и уже через несколько часов более 1000 ЭВМ оказалось заражено, причем на некоторых из них работа фактически остановилась, настолько они были загружены передачей вируса на другие компьютеры. Это сильно затруднило обмен информацией между системными программистами, разрабатывающими средства борьбы с вирусом, так как электронная почта стала работать очень ненадежно. Тем не менее, к вечеру 3 ноября вирус был уничтожен, а в операционных системах ликвидированы ошибки, сделавшие возможным его распространение. Хотя вирус и не привел ни к каким разрушениям, а лишь парализовал работу пользователей на полтора дня, Моррис был исключен из университета сроком на 2 года. Рассматривалась возможность привлечения его к суду по существовавшим в то время уголовным статьям [6] ●.

Кроме вируса Морриса, существуют еще несколько программ-червей, которые пытаются проникнуть в операционные системы, пользуясь стандартными именами директорий и паролями. Однако серьезного распространения они не получили, так как немедленно выявляются по большому числу неудачных попыток входа в систему. Кроме того, пароли системных

директорий обычно периодически меняются, поэтому такие черви сделаны скорее ради шутки, а не с целью заражения большого числа ЭВМ.

Примером подобной программы может служить червь WINK (Worm Nuclear Killer — Червь Ядерный Убийца), который встречался на компьютерах типа VAX с операционной системой VAX/VMS в CERN и других европейских компьютерных центрах в 1989—1990 гг. Червь представляет собой batch-файл, написанный на командном языке DCL системы VMS. При запуске вирусная программа пытается подобрать пароли стандартных пользователей (SYSTEM, BACKUP, GAME и т. п.), используя специальный список из $\simeq 40$ наименований (имена, названия директорий и др.). В случае успеха червь прикрепляется к batch-файлам во «вскрытой» директории, обеспечивая тем самым свое распространение. При поражении системных директорий изменяется стандартный конфигурационный файл SYLOGIN.COM, и при входе в систему пользователь вместо имени компьютера получает сообщение о наличии на машине червя WNK. Насколько известно автору, Nuclear Killer не обладает деструктивным действием.

Другой вирус такого типа поразил внутреннюю сеть IBM в 1987 г. Он рисовал на экране дисплея новогоднюю елку и рассылал себя по адресам, найденным на зараженной машине.

Таким образом, кроме вируса Морриса, предпринимались лишь отдельные несерьезные попытки создать вирус для больших ЭВМ. В связи с наличием сложных систем защиты файлов и ядра операционной системы, а также с принятием в ряде стран законов об усилении уголовной ответственности за подобные действия, дальнейшее распространение вирусов на больших компьютерах представляется весьма маловероятным.

1.2.2. *Вирусы на персональных компьютерах, отличных от IBM PC.* Фактически основной ареал распространения вирусов — персональные компьютеры с простой операционной системой, не имеющей почти никаких средств защиты. И хотя впервые вирусные программы появились именно на IBM PC-совместимых машинах, есть они и на других компьютерах такого класса.

В настоящее время известно о существовании вирусов для компьютеров типа Macintosh, один из которых поражает прикладные программы [25] и является весьма изощренным. Представитель фирмы Apple заявил, что фирма намерена провести расследование с целью привлечения автора к уголовной ответственности.

К сожалению, в отличие от многопользовательских систем, найти автора вируса для персональных ЭВМ часто бывает очень трудно, так как он может распространить вирус через сети, компьютерные клубы и многими другими способами, оставаясь при этом «в тени».

Существуют вирусы и на простых персональных компьютерах типа Commodor Amiga и Atari ST. Известно об обнаружении по крайней мере трех таких вирусных программ и в Советском Союзе.

1.2.3. *Вирусы на IBM PC-совместимых персональных компьютерах.* Мы переходим к основной теме обзора — вирусам на IBM PC-совместимых компьютерах. Кроме чрезвычайно простой операционной системы MS DOS, являющейся по сути монитором, авторов вирусов, несомненно, привлекает и широкое распространение подобных ЭВМ. Дело в том, что фирма IBM при анонсировании этого персонального компьютера сделала его архитектуру открытой и опубликовала все необходимые сведения для фирм-производителей как аппаратного, так и программного обеспечения [26]. Это способствовало быстрому созданию большого количества при-

кладных программ (редакторы, компиляторы, базы данных, процессоры текстов, игры и т. д.) и резкому удешевлению компьютеров, благодаря одновременному производству их множеством мелких фирм. В свою очередь, наличие большого числа программ, не защищенных от копирования, привело к широкому обмену ими.

Дальнейшее объединение компьютеров в сети только способствовало созданию крайне благоприятных условий для передачи вирусов с одной

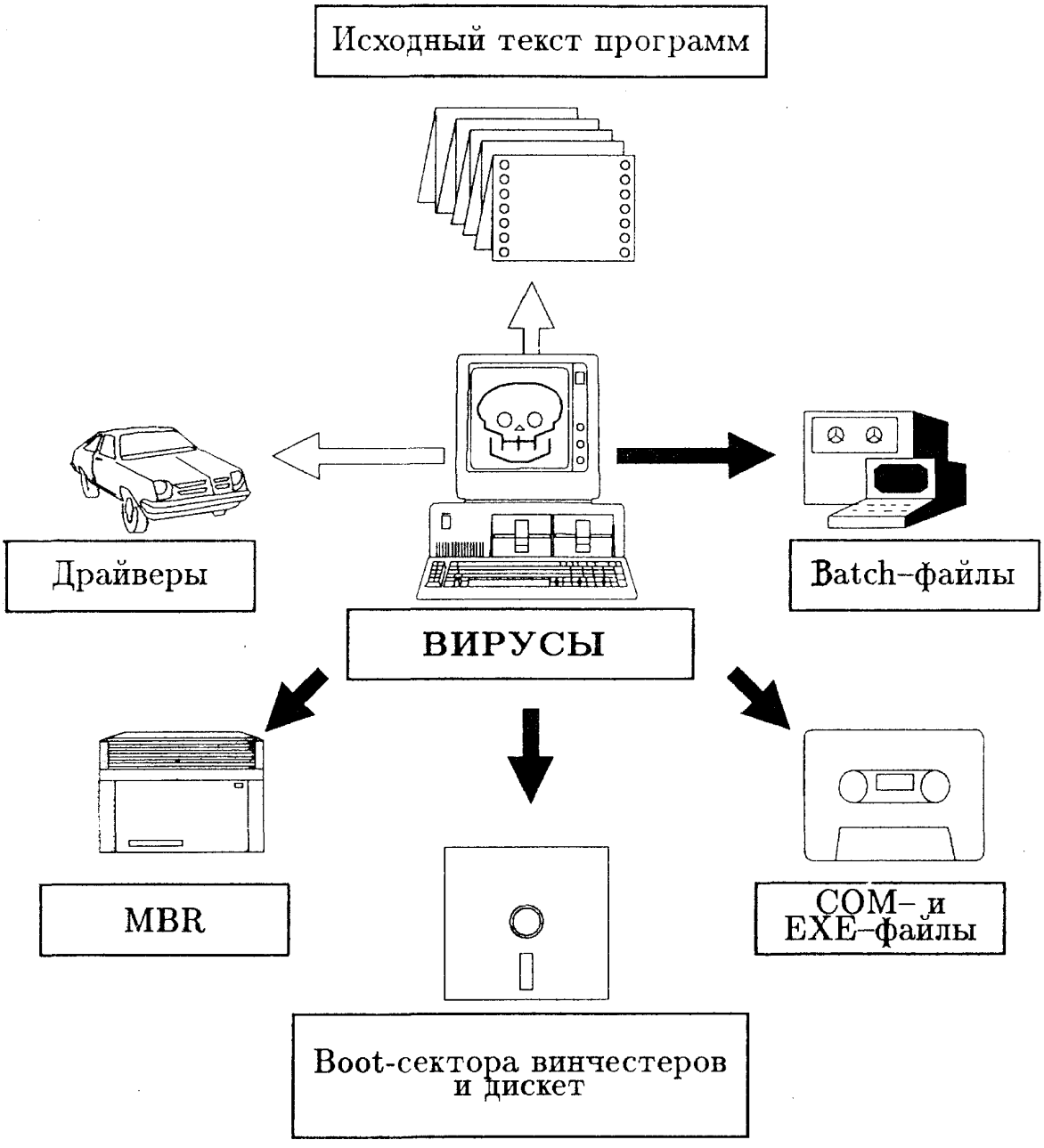

Рис. 1. Среда обитания вирусов на IBM PC-совместимых ЭВМ. Темные стрелки—вирусы такого типа существуют, светлые стрелки — вирусы пока не существуют или информация о них недостоверная

ЭВМ на другую. Широкое распространение IBM PC-совместимых компьютеров в среде непрофессионалов тоже приводит к быстрому размножению вирусов и затягивает сроки их обнаружения.

Практическое отсутствие авторских прав на программный продукт в СССР и повсеместный «подпольный» обмен им делают советский рынок персональных ЭВМ идеальным для существования вирусов. И тот факт,

что лишь около трети известных в мире вирусных программ добралось до нашей страны, означает лишь задержку в распространении, связанную с большим дефицитом компьютеров и высокими ценами на них.

Ниже будут рассмотрены все тонкости анатомии и жизненного цикла вирусов, приведена попытка их классификации и даны практические рекомендации по обнаружению вируса на персональном компьютере.

1.2.3-1. Где живут вирусы? — Необходимое условие размножения вирусной программы — хотя бы однократное исполнение своего кода. В связи с этим вирусы могут «жить» лишь в программах (либо являющихся частью операционной системы, либо прикладных).

Места возможного внедрения вирусов в системе MS DOS показаны на рис. 1. Рассмотрим эти компоненты программного обеспечения более подробно.

MBR-вирусы. Внедряют себя или часть своего тела в MBR на место программы, управляющей загрузкой системы. Получают управление при старте системы с hard-диска.

Вирусы драйверов. Поражают драйверы внешних устройств. Получают управление всякий раз, когда система обращается к периферии, обслуживаемой данным драйвером.

Boot-вирусы. Помещают себя или свою часть в boot-сектора дискет и партиций на место программы, осуществляющей загрузку системы. Получают управление при старте системы с hard- или floppy-диска.

COM- и EXE-вирусы или *вирусы общего назначения.* Прикрепляются к исполняемым модулям DOS. Получают управление в момент запуска зараженной программы.

Batch-вирусы. Довольно экзотический вид вирусов [7] ●; представляют собой программу, написанную на командном языке MS DOS. В связи с большим размером и из-за прозрачности командного языка практического распространения не получили.

Вирусы, поражающие исходный текст программ. Теоретически возможный тип вируса, представляющий собой программу на языке высокого уровня, внедряющуюся в файлы, написанные на этом языке. После транслирования и запуска такой программы вирус переписывает себя в другие файлы. Сходными чертами обладает вирус Морриса, передающий часть своего кода в виде программы на языке С. Принципиально возможно внедрение вируса и в системные библиотеки для языков высокого уровня, так чтобы ему передавалось управление при выполнении какой-либо стандартной функции (см. [3]). Однако такие вирусы могут эффективно распространяться лишь в среде пользователей, часто использующих компиляторы. Обычно такие люди являются достаточно квалифицированными в области программирования, чтобы быстро распознать наличие вируса и заменить системную библиотеку оригинальной. О дальнейших перспективах сказать трудно, но пока о появлении таких вирусов не сообщалось.

Некоторые типы вирусных программ способны «жить» более чем в одном из указанных мест. Так, вирус Marijuana (см. ниже и [4]) поражает boot-сектор гибких дисков и MBR винчестеров.

Следует понимать, что других мест, где способен жить вирус, на компьютерах типа IBM PC просто *не может существовать*! Конечно, не исключено проникновение вирусов в BIOS, но фирма-изготовитель такой микросхемы долго не проживет. Многочисленные истории о вирусах, живущих в CMOS-памяти (память, питаемая от батареек, в которой хранятся сведения о конфигурации компьютера), принадлежат к серии легенд. По-

скольку управление никогда не передается CMOS-памяти, находиться только в ней вирус не может. Известны, правда, вирусные программы, использующие CMOS-память компьютеров типа IBM PC/AT-386 и 486 (у которых она больше, чем у обычных AT), для хранения части своего кода. При этом действительно может наблюдаться странное явление: даже после форматирования дисков машина, выведенная из строя вирусом, отказывается работать, и только сброс содержимого CMOS-памяти позволяет восстановить работоспособность компьютера. Объяснение такого «парадокса» очень простое. На последних моделях серии 386 и 486 часть CMOS-памяти отведена под номер данного компьютера, о чем пользователь может даже не догадываться. Программа POST проверяет этот номер, и в случае его несовпадения с хранящимся в ней значением, отказывается загружать систему. Если вирус поместил часть своего кода в CMOS и повредил информацию о номере, то до полного обнуления памяти (когда POST автоматически запускает программу SETUP) компьютер работать не будет.

Сообщалось также о существовании довольно интересных вирусов загрузчика (т. е. MBR- или boot-вирусов), пережидающих в оперативной памяти процедуру форматирования диска, если она была запущена в зараженной операционной системе [8]. Тогда после окончания форматирования вирус тут же помещает себя вновь в загрузочный сектор, поэтому уничтожить его иначе, как с неинфицированной дискеты с операционной системой, не представляется возможным.

1.2.3-2. Размножение вирусов.—Все вирусы можно условно разделить на две категории: остающиеся резидентными в памяти компьютера после завершения своей работы или не делающие этого. Подавляющее большинство вирусов принадлежит к первому типу, так как резидентная часть обеспечивает быстрое и эффективное размножение. Перед тем как рассмотреть такие вирусы, кратко остановимся на самовоспроизводстве вирусных программ без резидентной части.

1.2.3-2.1. *Размножение вирусов без резидентной части.*— Такие вирусы вынуждены перемещать свое тело в другие модули только во время работы зараженного программного кода, что ограничивает их класс вирусами общего назначения. При запуске инфицированной программы управление передается телу вируса, который находит по какому-либо алгоритму следующую программу-кандидат на заражение и пытается инфицировать ее. Как это делается?

Все известные к моменту написания статьи вирусы общего назначения помещают свое тело либо в начало (COM-файлы), либо в конец (EXE- и COM-файлы) заражаемого модуля. Единственным исключением является вирус Lehigh, о котором будет сказано чуть позже. При этом вирусы изменяют программу так, чтобы управление передавалось на их тело при запуске зараженной программы.

В случае прикрепления к началу COM-модуля это происходит автоматически — сначала исполняются команды вируса, а потом начинает выполняться текст программы. Поскольку изначально он смещен в памяти на длину вирусного кода, перед окончанием своей работы вирус сдвигает программу в сторону младших адресов. Если вирус прикрепляется к концу файла, то ему необходимо переменить код исходной программы так, чтобы управление передалось на его тело. Для COM-файла это обычно достигается заменой его первых трех байтов [9] оператором безусловного перехода на начало вируса (эта команда имеет тип near и как раз занимает 3 байта).

В случае EXE-модуля необходимо изменить первые байты заголовка так, чтобы скорректировать объем памяти, необходимый программе, и длину загружаемой части. Далее, вирус либо меняет точку входа, записав в заголовок новое начальное значение регистров CS, IP, вычисленное в процессе заражения (стандартный путь), либо, вместо первых байтов текста программы у точки входа, записывает команду безусловного перехода на свое начало (теперь она занимает 3 или 5 байтов, в зависимости от типа адресации, так как оператор перехода имеет тип far). Если COM-файлы удлиняются при прикреплении вируса на фиксированное количество байтов, то для EXE-модулей это не совсем так. Дело в том, что при заражении EXE-программы вирус обычно выравнивает свое начало на границу параграфа (16 байт памяти), что в дальнейшем облегчает ему операции по резервированию памяти и другие действия. В связи с этим удлинение EXE-файлов равно сумме базовой длины вируса и числа от 0 до 15, зависящего от первоначального размера файла.

Во всех случаях вирус запоминает где-то внутри своего тела измененные в процессе заражения байты заголовка или исходного текста с целью восстановления их перед передачей управления собственно программе. Подавляющее большинство вирусов прикрепляется к концу файла. Во-первых, это — единственно возможный путь заражения EXE-модулей (поэтому вирусные программы, заражающие и EXE-, и COM-файлы в целях экономии обычно помещают себя в конец файла). Во-вторых, даже в случае COM-модулей размещение вируса в начале файла требует переписывания на диске всего тела программы (так как в системе MS DOS любой файл должен начинаться с первого байта кластера на диске), что сильно увеличивает время работы вирусного кода и делает его присутствие весьма заметным. Кроме того, перед передачей управления программе тоже необходимо смещать ее в памяти.

Вирус Lehigh, являющийся весьма специфическим, заражает только файл командного интерпретатора COMMAND. COM, структура которого хорошо известна. Поэтому вирус помещает себя не в начало или конец файла, а непосредственно внутрь него, используя область стека, зарезервированную в тексте программы. При этом длина COMMAND. COM либо совсем не изменяется, либо изменяется всего на 20 байт (существуют две разновидности вируса Lehigh), что маскирует внедрение вируса. В остальном все происходит так же: изменяются первые байты с целью передачи управления телу вируса. Других вирусов, помещающих себя внутрь заражаемой программы, в мире пока не наблюдалось.

После осуществления попытки заражения вирус возвращает управление собственно программе, которая его запустила, предварительно восстановив измененные байты ее кода или информацию о начальных значениях регистров (по содержимому старого заголовка — EXE-модули).

В принципе, в процессе работы такой вирус может заразить много файлов, однако на практике этого не происходит, так как подобные действия были бы слишком заметными. Обычно за один запуск заражается не более одного файла, что вполне достаточно для эффективного размножения. Типичным примером вируса без резидентной части является вирус Restart (см. раздел 3).

Алгоритмы поиска следующего кандидата на заражение могут быть самыми различными: первый незараженный файл в текущей поддиректории; в директориях DOSовского пути (path); на всем диске и т. п. Некоторые вирусы такого типа специально не заражают командный интерпретатор, чтобы их труднее было обнаружить.

1.2.3-2.2. *Размножение boot- и MBR-вирусов.*— Эти вирусы получают управление всякий раз, когда происходит перезагрузка системы с дискеты (boot) или с винчестера (MBR и boot). Для того чтобы успешно размножаться, они должны иметь резидентную часть, остающуюся активной и после процесса загрузки.

Все известные к 1990 г. boot-вирусы перехватывают hardware прерывание 13h, с помощью которого осуществляется доступ к гибким и твердым дискам. Как только производится попытка обращения к еще не зараженному диску, резидентная часть вируса проделывает следующие операции:

— поиск свободного сектора на этом диске;

— спасение master boot- или boot-программы в этот сектор;

— запись своего тела на место master boot- или boot-программы (в случае длинного вируса в загрузочный сектор записывается лишь его часть, а остальное тело размещается либо в специальных служебных секторах диска (корневой каталог и т. п.), либо в произвольных свободных секторах, помечаемых как плохие [10] ● для сохранности информации);

— пометка сектора со спасенной загрузочной программой, как плохого, для защиты информации, находящейся в нем, от стирания или перезаписи.

Если диск, зараженный таким образом, является загружаемым, то при первой попытке старта системы с него происходит следующее:

— программа-вирус получает управление;

— в целях маскировки, вирус перемещает свое тело в верхние адреса памяти;

— дисковое прерывание 13h перехватывается вирусом;

— в память загружается старая boot-программа, находящаяся в известном месте на диске;

— управление передается ей, после чего осуществляется обычная загрузка системы.

Некоторые вирусы (например, Alameda Virus, см. [4, 6]) не утруждают себя пометкой сектора со спасенной MBR или boot-record как плохого, в результате чего через некоторое время он оказывается стерт при очередном запросе на дисковую память, и система перестает загружаться.

Остановимся подробнее на маскировке вируса в памяти. Дело в том, что оставаться на месте вирус не может, так как его тело будет уничтожено после окончания выполнения программы загрузки. Поэтому, чтобы стать резидентным, он обычно перемещает себя в старшие адреса памяти, после чего корректирует максимальный ее объем, доступный операционной системе, уменьшая его значение на длину своего тела (обычно 1 — 2 Кбайта). В результате после загрузки системы MS DOS будет считать, что на машине установлено чуть меньше памяти, что чаще всего незаметно для пользователя.

Таким образом, достаточно обращения к еще не зараженной системной дискете на инфицированном вирусом загрузчика компьютере, чтобы дискета стала разносчиком вируса и заразила другие машины при попытке загрузки с нее операционной системы.

Некоторые из подобных вирусов отлавливают обращение к MBR- или boot-сектору, анализируя состояние регистров в момент перехвата прерывания 13h. В случае, если производится попытка прочитать или изменить загрузочный сектор, вирус обманывает систему, «подсовывая» вместо истинного сектора с программой загрузки старую спасенную копию. Поэтому такие вирусы невозможно обнаружить путем сравнения загру-

зочных секторов с их копиями, хранящимися в специальных файлах, если операционная система компьютера заражена.

Кроме уже названных вирусов Alameda и Marijuana, примерами вирусов загрузчика могут служить Italian и Pakistan Brain (см. ниже, а также [4, 6]). Вирусы такого типа распространяются не слишком быстро, так как их переносчиками являются только системные дискеты. Вместе с тем обнаружить их не просто, если не предпринимать специальных мер, поэтому они довольно часто встречаются.

1.2.3-2.3. *Размножение резидентных вирусов общего назначения.* — Механизм прикрепления вирусов общего назначения с резидентной частью к файлам ничем не отличается от описанного в разделе 1.2.3-2.1. Однако способ размножения отличается кардинально. При запуске зараженной программы происходит следующее:

— управление передается на тело вируса;

— проверяется, заражена ли уже система; если это не так, то выполняются следующие два пункта:

1) вирус маскируется в памяти;

2) некоторые из DOSовских прерываний, в том числе основное прерывание 21h, перехватываются вирусом;

— восстанавливаются элементы программного кода, испорченные вирусом в программе-носителе;

— управление передается собственно ей.

Итак, размножения вируса во время работы зараженной программы не происходит. Как же оно осуществляется?

Как только на компьютере с инфицированной операционной системой происходит запуск какой-либо программы, резидентная часть вируса проделывает следующие операции:

— перехватывает прерывание 21h (подфункция 4Bh) — загрузка в память и запуск программы;

— проверяет, заражена ли уже программа, которую нужно запустить, и если нет, то пытается инфицировать ее посредством приписывания своего тела к файлу с ее кодом (см. 1.2.3-2.1);

— передает управление стандартному прерыванию 21h MS DOS (точка входа которого спасается внутри тела вируса при инфицировании системы), загружающему и запускающему программу.

Таким образом, при запуске любой программы вслед за инфицированной она может быть заражена вирусом (некоторые вирусы поражают не все, а только COM-модули или файлы, длина которых лежит в определенных пределах; другие не инфицируют COMMAND. COM).

Поскольку часто программой, запускаемой вслед за инфицированной, является командный интерпретатор, подгружаемый с диска, он вскоре оказывается зараженным (конечно, если вирус специально не пропустит его). После этого даже перезагрузка системы не спасет от заражения, так как запуск инфицированного COMMAND.COM после старта системы сразу активизирует резидентную часть вируса.

Проверка зараженности операционной системы обычно осуществляется для экономии времени, а также, чтобы в системе не находилось слишком много резидентных копий вирусного кода. С этой целью вирус либо помещает ключевое слово в зарезервированную ячейку памяти, либо использует не поддерживаемую MS DOS подфункцию какого-либо из перехватываемых прерываний для передачи «пароля».

Маскировка вируса общего назначения в памяти может происходить так же, как и для вирусов загрузчика (см. п. 1.2.3-2.2), однако, есть и

другие варианты. Дело в том, что MS DOS при работе использует множество областей памяти (так называемые буферы DOS) для служебных целей. Некоторые вирусы искусно прячут свое тело в эти буферы, изменяя их длину и все ссылки на них. Так, вирус Yankee Doodle (см. раздел 3), маскируется настолько хорошо, что не может быть обнаружен даже самыми лучшими на сегодняшний день программами, составляющими карту памяти (о них будет сказано в разделе 2).

Некоторые «интеллектуальные» вирусы перехватывают и другие прерывания. Тот же Yankee Doodle переключает на себя прерывание, используемое отладчиками для трассировки программы. Если пытаться посмотреть структуру зараженного файла в отладчике, то вирус отслеживает это и удаляет себя из файла. Тем самым усложняется процедура дизассемблирования вирусного кода и создания антивируса.

Другой каверзный вирус — Dark Avenger (см. раздел 3) — перехватывает открытие и закрытие файлов и заражает их, если они имеют расширение .COM или .EXE. Достаточно просмотреть такой файл текстовым редактором или командой TYPE, чтобы он оказался заражен! Если антивирус вылечивает файл в зараженной таким вирусом операционной системе, то он тут же будет инфицирован вновь при закрытии.

Многие вирусы используют также прерывание по таймеру, чтобы активизироваться в определенное время суток.

1.2.3-3. Признаки зараженности компьютера.— Чаще всего наличие вирусов на персональной ЭВМ легко обнаружить до их активизации. Из материала предыдущих разделов можно указать следующие подозрительные явления на компьютере, которые должны насторожить опытного пользователя:

— увеличение размера некоторых файлов. Как следует из пункта 1.2.3-2.1, это — типичное проявление COM- и EXE-вирусов;

— повторяющиеся сбои и «зависание» системы при запуске некоторых стандартных программ. Такая ситуация также очень подозрительна, так как не очень хорошо написанные вирусы неправильно заражают специальные типы файлов. Например, если сумма длины вируса и COM-файла превышает 64 Кбайта, а при заражении это не проверяется, то впоследствии, при попытке запуска такой программы, она не будет загружаться с диагностикой Out of memory (нехватка памяти). Некоторые вирусы неправильно заражают EXE-файлы, считая их COM-модулями, так как различают программы не по внутреннему формату, а по расширению их имени. Это также приводит к зависанию при попытке запуска. Другие вирусы (Dark Avenger, Restart) медленно портят файлы, что тоже может служить причиной сбоев при работе стандартных программ. Наконец, тот же вирус Dark Avenger при работе сканирует BIOS с целью определения точки входа прерывания 13h. Используемый для этого алгоритм приводит к «зависанию» программы на некоторых компьютерах:

— появление новых дефектных секторов и кластеров на гибких дисках и винчестерах. Дело в том, что плохие кластеры помечаются лишь при форматировании диска или при запуске специальных программ. Если ни того, ни другого не происходило, «беспричинное» появление дефектных кластеров скорее всего означает наличие на компьютере вируса загрузчика.

— увеличение времени загрузки системы или программ, замедление работы компьютера — тоже характерные признаки наличия вирусов.

1.2.3-4. Активизация вирусов.— По характеру наносимого вреда вирусы делятся на:

— *«безвредные»,* т. е. не производящие никаких побочных действий кроме размножения (Vacsina, Micro88; см. [4] и раздел 3).

— *развлекательные,* т. е. не обладающие деструктивным эффектом, а лишь создающие зрительные или звуковые эффекты (Чуча [27], Younkee Doudle, Falling Letters, Marijuana — см. раздел 3), например появление надписей, исполнение мелодии.

— «*боевые*», т. е. предназначенные для разрушения файловой системы (Alameda, Pakistan Brain, Lehigh), изменения отдельных файлов (Restart, Dark Avenger, dBASE [11] [9]), а также для вывода из строя отдельных элементов hardware компьютера. Есть сведения о существовании вируса, прожигающего экраны монохромных мониторов, пользуясь особенностями в схеме управления ими. Принципиально, можно создать и вирус, выводящий из строя дисковод гибкого диска (посредством установления максимальной скорости движения головки и периодического перемещения ее от первой дорожки к последней, когда пользователя поблизости нет (например, если к клавиатуре никто не обращался в течение длительного времени)).

Активизация боевых и развлекательных вирусов происходит при самых разных условиях. Здесь все зависит от фантазии автора. Можно привести несколько групп условий активизации:

— по таймеру, в определенное время суток (Yankee Doodle);

— в зависимости от показания системных часов (Falling Letters, Jerusalem);

— периодически, раз в несколько запусков зараженных программ (Dark Avenger, Restart);

— после инфицирования определенного числа файлов (Lehigh).

Существуют и более сложные логические условия срабатывания вируса (Italian).

Следует иметь в виду, что даже «безвредные» вирусы вредны!

— Они увеличивают размер файлов и время загрузки программ.

— Они легко могут быть трансформированы в боевые.

— Даже самые совершенные вирусы, не говоря уже о не очень качественных, могут приводить при определенных условиях к «зависанию» системы.

1.2.3-5. П о п ы т к и к л а с с и ф и к а ц и и . — Большое количество вирусов имеет несколько распространенных названий, данных им первыми исследователями, часто независимо друг от друга. Так, вирус Jerusalem имеет по крайней мере еще пять весьма употребляемых имен (Israeli, Black Friday, Friday the 13th, Time, Black hole). Такое многообразие названий затрудняет лечение вирусов, так как часто бывает непонятно, против какого вируса предназначен конкретный антивирус.

Ситуация несколько напоминает имеющую место в физике элементарных частиц, когда наряду с общеупотребимыми названиями (типа h-мезон) усиленно культивируются обозначения Particle Data Group (f_4-мезон), что часто приводит к путанице.

В настоящее время классификация вирусов невероятно запутана и более всего похожа на приводимую Х. Л. Борхесом в рассказе «Аналитический язык Джона Уилкинса» [28]. Кстати, этот пример используется в книге Л. Б. Окуня «Физика элементарных частиц» [29].

Представляется разумным создание единой системы нотации вирусов, позволяющей по внешним признакам легко идентифицировать их. Одна из первых попыток такого типа была предпринята Н. Н. Безруковым [4, 30]. Согласно его классификации, каждый вирус обозначается

определенным сочетанием букв и цифр. Нотация включает в себя три элемента:

— классификационный код, содержащий основные характеристики вируса, достаточные для его идентификации;

— дескриптор, представляющий собой формализованный список его свойств;

— сигнатуру, т. е. строку для контекстного поиска тела вируса в зараженном файле.

Если дескриптор и сигнатура в основном могут быть полезны авторам программ-антивирусов [12], то по классификационному коду определить тип вируса может даже человек, не являющийся специалистом в этой области.

Остановимся подробнее на классификационном коде вирусов. Он состоит из буквенного префикса, цифрового корня и суффикса.

Префикс представляет собой одну или несколько букв, указывающих на тип вируса. Так, вирусы общего назначения, заражающие COM-файлы, имеют в качестве одной из букв префикса символ C. Если они заражают еще и EXE-модули, то префикс имеет вид CE. Для вирусов с резидентной частью появляется дополнительная буква R. Для вирусов загрузчиков используются префиксы B, D, M или их сочетания в зависимости от того, заражают ли они boot-сектора жестких (B) и гибких (D) дисков, а также MBR (M).

Цифровой корень означает характерную длину вируса. При этом, поскольку вирусы, поражающие EXE-файлы, удлиняют не все из них одинаково, имеется в виду некое базовое значение (т. е. изменение длины COM-файла или EXE файла, выровненного по границе параграфа).

Необязательный суффикс может обозначать номер или свойства неразличимого по корню и префиксу «штамма» данного вируса.

Например, вирус Falling Letters имеет две разновидности длиной 1701 и 1704 байта и заражает только COM-файлы, обладая при этом резидентной частью. Поэтому два штамма этого вируса обозначаются RC-1701 и RC-1704. Существует еще одна разновидность RC-1704, форматирующая диск. Разумно обозначить ее RC-1704F. Обычно вирусы, различающиеся лишь суффиксом, вылечиваются одним и тем же антивирусам, поэтому, в принципе, для лечения он не так важен.

Вирус загрузчика Italian, занимающий два сектора на диске, согласно этой классификации имеет код RBD-1024, а вирус Marijuana — RDM-512.

2. Компьютерная фармакология. Теперь нам известно достаточно много о вирусах. Однако лучше всего не только хорошо знать их, но и бороться с ними. Поэтому весь этот раздел статьи посвящен различным антивирусам и другим средствам защиты от вирусных программ. Широкое распространение вирусов привело к созданию многочисленного программного продукта такого типа как отдельными программистами-любителями, так и серьезными фирмами. Ситуация напоминает известный закон соревнования снаряда и брони.

Прежде чем начать разговор об антивирусах, хотелось бы предупредить, что бездумное их применение может принести такой же вред, как употребление всей домашней аптечки при первых признаках насморка! При неправильном обращении антивирусы едва ли помогут вылечить компьютер. Причины этого объяснены в следующих двух разделах.

2.1. О правилах хорошего тона при создании антивирусов.

«...Не навреди!».
(Из клятвы Гиппократа)

В настоящее время в мире известно несколько сот антивирусных программ. Многие из них полностью или частично дублируют друг друга. Понять, против какого вируса предназначен тот или иной антивирус, не всегда бывает возможно, так как документация к таким программам часто отсутствует или пишется на нераспространенных языках (итальянский, немецкий, польский, русский и др.). Поскольку вирусы явно не признают государственных границ, бороться с ними нужно сообща! Поэтому, на наш взгляд, одно из правил хорошего тона при создании антивирусов заключается в том, чтобы вся диагностика и документация к ним были написаны на общепризнанном стандарте для научных сообщений и коммуникаций — английском языке. Никому не приходит в голову переводить на русский язык FORTRAN или C. Точно так же и для лечения вирусов не обязательно хорошо знать английский, чтобы понять диагностические сообщения. Именно из этих соображений все названия вирусов в данной статье приведены только на английском языке (кроме вируса «Чуча», использующего кириллицу).

Автор призывает просто безжалостно стирать антивирусные программы, не имеющие достаточно понятного руководства по использованию (либо в виде отдельного файла, либо внутри самого антивируса).

Дело в том, что применение их вряд ли принесет сколько-нибудь ощутимую пользу, а ущерб может быть очень велик. Действительно, программы, не имеющие хорошей документации по использованию, чаще всего пишутся непрофессионалами (так как опытные программисты знают, что программа без описания не является программным продуктом). Такие самоделки обычно создаются наспех и имеют очень низкое качество. Это приводит к тому, что после работы подобных программ, если они идентифицируют вирус, большое количество файлов оказывается безвозвратно испорчено. Чаще всего такое происходит из-за того, что авторы программ-антивирусов неаккуратно выбирают контекстную строку для поиска вируса, в результате чего несколько сильно различающихся модификаций вируса лечатся программой по одному и тому же принципу, что и приводит к необратимым потерям.

Другая распространенная ошибка авторов подобных программ заключается в том, что их действие проверяется лишь на нескольких стандартных EXE-файлах, которые обычно имеют длину, кратную 16 байтам. Если же попытаться вылечить EXE-файлы другой длины, то чаще всего вирус оказывается удален из файла не до конца, а иногда наоборот, вместе с ним бывает выброшено и несколько байтов кода самой программы. То же самое может получиться при лечении модулей, содержащих информацию для отладчика, или программ, предназначенных для одновременного использования под системами MS DOS и OS/2 (большинство новых продуктов фирмы MicroSoft). Разумеется, не все вирусы позволяют абсолютно точно восстановить файлы, зараженные ими, но если такое возможно, следует уделить достаточно времени поиску нюансов при заражении различных типов файлов.

Хочется напомнить, что когда изобретается новое лекарство, перед его серийным выпуском обязательно происходят длительные клинические испытания. И даже то, что компьютер заражен вирусом, который нужно

срочно удалить, не является оправданием написания и копирования таких недоделанных программ, так как они слишком быстро распространяются и мгновенно выходят из-под контроля [13].

Основной принцип, которым следует руководствоваться при создании антивирусов — «не навреди!». Ведь *лучше иметь зараженную работающую программу, чем необратимо испорченную, но не содержащую вируса.* Точно так же нужно и выбирать антивирусные программы для использования на своем компьютере.

2.2. О вреде самолечения. Среди пользователей распространена практика запуска целой серии антивирусных программ (десятка и более) при первых признаках сбоев в работе компьютера. Чаще всего такие сбои вызваны ошибками самого пользователя или использованием некачественного (в большинстве случаев самодельного) программного обеспечения.

Не говоря уже о том, что подобная процедура занимает много времени, она просто может привести к заражению всего компьютера и потере большого количества файлов. В чем заключается опасность?

— Антивирусы работают в тесном контакте с вирусами, поэтому часто сами оказываются зараженными. При последовательном использовании десятка подобных программ, обычно взятых у друзей или коллег по работе, вероятность заражения еще не инфицированного компьютера становится весьма высокой.

— Многие антивирусы неправильно лечат «штаммы» того вируса, на который они рассчитаны (см. раздел 2.1), что приводит к потере файлов.

— При заражении компьютера «серьезным» вирусом, таким, например, как Dark Avenger, подобный запуск серии антивирусов приведет только к заражению *всех* исполняемых файлов на компьютере, а также к появлению большого количества испорченных секторов, которые могут находиться и в исполняемых файлах и в файлах с данными.

Так же, как и в медицине, при подозрении на наличие вируса на компьютере, лучше всего обратиться к помощи специалиста! В разделе 2.4 будут приведены некоторые простые правила, следуя которым, можно почти наверняка уберечь компьютер от заражения.

2.3. Какие бывают антивирусы?

«Если враг не сдается —
его уничтожают!».
М. Горький

Все программы-антивирусы можно условно разделить на несколько классов, представленных на рис. 2. Рисунок охватывает как средства собственно борьбы с вирусами, так ж вспомогательные программы, облегчающие идентификацию вирусов и помогающие уберечь файлы от заражения. Рассмотрим их более подробно.

Индикаторы. Программы, осуществляющие поиск характерных для различных вирусов последовательностей кодов в тексте зараженных модулей. Наиболее известными программами этого типа являются SCAN (© 1990 by McAfee Associates) и VIRSCAN (© 1990 by IBM).

Индикаторы-фаги. Кроме определения вируса по характерному элементу кода, предпринимают попытку вылечить файл, более или менее успешную, в зависимости от их качества. Наиболее хорошие фаги способны обезвреживать резидентную часть вирусов, позволяя продолжать работу после лечения, не прибегая к перезагрузке системы. Различают

универсальные фаги, способные лечить множество вирусов (CLEAN57 (McAfee Associates), VR (SiP), AIDSTEST (Д. Лозинский), ANTI-KOT (О. Котик) и др.), и специализированные фаги, настроенные на конкретный тин вируса, и, быть может, на его «штаммы» (DISARM (J. Blach & M. Weiner – Falling Letters 1701), DR-NO (H. Leeb - Restart), PASTER (Г. Ландсберг — Falling Letters 1701/1704)). Имеет место эмпирическое правило: чем больше типов вирусов вылечивает программа, тем менее

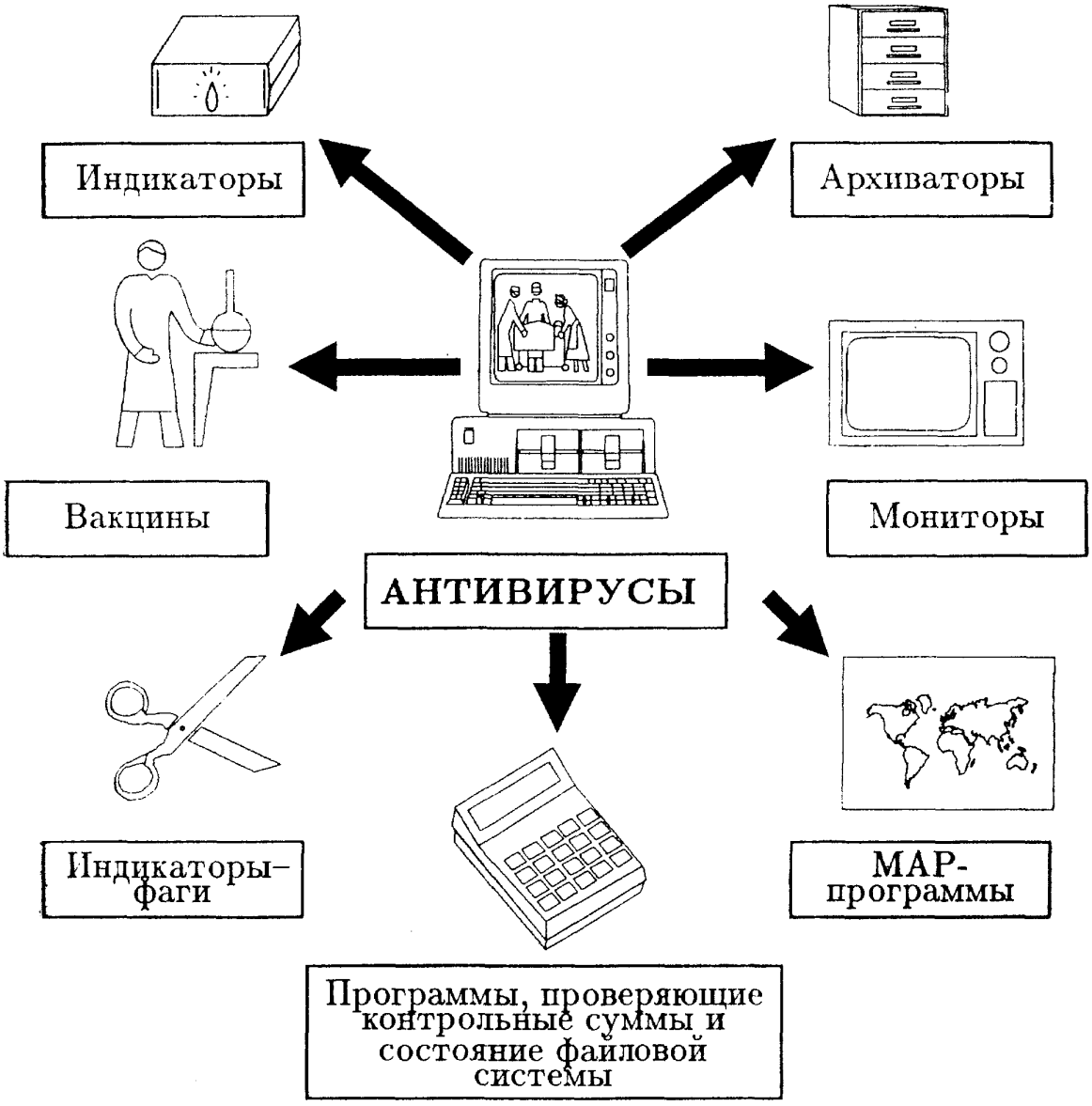

Рис. 2. Типы компьютерных вирусов

качественно она это делает. Так, VR и AIDSTEST портят файлы, зараженные разновидностью 1704 вируса Falling Letters; CLEAN57 не справляется в большинстве случаев с Yankee Doodle и т. д. Представляется разумным использовать универсальные индикаторы или фаги в режиме индикации, а затем лечить обнаруженный вирус с помощью хорошего специализированного фага.

Вакцины. Включают в код программ проверочную часть, сравнивающую контрольную сумму, длину, фрагменты кода со спасенными значениями. Иногда могут восстанавливать зараженные программы. Обычно действуют подобно вирусу общего назначения, прикрепляясь к защи-

щаемой программе и проверяя ее при загрузке в память перед исполнением. Преимущество вакцин в том, что они могут распознавать новые типы вирусов; недостатки — в невозможности вылечить зараженный файл, если он не был предварительно вакцинирован, увеличении времени загрузки программы, неспособности вылечивания вирусов типа Dark Avenger, вновь заражающих файл при его закрытии и т. д. Примеры программ-вакцин: STAMPER (А. Чижов), PROTECT (Д. Стефанков). Несколько другой подход используется в универсальной вакцине PHENIX (Г. Ландсберг) (см. раздел 4), что позволило устранить в ней большинство недостатков, свойственных обычным вакцинам.

Программы, проверяющие контрольные суммы и состояние файловой системы. Принцип действия заключается в записи контрольных сумм файлов или другой информации в специальной базе данных с последующим сравнением их с текущим состоянием системы. Этот способ позволяет выявить практически любой вирус (особенно, если контрольная сумма вычисляется несколькими способами). Недостатками являются длительность процедуры подсчета контрольных сумм и необходимость постоянно обновлять базу данных в случае появления новых версий программ с тем же именем, а также при изменении файловой структуры (создание новых поддиректорий, копирование, переименование, стирание файлов и т. п.). Примеры таких программ CRCDOS (R. Faith), SENTRY (McAfee Associates), Vacine 1.3 (Art Hill).

Мониторы. Отлавливают подозрительные события на компьютере (попытка открытия EXE- или COM-файлов на запись, перехват некоторых прерываний и т. п.). При их появлении запрашивают разрешение пользователя на выполнение. Примеры таких программ: VIRBLK (M. Fitz), ANTI4US (E. Lantung). Пока мониторы бессильны против вирусов, использующих прямой доступ к диску (например, Yankee Doodle). Фирма McAfee Associates производит симбиоз индикатора и монитора (SCANRES; последние версии называются VSHIELD) — резидентную программу, проверяющую все загружаемые файлы на наличие в них характерных элементов большого количества вирусов. Кроме программных мониторов существуют еще hardware-мониторы, обычно релизованные как расширение BIOS, перехватывающее прерывание 13h и отлавливающее попытку записи в загрузочные сектора (например, [31]). Они предназначены для борьбы с boot-вирусами. Однако автору кажется, что против новых вирусов мониторы без индикатора будут бессильны, так как ничего не мешает интеллектуальным вирусам использовать для своих действий точку входа прерывания 13h стандартного BIOS (которую не так сложно найти путем простого синтаксического анализа). Тем самым все мониторы подобного типа оказываются «выключенными из игры», так как вирус не будет использовать даже явного обращения к прерыванию 13h.

MAP-программы. Предназначены для построения карты памяти на компьютере с указанием перехваченных различными программами прерываний. По таким картам иногда можно обнаружить наличие вируса, но в основном их следует рассматривать как вспомогательное средство для специалистов по борьбе с вирусами. Примеры подобных программ: VTSR (Golden Bow), PCMAP (Д. Стефанков). Другой тип MAP-программ показывает карту диска с указанием плохих секторов на нем. С помощью подобных утилит можно выявлять наличие вирусов загрузчика. В качестве одного из таких средств можно указать программу VMAP (Golden Bow).

Архиваторы. Программы, предназначенные для архивирования или

backupa данных. С одной стороны, это — надежный способ сохранить программу от вируса; с другой,— если вирус попадает в архив, он постоянно возникает вновь и вновь, и его очень трудно окончательно уничтожить. Наиболее хорошие архиваторы поставляет фирма «PKWARE Inc.» (PKARG, PKZIP), а backup-программы — «Central Point Software» (PCBACKUP).

Дополнительные сведения о программах-антивирусах можно найти в [16, 32, 33], а также в книге Р. Робертса (R. Roberts) Computer Viruses.

2.4. Как защититься от вирусов? Некоторые пользователи персональных ЭВМ настолько запуганы наличием вирусов, что не решаются даже обновлять свое программное обеспечение, пользоваться чужими программами и т. п. Конечно, самоизоляция — это тоже выход, но обычно и она не приводит к желаемому результату, если только Ваш компьютер не заперт в сейф, а прорезь дисковода не залита эпоксидным клеем...

Гораздо проще и безопаснее понимать, как можно заразиться вирусом, и предпринимать ряд профилактических мер перед перенесением на компьютер нового программного обеспечения. Итак, что это за меры?

Если новое программное обеспечение досталось Вам не на фирменных оригиналах, защищенных от записи, то перед запуском его на компьютере проверьте дискету хорошим индикатором вирусов, например, программой SCAN, желательно последней ее версией. При этом, если на дискете часть программ находится в архивах, предварительно распакуйте их в какую-нибудь директорию своего hard-диска (на дискете обычно не остается места для подобной операции), например, в директорию \TMP. Если индикатор не обнаружил вируса на дискете и в архивах, то скорее всего Вы имеете дело с неинфицированным программным продуктом. Для страховки (а вдруг Вам достался неизвестный еще вирус?) можно проделать следующее.

Если дискета содержит операционную систему и предполагается загрузить компьютер с нее, то:

— проверьте ее на наличие кластеров, помеченных, как плохие (если таковые имеются, то это весьма подозрительно);

— сразу же после загрузки обратитесь к своему hard-диску, например, командой COPY (но не запускайте программ с него!);

— после этого немедленно перезагрузите систему с заведомо хорошей дискеты, защищенной от записи и содержащей, кроме операционной системы, копии boot-сектора и MBR для Вашего винчестера. Получить эти файлы можно либо с помощью специальных программ (BOOTCHEK из McConachie Associates, PHENIX от Г. Ландсберга и др.), либо с помощью известной программы Norton Utilities. После перезагрузки сравните содержимое этих файлов с состоянием винчестера. Если они совпадают, то на дискете нет вируса загрузчика. В противном случае дискета заражена, и необходимо сразу же восстановить испорченные секторы винчестера с помощью тех же программ.

Даже если дискета поражена вирусом загрузчика, файлы на ней все равно можно использовать, если, конечно, они не требуют запуска именно с этой дискеты. Чаще всего дискету можно вылечить от вируса загрузчика командой SYS, переносящей «чистую» операционную систему и заново форматирующей загрузочный сектор (в этом случае версии старой и новой системы должны совпадать!).

Если дискета содержит исполняемые файлы (*а дискеты с операцион-*

ной системой всегда имеют по крайней мере один такой файл — командный интерпретатор), *то:*

— загрузившись со своего hard-диска и не используя shell-программ типа Norton Commander или PCShell, запустите по очереди исполняемые файлы на дискетах. Внимательно следите за длиной своего командного интерпретатора. Если она не изменилась, попробуйте запустить несколько стандартных DOSовских программ, которые легко восстановить в случае потери (MORE, ASSIGN, ATTRIB, собственно командный интерпретатор COMMAND. COM и т. п.). Если и их длина не изменилась, с подавляющей вероятностью Вы имеете дело с незараженными программами и можете смело с ними работать. *При первых признаках изменения длины запускаемых файлов* немедленно сотрите все файлы на винчестере, которые Вы успели запустить. Последним надо стереть командный интерпретатор. После этого перезагрузитесь с системной дискеты и восстановите стертые файлы.

Дискету с зараженными файлами или boot-сектором лучше всего послать фирме-изготовителю индикатора с тем, чтобы она учла наличие нового вируса в своих следующих версиях программы. Если Вам известны люди, активно занимающиеся созданием антивирусов, следует передать копию дискеты и им.

Руководствуясь этими простыми требованиями, Вы почти гарантированы от проникновения вирусов на Ваш компьютер!

3. Вирусы в СССР. Как уже отмечалось выше, в СССР к 1990 г. известно около 25 вирусов из общего числа $\approx$70 зарегистрированных к этому времени в мире. Настоящий раздел посвящен наиболее распространенным в нашей стране вирусам и содержит их краткие характеристики, признаки заражения, а также рекомендации по лечению инфицированных компьютеров.

3.1. Вирус Restart. Один из первых вирусов, зарегистрированных в СССР. Существует множество других названий этого вируса, среди которых Vienna virus, Time bomb. По классификации Н. Н. Безрукова (см. 1.2.3-5) имеет код С-648, т. е. заражает лишь COM-файлы, удлиняя их на 648 байтов, и не остается при этом резидентным. Вирус помещает свое тело в конец заражаемой программы. При запуске ищет следующую программу-кандидат на инфицирование в текущем каталоге, а также в директориях DOSовского пути. С вероятностью 1/8 не заражает найденную программу, а портит ее (посредством записи на место 5 первых байтов файла команды безусловного перехода на адрес перезагрузки FFFFh : 0000h)[14] ●. Запуск такой программы аналогичен нажатию комбинации клавиш Ctrl—Alt—Del и приводит к перезагрузке системы. Если испорченный таким образом файл запускается из AUTOEXEC. BAT, процесс перезагрузки зацикливается. В качестве признака зараженности файла вирус использует «нефизическое» значение поля секунд (62 секунды) в дате создания. Имеется множество антивирусов-фагов, вылечивающих зараженные (но не испорченные!) файлы, среди которых SERUMS (M. Fitz, H. Veit), ANTI-KOT (О. Котик), AIDSTEST (Д. Лозинский).

3.2. Вирус Micro 88. Является несколько усовершенствованной версией вируса Restart. Заражает лишь COM-файлы, увеличивая их длину на 534 байта. Классификационный код С-534. В отличие от вируса

Restart не портит файлы, а лишь инфицирует их. Кандидаты на заражение ищутся только в текущей директории. Инфицированные модули помечаются установлением месяца 13 в дате создания. Антивирусы — фаги: ANTI-KOT (О. Котик), AIDSTEST (Д. Лозинский).

3.3. Вирус Jerusalem. Имеет множество других названий (см. п. 1.2.3-5). Заражает как EXE-, так и COM-файлы, увеличивая их длину на 1808 байтов. Вирус остается резидентным в памяти компьютера, перехватывая прерывания 21h и 08h (прерывание по таймеру). Классификационный код вируса Jerusalem RCE-1808. При заражении COM-файлов вирусный код записывается в начало файла, а к концу дополнительно приписываются пять байтов, содержащих символы «MsDos» (используемые для распознавания уже зараженных файлов). При инфицировании EXE-модулей вирус помещает себя в конец файла, однако при этом ключевое слово не приписывается, поэтому EXE-модули могут заражаться неоднократно, «раздуваясь» до очень больших размеров. Через некоторое время после начала работы компьютера, вирус замедляет его быстродействие во много раз, используя холостой цикл при обработке таймерного прерывания. Кроме того, в нижнем левом углу экрана появляется черный квадрат. Если системная дата установлена на 13-е число, приходящееся на пятницу, то вместо заражения вирус стирает загружаемые программы. Jerusalem различает EXE- и COM-файлы не по внутреннему формату, а по названию, поэтому делает неработоспособными модули, имеющие неправильное расширение имени. Антивирусы-фаги: ANTI-KOT (О. Котик), AIDSTEST (Д. Лозинский).

3.4. Вирус Falling Letters. Имеет, по крайней мере, две разновидности — длиной 1701 и 1704 байта. Заражает только COM-файлы, оставаясь при этом резидентным. Классификационные коды двух «штаммов» этого вируса — RC-1701 и RC-1704. Активизируется на компьютерах без внутренних часов или на машинах с часами, если системная дата находится между октябрем и декабрем 1988 г. Внешние проявления — «осыпание» случайных букв на экране, сопровождающееся характерным звуком капели. Вначале это развлекает пользователя, но затем делает работу на компьютере невозможной, так как с каждым разом «осыпание» происходит все чаще, а управление отключается от пользователя, пока не «упадет» последняя буква. Существуют небольшие модификации вируса, активизирующиеся по другим признакам (автору известна разновидность RC-1704, проявляющая себя по четным месяцам). Есть также модификация RC-1704F, форматирующая диск. Типичная ошибка большинства антивирусов-фагов (AIDSTEST (Д. Лозинский), VR (SiP)) в том, что они лечат RC-1701 и RC-1704 по одному и тому же алгоритму, что приводит к необратимой порче файлов, зараженных вирусом одного из этих двух типов. Автору известны две программы, лишенные этого недостатка: CLEAN (McAfee Associates) и PASTER (Г. Ландсберг). Индикатор-фаг PASTER способен обезвреживать резидентную часть вируса, даже если после него было запущено несколько резидентных программ. Это позволяет работать на вылеченном компьютере без его перезагрузки.

3.5. Вирусы Yankee Doodle. Имеют другое распространенное название — Five o'clock. Вирусы принадлежат к серии из нескольких похожих программ, играющих при определенных условиях мелодию Yankee Doodle Dandy. Автору известны две разновидности этого

вируса, удлиняющие COM-файлы на 1805 (RCE-1805) и 2885 (RCE-2885) байтов. Первая играет мелодию после нажатия комбинации клавиш Ctrl-Alt-Del (перезагрузка системы), вторая — в 16 : 59 : 53. Эти версии вируса не портят файловую систему. Имеется информация о существовании по крайней мере еще трех разновидностей вируса Yankee Doodle, последние из которых повреждают файлы. Вирусы написаны очень грамотно; при их создании были предприняты меры для нейтрализации программ-мониторов типа VIRBLK, ANTI4US (см. п. 2.3). Предусмотрена защита ет просмотра зараженных файлов отладчиками: при их использовании вирус RCE-2885 удаляет свое тело из файла. Существует несколько антивирусов-фагов, вылечивающих зараженные вирусами этой серии файлы: AIDSTEST (Д. Лозинский — 4 разновидности), VR (SiP — 3 разновидности), SHOPEN (Г. Ландсберг — RCE-2885). Программа SHOPEN способна обезвреживать резидентную часть вируса, даже при наличии других резидентных программ, что делает возможным работу на вылеченном компьютере без перезагрузки системы.

3.6. Вирус Vacsina. Имеет классификационный код RCE-1339. При заражении COM-файлов удлиняет их на 1339 байтов; при инфицировании EXE-модулей (вирус прикрепляется лишь к EXE-модулям с длиной, меньшей 64 Кбайтов) сначала удлиняет их на 132 байта, записывая в начало команду перехода на тело вируса, занимающегося только передачей управления собственно программе. После этого файл фактически перестает быть EXE-модулем и может быть вторично заражен вирусом Vacsina, но уже как COM-модуль. Не обладает деструктивным действием. Антивирусы-фаги, вылечивающие файлы от вируса Vacsina: ANTI-KOT (О. Котик), AIDSTEST (Д. Лозинский).

3.7. Вирус Dark Avenger. Имеет классификационный код RCE-1800. Другие названия этого вируса Sofia, Eddie. Dark Avenger чрезвычайно быстро распространяется, так как отслеживает не только запуск программ, но и открытие файлов с ними для чтения и записи, а также их закрытие. В связи с этим не может быть вылечен без нейтрализации резидентной части. Вирус один раз в 16 запусков зараженных программ (счетчик хранится в одном из незадействованных байтов boot-сектора) уничтожает относительно случайный сектор диска, помещая туда содержимое части оперативной памяти, начинающееся фразой «Eddie lives... somewhere in time!». Таким образом, вирус может испортить и файлы с данными. Вирус не позволяет точно восстановить длину зараженных EXE-модулей, если они имеют нестандартный заголовок, используемый для одновременного запуска под DOS и OS/2. Большинство антивирусов-фагов (VR (SiP), CLEAN (McAfee Associates)) неправильно восстанавливают длину EXE-модулей (при этом вылеченный файл становится несколько длиннее оригинала), даже когда такое возможно. Индикатор-фаг SOFIA (Г. Ландсберг) восстанавливает длину правильно всюду, где это осуществимо. В случае обнаружения зараженного OS/2-модуля он сообщает о том, что этот файл может быть вылечен неправильно, и его следует заменить фирменным оригиналом. Программа SOFIA способна также полностью нейтрализовывать резидентную часть вируса даже при наличии других резидентных программ, что позволяет работать на компьютере после лечения, не прибегая к перезагрузке системы.

3.8. Вирус Italian. Имеет классификационный код RBD-1024. Другие названия — Italian Bouncing и Ball. Этот вирус загрузчика

не обладает деструктивным действием. При определенных условиях по экрану начинает перемещаться точка, отражающаяся от его краев и некоторых символов. Как и большинство boot-вирусов, устраняется командой SYS, а также программами BOOTCHEK (McConachie Associates), AIDSTEST (Д. Лозинский).

3.9. Вирус Marijuana. Имеет классификационный код RBM-512. Другое название — Stone. Этот вирус также не обладает деструктивным действием. На гибких дисках он поражает boot-сектор, на жестких — таблицу партиций. С вероятностью 1/8 при загрузке на экране появляется надпись «Your PC is now stoned». Исходный загрузочный сектор помещается в последний сектор главного каталога на гибких дисках или в седьмой абсолютный сектор винчестера (обычно пустой). Есть сообщения о появлении нового штамма этого вируса, использующего кириллицу (видимо, повальная русификация западного программного продукта коснулась и вирусной сферы...). Методы лечения — те же, что и для вируса Italian (см. п. 3.8).

4. Универсальная антивирусная система PHENIX. В этом разделе кратко рассмотрена универсальная антивирусная система PHENIX, разработанная автором для комплексной защиты от вирусов. Подробнее она описана в отдельной работе [2], включающей в себя как объяснение принципов работы программы, так и инструкцию по ее использованию.

Из раздела 2 видно, что подавляющее большинство вирусов изменяет лишь малый фрагмент программного кода инфицируемых модулей. В связи с этим, если хранить информацию о длине программы, дате создания файла, а также элемент программного кода вблизи точки входа (и часть заголовка — в случае EXE-файлов), то часто возможно восстановить инфицированный вирусом общего назначения файл, даже если вирус этот новый и еще неизвестный! Действительно, по длине незараженного файла можно узнать размер вируса, а по фрагменту начального кода — в начале или в конце файла он находится. Итак, спасая информацию о заведомо неинфицированном файле (например, взятом с фирменных дистрибутивов), в дальнейшем можно не только обнаружить наличие в нем вируса, но обычно и устранить его.

Созданные ранее вакцины (см. п. 2.3) действовали подобно вирусам общего назначения без резидентной части, прикрепляясь к файлу и проверяя его незараженность перед передачей управления собственно программе. Такой способ обладает рядом недостатков. Во-первых, происходит удлинение файлов на несколько килобайтов, что уменьшает свободное пространство на диске. Во-вторых, увеличивается время загрузки программы в память (точнее — время от момента подачи команды на старт программы до начала выполнения собственно ее тела). В-третьпх, не все COM-файлы могут быть защищены подобным образом, так как их размер вместе с программой-вакциной не должен превышать 64 Кбайта. В-четвертых, при наличии на компьютере вируса типа Dark Avenger, отслеживающего открытие и закрытие файлов, лечение подобной вакциной вообще невозможно, так как только что вылеченный файл тут же заразится вновь при закрытии. Наконец, простота подобных программ, диктуемая условием экономии длины кода вакцины, в принципе, позволяет авторам вирусов легко преодолевать защиту. Все это привело к тому, что вакцинирующие программы не получили большого распространения.

Поэтому для устранения указанных недостатков в вакцине PHENIX используется другой принцип: хранятся только записи о состоянии файла, программа же, следящая за «здоровьем» компьютера, находится в отдельном файле и запускается периодически или при обнаружении странностей в поведении машины.

Возникает вопрос, где же хранить такую информацию (в дальнейшем называемую *защитной записью*)? Использование для этой цели базы данных, как это принято в программах, подсчитывающих контрольные суммы, неудобно по причинам, уже упоминавшимся в разделе 2.3: частое изменение файловой системы потребовало бы постоянного обновления базы данных с деятельным участием пользователя в этом процессе, так как он должен был бы постоянно отвечать на вопрос, является ли файл, не совпадающий по внутренней структуре с защитной записью, просто новой версией с тем же именем, или он заражен вирусом и его необходимо лечить. В связи с этим в PHENIXе используется концептуально другой подход: *защитная запись должна храниться в самом файле.* Это достигается либо помещением ее в конце файла, либо даже *внедрением записи в неиспользуемые области защищаемой программы* (область стека, незадействованная часть заголовка EXE-модулей и т. п.).

Таким образом, наличие короткой (около 40 байтов) защитной записи, не влияющей на скорость загрузки модуля, а при внедрении в тело программы — и на ее длину, позволяет восстановить файл, зараженный практически любым вирусом общего назначения! По оценкам автора, система PHENIX способна обезвреживать более 50 из существующих на сегодняшний день вирусов.

Для выявления и устранения вирусов загрузчика, во время вакцинирования файловой системы происходит также спасение загрузочных секторов и таблиц партиций. Начиная с версии 2.0, программа PHENIX при инсталляции ее на конкретный компьютер, производит синтаксический анализ кода BIOS с целью определения точки входа прерывания 13h, что дает уникальную возможность обнаружения и уничтожения boot-вирусов *в зараженной операционной системе* (см. п. 1.2.3-2.2 о перехвате прерывания 13h вирусами загрузчика).

В программе PHENIX приняты серьезные меры по шифровке своего кода, а также содержимого защитной записи и файлов с информацией о загрузочных секторах. Используется несколько видов контрольных сумм для проверки правильности восстановления инфицированных файлов.

Программа способна ликвидировать некоторые повреждения, создаваемые вирусами (например, восстанавливать файлы, испорченные вирусом Restart; см. п. 3.1), а также устранять дефекты в файлах, неправильно вылеченных плохими антивирусами-фагами. Не возникает никаких проблем с лечением многочисленных «штаммов» уже существующих вирусов, а также двух или более вирусов, одновременно находящихся на компьютере.

Система PHENIX имеет развитый интерфейс с пользователем на основе меню, что позволяет легко выбрать необходимую конфигурацию для работы. Имеется полная система обработки ошибок, включая ошибки дискового обмена.

Вакцина защищает как исполняемые модули, так и оверлейные части, драйверы и т. п. Защитная запись может быть в любой момент удалена из защищаемого файла. Имеется также возможность пометки отдельных файлов с целью пропуска их при защите и сканировании. Это полезно для программ типа SCAN (McAfee Associates), проверяющих свою конт-

рольную сумму при запуске. Информация о помеченных файлах тоже содержится в них самих, для чего используются некоторые тонкие особенности операционной системы MS DOS, связанные с хранением даты создания файла.

Программа является на сегодняшний момент одним из самых мощных средств обнаружения и уничтожения вирусов и при регулярном использовании надежно защищает компьютер от их проникновения.

Заключение. Есть ли повод для оптимизма? Вирусы распространились на IBM PC-совместимых компьютерах в рекордно короткий срок. Число их новых видов неуклонно растет, причем все быстрее и быстрее. Есть ли повод для оптимизма, или вирусы вскоре сделают работу в простых операционных системах невозможной?

На взгляд автора, ситуация не так уж безнадежна. Существующие в настоящее время средства защиты, уже закаленные в борьбе с вирусами, заметно усложняют создание новых их видов, незаметных для программ-антивирусов. На сегодняшний день, написание такого вируса — задача на порядок более сложная, чем это было 3 года назад. Можно надеяться, что озлобленные неудачники (а именно они, по мнению психологов, создают наиболее разрушительные вирусы), не смогут преодолеть этот барьер. Конструкторы вирусов, конечно, останутся. Хочется верить, что это будут действительно талантливые программисты, пишущие красивые вирусные программы для собственного удовлетворения и не ставящие своей целью разрушение данных и создание помех другим пользователям...

Вместе с определенным «глобальным» оптимизмом следует иметь в виду, что многие вирусы еще не появились в СССР. Тут не должно быть никаких иллюзий! Эти вирусы обязательно придут, как и вирусные программы, создаваемые в Советском Союзе [16] ●. И к их появлению надо быть готовыми!

В заключение хотелось бы упомянуть о некоторых источниках информации, использовавшихся при написании настоящего обзора и не указанных в библиографии. Ряд сведений о структуре вирусов содержится в инструкциях к программам-фагам ANTI-KOT (О. Котик), AIDSTEST (Д. Лозинский) и SCAN (McAfee Associates). Информация о программе-черве WNK была любезно предоставлена M. Ikeda. Автор благодарен всем этим лицам.

ПРИМЕЧАНИЯ

[1] Address = (segment $\ll$ 4) + offset, где $a \ll n$ означает сдвиг слова a влево на n битов, что эквивалентно умножению его на 2^n.

[2] Процессоры Intel 80286 и 80386 имеют расширенный набор команд, но большинство прикладных программ, рассчитанных на работу на любом компьютере типа IBM PC, не использует эту возможность.

[3] Здесь и далее символ h после числа обозначает шестнадцатиричную систему счисления (100 h = 256).

[4] Это напоминает поведение больного, не идущего на прием к врачу до наступления серьезной фазы болезни и заражающего других.

[5] Хэкер (от англ. hacker) — человек, занимающийся «компьютерным хулиганством», т. е. пытающийся незаконным образом использовать ЭВМ (подбор паролей, установление себе повышенного приоритета, «взламывание» защитных систем и т. п.).

[6] Когда автор писал этот обзор, поступило сообщение о том, что Моррис был оштрафован на крупную сумму денег.

[7] В настоящее время известен единственный такой вирус, описанный в книге [15].

[8] Есть еще несколько подобных «неуловимых» вирусных программ, ведущих себя, на первый взгляд, очень странно и необъяснимо. Наличие таких «интеллектуальных» вирусов и порождает массу легенд о неуловимости и сверхъестественности компьютерных бацилл. На самом деле, ничего необъяснимого в их поведении нет и быть не может, так как все вирусы представляют собой всего-навсего программы, иногда, правда, очень грамотно написанные.

[9] Некоторые вирусы, например Yankee Doodle (см. раздел 3), изменяют большее число байтов в начале COM-файлов, так как хранят на их месте некоторую служебную информацию.

[10] Практически все дисковые контроллеры (кроме, быть может, самых первых) обладают способностью помечать дефектные секторы на дисках, которые могут возникать из-за царапин, неоднородности магнитного слоя и т. п., как плохие. Далее, операционные системы не используют такие секторы.

[11] Этот вирус переставляет местами пары цифр в файлах с расширением .DBF (используемым базами данных). Обнаружить ошибки бывает очень сложно, пока, например, кто-нибудь не получит 0100 долларов вместо причитающихся 1000,

[12] Автор сомневается в полезности сигнатуры для создания антивирусов, так как именно ее сразу будут изменять создатели «штаммов».

[13] Автор имел неосторожность вылечить один компьютер от вируса Yankee Doodle пробной версией (V 1.0) своего антивируса SHOPEN, после чего, несмотря на просьбу не распространять эту несовершенную копию, в течение полугода вынужден был заменять ее качественной версией (V 1.7) на многих персональных компьютерах ИФВЭ.

[14] Выражение $a : b$ обозначает far адрес с segment = a, offset = b.

[15] Об одном отечественном вирусе — Чуче — уже упоминалось в разделе 1.2.3-4. По-видимому, это — первая советская вирусная программа. Она безвредна, а ее проявление заключается в том, что при определенных условиях на экране появляется надпись «Хочу Чучу!». После этого компьютер отказывается работать, пока пользователь не введет с клавиатуры слово «Чуча».

СПИСОК ЛИТЕРАТУРЫ

[1] MS DOS 3.30 Technical Reference.— Microsoft Press, 1984 — 1988.
2. *Ландсберг Г. Л.* Препринт. ИФВЭ 90-122.— Протвино, 1990.
3. *Чижов А. А.* // В мире персональных компьютеров. 1988. № 1. С. 121.
4. *Безруков Н. Н.* Компьютерная вирусология. Ч. 1.— Киев: КНИГА, 1989.
5. *Карасик И. Ш.* // Интеркомпьютер. 1989. № 2. С. 14.
6. *Карасик И. Ш.* // Интеркомпьютер. 1990. № 1. С. 39.
7. *Карасик И. Ш.* // Мир ПК. 1989. № 3. С. 127.
8. *Greenberg R. M.* // Byte. 1989. V. 14, No. 6.
9. *McAfee J.* // Datamation. 1989. V. 35, No. 4. P. 29.
10. *Denning P. J.*//Am. Sci. 1988. V. 76. P. 236.
[11]. *Eliot M.* // Science. 1988. V. 240, No. 4849. P. 133.
12. *Coken F.* // Computers and Security. 1988. V. 7. P. 167.
13. *Бончев В.* // Компьютер за вас. (*болг.*) 1989. № 3—4. С. 8.
14. New viral strains take hold//Computing. December 15, 1988. P. 4.
15. Computer Viruses: A High-Tech. Decease.— MI. 1988.
16. *McAfee J.*, *Haykes K.* Computer Viruses, Warms, Data-Diddlers, Killer Programme and Other Threats to the System: What They Are, How They Work and How to Defend Your PC or Mainframe.— New York, 1989.
17. *Cohen F.* // Computers and Security. 1989. V. 8, No. 8.
18. *Dewdney A. K.* // Sci. American. 1985. V. 252, No. 3. P. 14.
19. *Dewdney A. K.* // Ibidem. V. 250, No. 5.
20. *Shock J. F., Hupp J. A.* //Commun. ACM. 1982. V. 25. P. 172.
[21] *Solomon A.* // Pers. Comput. World. 1988. V. 11. P. 166.
22. *Crowford D.* //Commun. ACM. 1989. V. 32. P. 780.

23. Byte. 1989. V. 14, No. 9. P. 19.
24. *Дьюдни А. К.* // В мире науки. 1989, № 5. С. 82.
25. В мире персональных компьютеров. 1988. № 1. С. 122.
26. Technical Reference for the IBM Personal Computer XT. Part Number 6936763.
27. Химия и жизнь. 1989. № 7.
28. *Борхес Х. Л.* Проза разных лет.— М.: Радуга, 1984.— С. 218.
29. *Окунь Л. Б.* Физика элементарных частиц.— М.: Наука, 1988.— С. 177—178.
30. *Безруков Н. Н.* // Интеркомпьютер. 1990. № 2. С. 37.
31. *Чижов М. В.* Препринт ОИЯИ Р11-90-313.— Дубна, 1990.
32. *Карасик И. Ш.* // Интеркомпьютер. 1990. № 2. С. 40.
33. PC Magazine. April 1989. P. 193.

Статья поступила 3.10.90 г.