**Оглавление**

Введение 3

1. История компьютерных вирусов — от древности до наших дней 4

1.1. Немного археологии 4

1.2. Начало пути 4

1.3. Полиморфизм - мутация вирусов 5

1.4. Автоматизация производства и конструкторы вирусов 6

2. Хронология событий 7

3. Перспективы: что будет завтра и послезавтра 16

3.1. Что будет завтра? 16

3.2. Что будет послезавтра? 16

4. Классификация компьютерных вирусов 18

5. Методы борьбы с вирусами. 20

5.1. Методы обнаружения и удаления компьютерных вирусов 20

5.2. DOCTOR WEB – одна из популярнейших антивирусных программ. 20

Заключение 22

Список литературы 23

# Введение

Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему уже написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются сотни (или тысячи) специалистов в десятках (а может быть, сотнях) компаний. Казалось бы, тема эта не настолько сложна и актуальна, чтобы быть объектом такого пристального внимания. Однако это не так. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономичсеских величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

При этом следует иметь в виду, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов. Примерно так же плохо обстоят дела на другой стороне тандема «человек-компьютер». Как пользователи, так и профессионалы-программисты часто не имеют даже навыков «самообороны», а их представления о вирусе порой являются настолько поверхностными, что лучше бы их (представлений) и не было.

Немногим лучше обстоят дела на Западе, где и литературы побольше (издается аж три ежемесячных журнала, посвященных вирусам и защите от них), и вирусов поменьше (поскольку «левые» китайские компакт-диски особо на рынок не поступают), и антивирусные компании ведут себя активнее (проводя, например, специальные конференции и семинары для специалистов и пользователей).

У нас же, к сожалению, все это не совсем так. И одним из наименее »проработанных» пунктов является литература, посвященная проблемам борьбы с вирусами. На сегодняшний день имеющаяся на прилавках магазинов печатная продукция антивирусного толка либо давно устарела, либо написана непрофессионалами, либо авторами типа Хижняка, что гораздо хуже.

Довольно неприятным моментом является также опережающая работа Российского компьютерного «андеграунда»: только за два года было выпущено более десятка электронных номеров журнала вирусописателей «Infected Voice», появилось несколько станций BBS и WWW-страниц, ориентированные на распространение вирусов и сопутсвующей информации.

Все это и послужило толчком к тому, чтобы собрать воедино весь материал, который скопился у меня за восемь лет профессиональной работы с компьютерными вирусами, их анализа и разработке методов обнаружения и лечения.

**Обязательным (необходимым) свойством компьютерного вируса** является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

# 1. История компьютерных вирусов — от древности до наших дней

## 1.1. Немного археологии

Мнений по поводу даты рождения первого компьютерного вируса очень много. Мне доподлинно известно только одно: на машине Беббиджа его не было, а на Univac 1108 и IBM-360/370 они уже были («Pervading Animal» и «Christmas tree»). Таким образом, первый вирус появился где-то в самом начале 70-х или даже в конце 60-х годов, хотя «вирусом» его никто еще не называл. На этом разговор о вымерших ископаемых предлагаю считать завершенным.

# 1.2. Начало пути

Поговорим о новейшей истории: «Brain», «Vienna», «Cascade» и далее. Те, кто начал работать на IBM-PC аж в середине 80-х, еще не забыли повальную эпидемию этих вирусов в 1987-89 годах. Буквы сыпались на экранах, а толпы пользователей неслись к специалистам по ремонту дисплеев (сейчас все наоборот: винчестер сдох от старости, а валят на неизвестный передовой науке вирус). Затем компьютер заиграл чужеземный гимн «Yankee Doodle», но чинить динамики уже никто не бросился - очень быстро разобрались, что это - вирус, да не один, а целый десяток.

Так вирусы начали заражать файлы. Вирус «Brain» и скачущий по экрану шарик вируса «Ping-pong» ознаменовали победу вируса и над Boot-сектором. Все это очень не нравилось пользователям IBM-PC, и - появились противоядия. Первым попавшимся мне антивирусом был отечественный ANTI-KOT: это легендарный Олег Котик выпустил в свет первые версии своей программы, которая уничтожала целых 4 (четыре) вируса (американский SCAN появился у нас в стране несколько позднее). Кстати, всем, кто до сих пор сохранил копию этого антивируса, предлагаю немедленно ее стереть (да простит меня Олег Котик!) как программу вредную и ничего, кроме траты лишних нервов и ненужных телефонных звонков, не приносящую. К сожалению, ANTI-KOT определяет вирус «Time» («Иерусалимский») по комбинации «MsDos» в конце файла, а некоторые другие антивирусы эти самые буквы аккуратно прицепляют ко всем файлам с расширением COM или EXE.

Следует обратить внимание на то, что истории завоевания вирусами России и Запада различаются между собой. Первым вирусом, стремительно распространившимся на Западе был загрузочный вирус «Brain», и только потом появились файловые вирусы «Vienna» и «Cascade». В России же наоборот, сначала появились файловые вирусы, а годом позже - загрузочные.

Время шло, вирусы плодились. Все они были чем-то похожи друг на друга, лезли в память, цеплялись к файлам и секторам, периодически убивали файлы, дискеты и винчестеры. Одним из первых «откровений» стал вирус «Frodo.4096» - первый из известных мне файловых вирусов-невидимок (стелс). Этот вирус перехватывал INT 21h и, при обращении через DOS к зараженным файлам, изменял информацию таким образом, что файл появлялся перед пользователем в незараженном виде. Но это была только надстройка вируса над MS-DOS. Не прошло и года, как электронные тараканы полезли внутрь ядра DOS (вирус-невидимка «Beast.512»). Идея невидимости продолжала приносить свой плоды и далее: летом 1991 года пронесся, кося компьютеры как бубонная чума, вирус «Dir\_II». «Да-a-a!» сказали все, кто в нем копался.

Но бороться с невидимками было довольно просто: почистил RAM - и будь спокоен, ищи гада и лечи его на здоровье. Побольше хлопот доставляли самошифрующиеся вирусы, которые иногда всречались в очередных поступлениях в коллекции. Ведь для их идентификации и удаления приходилось писать специальные подпрограммы, отлаживать их. Но на это никто тогда не обращал внимания, пока... Пока не появились вирусы нового поколения, те, которые носят название полиморфик-вирусы. Эти вирусы используют другой подход к невидимости: они шифруются (в большинстве случаев), а в расшифровщике используют команды, которые могут не повторяться при заражении различных файлов.

## 1.3. Полиморфизм - мутация вирусов

Первый полиморфик-вирус появился в начале 90-х кодов - «Chameleon», но по-настоящему серьезной проблема полиморфик-вирусов стала лишь год спустя - в апреле 1991-го, когда практически весь мир был охвачен эпидемией полиморфик-вируса «Tequila» (насколько мне известно, эта эпидемия практически не затронула Россию, а первая Российская эпидемия, вызванная полиморфик-вирусом, произошла аж три года спустя - год 1994, это был вирус «Phantom1»).

Популярность идеи самошифрующихся полиморфик-вирусов вылилась в появление генераторов полиморфик-кода - в начале 1992 появляется знаменитый вирус «Dedicated», базирующийся на первом известном полиморфик-генераторе MtE и открывший серию MtE-вирусов, а через довольно короткое время появляется и сам полиморфик-генератор. Представляет он из себя объектный модуль (OBJ-файл), и теперь для того чтобы из самого обычного нешифрованного вируса получить полиморфик-мутанта достаточно лишь слинковать их объектные модули - OBJ-файл полиморфик-генератора и OBJ-файлом вируса. Теперь автору вируса, если он желает создать настоящий полиморфик-вирус, не придется корпеть над кодами собственного за/расшифровщика. При желании он может подключить к своему вирусу полиморфик-генератор и вызывать его из кодов вируса.

К счастью, первый MtE-вирус не попал в «живую природу» и не вызвал эпидемии, а разработчики антивирусных программ, соответственно, имели некоторый запас времени для подготовки к отражению новой напасти.

Всего год спустя производство полиморфик-вирусов становится уже «ремеслом», и в 1993 году произошел их «обвал». В поступающих в коллекцию вирусах удельный вес самошифрующихся полиморфик-вирусов становится все больше и больше. Создается впечатление, что одним из основных направлений в трудном деле создания вирусов становится разработка и отладка полиморфик-механизма, а конкуренция среди авторов вирусов сводится не к тому, кто из них напишет самый крутой вирус, а чей полиморфик-механизм окажется круче всех.

Вот далеко не полный список тех из них, которые можно назвать стопроцентно полиморфичными (конец 1993):

Bootache, CivilWar (четыре версии), Crusher, Dudley, Fly, Freddy, Ginger, Grog, Haifa, Moctezuma (две версии), MVF, Necros, Nukehard, PcFly (три версии), Predator, Satanbug, Sandra, Shoker, Todor, Tremor, Trigger, Uruguay (восемь версий).

Для обнаружения этих вирусов приходится использовать специальные методы, к которым можно отнести эмуляцию выполнения кода вируса, математические алгоритмы восстановления участков кода и данных в вирусе и т.д. К не-стопроцентным полиморфикам (т.е. которые шифруют себя, но в расшифровщике вируса всегда существуют постоянные байты) можно отнести еще десяток новых вирусов:

Basilisk, Daemaen, Invisible (две версии), Mirea (несколько версий), Rasek (три версии), Sarov, Scoundrel, Seat, Silly, Simulation.

Однако и они требуют расшифровки кода для их детектирования и восстановления пораженных объектов, поскольку длина постоянного кода в рассшифровщике этих вирусов слишком мала.

Параллельно с полиморфик-врусами развиваются полиморфик-генераторы. Появляется несколько новых, использующих более сложные методы генерации полиморфик-кода, они распространяются по станциям BBS в виде архивов, содержащих объектные модули, документацию и примеры использования. В конце 1993 года было известно уже семь генераторов полиморфик-кода. Это:

MTE 0.90 (Mutation Engine), четыре различные версии TPE (Trident Polymorphic Engine), NED (Nuke Encryption Device), DAME (Dark Angel's Multiple Encryptor)

С тех пор новые полиморфные генераторы появлялись по несколько штук в год, и приводить их полный список вряд ли имеет смысл.

## 1.4. Автоматизация производства и конструкторы вирусов

Лень - движущая сила прогресса. Эта народная мудрость не нуждается в комментариях. Но только в середине 1992 года прогресс в виде автоматизации производства дошел и до вирусов. Пятого июля 1992 года объявлен к выпуску в свет первый конструктор вирусного кода для IBM-PC совместимых компьютеров - пакет VCL (Virus Creation Laboratory) версии 1.00.

Этот конструктор позволяет генерировать исходные и хорошо откомментированные тексты вирусов (файлы, содержащие ассемблерный текст), объектные модули и непосредственно зараженные файлы. VCL снабжен стандартным оконным интерфейсом. При помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, подключить до десяти эффектов, сопровождающих работу вируса и т.п. Вирусы могут использовать стандартный способ поражения файлов в их конец, или записывать себя вместо файлов, уничтожая их первоначальное содержимое, или являться вирусами-спутниками (международный термин - компаньон-вирусы [companion]).

И все сразу стало значительно проще: захотел напакостить ближнему - садись за VCL и, за 10-15 минут настрогав 30-40 разных вирусов, запусти их на неприятельском компьютере(ах). Каждому компьютеру - отдельный вирус!

Дальше - больше. 27 июля появилась первая версия конструктора PS-MPC (Phalcon/Skism Mass-Produced Code Generator). Этот конструктор не содержит в себе оконного интерфейса и генерирует исходные тексты вирусов по файлу конфигурации. Этот файл содержит в себе описание вируса: тип поражаемых файлов (COM или EXE); резидентность (PS-MPC создает также и резидентные вирусы, чего не позволяет конструктор VCL); способ инсталляции резидентной копии вируса; возможность использования самошифрования; возможность поражения COMMAND.COM и массу другой полезной информации.

На основе PS-MPC был создан конструктор G2 (Phalcon/Skism's G2 0.70 beta), который поддерживает файлы конфигурации стандарта PS-MPC, однако при генерации вируса использует большее количество вариантов кодирования одних и тех же функций.

Имеющаяся у меня версия G2 помечена первым января 1993 года. Видимо, новогоднюю ночь авторы G2 провели за компьютерами. Лучше бы они вместо этого попили шампанского, хотя одно другому не мешает.

Итак, каким же образом повлияли конструкторы вирусов на электронную фауну? В коллекции вирусов, которая хранится на моем «складе», количество «сконструированных» вирусов следующее: на базе VCL и G2 - по несколько сотен;  
на базе PS-MPC - более тысячи.

Так проявилась еще одна тенденция в развитии компьютерных вирусов: все большую часть в коллекциях начинают занимать «сконструированные» вирусы, а в ряды их авторов начинают вливаться откровенно ленивые люди, которые сводят творческую и уважаемую профессию вирусописания к весьма заурядному ремеслу.

# 2. Хронология событий

Пора перейти к более детальному описанию событий. Начнем с самого начала.

конец 1960 - начало 1970-х

На мейнфреймах этого времени периодически появлялись программы, которые получили название «кролик» (the rabbit). Эти программы клонировали себя, занимали системные ресурсы и таким образом снижали производительность системы. Скорее всего «кролики» не передавались от системы к системе и являлись сугубо местными явлениями - ошибками или шалостями системных программистов, обслуживавших компьютер. Первый же инцидент, который смело можно назвать эпидемией «компьютерного вируса», произошел на системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам - делал практически то же самое, что тысячи современных компьютерных вирусов.

первая половина 1970-х

Под операционную систему Tenex создан вирус «The Creeper», использовавший для своего распространения глобальные компьютерные сети. Вирус был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. Для борьбы с этим вирусом была создана программа «The Reeper» - первая известная антивирусная программа.

Начало 1980-х

Компьютеры становятся все более и более попуярными. Появляется все больше и больше программ, авторами которых являются не софтверные фирмы, а частные лица, причем эти программы имеют возможность свободного хождения по различным серверам общего доступа - BBS. Результатом этого является появление большого числа разнообразных «троянских коней» - программ, которые при их запуске наносят системе какой-либо вред.

1981

Эпидемия загрузочного вируса «Elk Cloner» на компьютерах Apple II. Вирус записывался в загрузочные сектора дискет, к которым шло обращение. Проявлял он себя весьма многосторонне - переворачивал экран, заставлял мигать текст на экране и выводил разнообразные сообщения.

1986

Пандемия первого IBM-PC вируса «Brain». Вирус, заражающий 360Kб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» являлась скорее всего неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус.

Вирус был написан в Пакистане братьями Basit и Amjad Farooq Alvi, оставившими в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Как утверждали авторы вируса, они являлись владельцами компании по продаже программных продуктов и решили выяснить уровень пиратского копирования в их стране. К сожалению, их эсперимент вышел за границы Пакистана.

Интересно, что вирус «Brain» являлся также и первым стелс-вирусом - при попытке чтения зараженного сектора он «подставлял» его незараженный оригинал.

В том же 1986 году программист по имени Ральф Бюргер (Ralf Burger) обнаружил, что программа может делать собственные копии путем добавления своего кода к выполняемым DOS-файлам. Его первый вирус, названный «VirDem», демонстрировал эту возможность. Этот вырус был проаннонсирован в декабре 1986 на форуме компьютерного «андеграунда» - хакеров, специализировавшихся в то время на взломе VAX/VMS-систем (Chaos Computer Club in Hamburg).

1987

Появление вируса «Vienna». Копия этого вируса попадает в руки все того же Ральфа Бюргера, который дизассемблирует вирус и помещает результат в свою книгу «Computer Viruses: A High Tech Desease» (русский аналог - «Пишем вирус и антивирус» г. Хижняка). Книга Бюргера популяризовала идею написания вирусов, объясняла как это происходит и служила таким образом толчком к написению сотен или даже тысяч компьютерных вирусов, частично использовавших идеи из этой книги.

В том же году независимо друг от друга появляется еще несколько вирусов для IBM-PC. Это знаменитые в прошлом «Lehigh», заражающий только COMMAND.COM, «Suriv-1» (другое название - «April1st»), заражающий COM-файлы, «Suriv-2», заражающий (впервые) EXE-файлы, и «Suriv-3», заражающий как COM-, так и EXE-файлы. Появляются также несколько загрузочных вирусов («Yale» в США, «Stoned» в Новой Зеландии и «PingPong» в Италии) и первый самошифрующийся файловый вирус «Cascade».

Не остались в стороне и не-IBM-компьютеры: было обнаружено несколько вирусов для Apple Macintosh, Commodore Amiga и Atari ST.

В декабре 1987 произошла первая известная повальная эпидемия сетевого вируса «Cristmas Tree», написанного на языке REXX и распрастранявшего себя в сперационной среде VM/CMS. 9-го декабря вирус был запущен в сеть Bitnet в одном из университетов Западной Германии, проник через шлюз в European Academic Research Network (EARN) и затем - в сеть IBM VNet. Через четыре дня (13 декабря) вирус парализовал сеть - она была забита его копиями (см. пример про клерка несколькими страницами выше). При запуске вирус выводил на экран изображение новогодей (вернее, рождественской) елочки и рассылал свои копии всем пользователям сети, чьи адреса присутствовали в соответствующих системных файлах NAMES и NETLOG.

1988

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом «Jerusalem» - в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей пандемии - сообщения о зараженных компьютерах поступали из Европы, Америки и Ближнего Востока. Название, кстати, вирус получил по месту одного из инцидентов - университета в Иерусалиме.

Вместе с несколькими другими вирусами («Cascade», «Stoned», «Vienna»), вирус «Jerusalem» распространился по тысячам компьютеров, оставаясь незамеченным - антивирусные программы еще не были распространены в то время так же широко как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Показателен тот факт, что в том же году компьютерный гуру и человек-легенда Питер Нортон высказался против существования вирусов. Он объявил их несуществующим мифом и сравнил со сказками о крокодилах, живущих в канализации Нью-Йорка. Этот казус, однако, не помешал фирме Symantec через некоторое время начать собственный антивирусный проект - Norton Anti-Virus.

Начали появляться заведомо ложные сообщения о компьютерных вирусах, никакой реальной информации не содержащие, но вносившие панику в стройные ряды компьютерных пользователей. Одна из первых таких «злых шуток» (современный термин - «virus hoax») принадлежит некому Mike RoChenle (псевдоним похож на «Microchannel»), который разослал на станции BBS большое количество сообщений о якобы существующем вирусе, который передается от модема к модему и использует для этого скорость 2400 бод. Как это ни смешно, многие пользоватеили отказались от стандарта тех дней 2400 и снизили скорость своих модемов до 1200 бод. Подобные «hoax»-ы появляются и сейчас. Наиболее известны на сегодняшний день - GoodTimes и Aol4Free.

Ноябрь 1988: повальная эпидемия сетевого вируса Морриса (другое название - Internet Worm). Вирус заразил более 6000 компьютерных систем в США (включая NASA Research Institute) и практически парализовал их работу. По причине ошибки в коде вируса он, как и вирус-червь «Cristmas Tree», неограниченно рассылал свои копии по другим компьютьерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

Вирус использовал для своего размножения ошибки в операционной системе Unix для VAX и Sun Microsystems. Помимо ошибок в Unix вирус использовал несколько других оригинальных идей, например, подбор паролей пользователей. Подробнее об этом вирусе и связанным с ним инцидентом можно прочитать в достаточно подробной и интересной статье Игоря Моисеева в журнале КомпьютерПресс, 1991, N8,9.

Декабрь 1988: сезон вирусов-червей продолжается, на этот раз в сети DECNet. Вирус-червь HI.COM выводил на экран изображение елочки и извещал пользователей, что им следует «stop computing and have a good time at home!!!»

Появляются новые антивирусные программы, например, Dr.Solomon's Anti-Virus Toolkit, являющийся на сегодняшний день одним из самых мощных антивирусов.

1989

Появляются новые вирусы - «Datacrime», «FuManchu» и целые семейства - «Vacsina» и «Yankee». Первый имел крайне опасное проявление - с 13 октября по 31 декабря он форматировал винчестер. Этот вирус вырвался «на свободу» и вызвал повальную истерию в средствах массовой информации в Голландии и Великобритании.

Сентябрь 1989: на рынок выходит еще одна антивирусная программа - IBM Anti-Virus.

Октябрь 1989: в сети DECNet зафиксирована еще одна эпидемия вируса-червя - «WANK Worm».

Декабрь 1989: инцидент с «троянским конем» «Aids». Было разослано 20.000 его копий на дискетах, помеченных как «AIDS Information Diskette Version 2.0». После 90 загрузок системы «троянец» шифровал имена всех файлов на диске, делал их невидимыми (атрибут «hidden») и оставлял на диске только один читаемый файл - счет на 189 долларов, который следовало послать по адресу PO Box 7, Panama. Автор «троянца» был пойман и приговорен к тюремному заключению.

Следует отметить тот факт, что 1989 год являлся началом повальной эпидемии компьютерных вирусов в России - все те же вирусы «Cascade», «Jerusalem» и «Vienna» заполонили компьютеры российских пользователей. К счастью, российские программисты довольно быстро разобрались с принципами их работы и практически сразу появилось несколько отечественных противоядий-антивирусов.

Мое первое знакомство с вирусом (это был вирус «Cascade») произошло в октябре 1989 года - вирус оказался обнаруженным на моем рабочем компьютере. Именно это и послужило толчком для моей профессиональной переориентации на создание программ-антивирусов. Кстати, тот первый вирус я вылечил популярной в те времена антивирусной программой ANTI-KOT Олега Котика. Месяцем позже второй инцидент (вирус «Vacsina») был закрыт при помощи первой версии моего антивируса -V (который несколькими годами позже был переименован в AVP - AntiViral Toolkit Pro). К концу 1989 года на просторах России паслось уже около десятка вирусов (перечислены в порядке их появления): две версии «Cascade», несколько вирусов «Vacsina» и «Yankee», «Jerusalem», «Vienna», «Eddie», «PingPong».

1990

Этот год принес несколько довольно заметных событий. Первым из них является появление первых полиморфик-вирусов «Chameleon» (другое название - «V2P1», «V2P2» и «V2P6»). До этого момента антивирусные программы для поиска вирусов пользовались так называемыми «масками» - кусками вирусного кода. После появления вирусов «Chameleon» разработчики антивирусных программ были вынуждены искать другие методы их обнаружения.

Вторым событием являлось появление болгарского «завода по производству вирусов»: огромное количество новых вирусов имели болгарское происхождение. Это были целые семейства вирусов «Murphy», «Nomenclatura», «Beast» (или «512», «Number-of-Beast»), новые модификации вируса «Eddie» и др. Особенную активность проявлял некто Dark Avenger, выпускавший в год по несколько новых вирусов, использовавших принципиально новые алгоритмы заражения и скрытия себя в системе. В Болгарии же впервые появлась и первая BBS, ориентированная на обмен вирусами и информацией для вирусописателей.

В июле 1990 произошел инцидент с компьютерным журналом PC Today (Великобретания). Он содержал флоппи-диск, зараженный вирусом «DiskKiller». Было продано более 50.000 копий журнала.

Во второй половине 1990-го появились два стелс-монстра - «Frodo» и «Whale». Оба вируса использовали крайне сложные стелс-алгоритмы, а девятикилобайтный «Whale» к тому же применял несколько уровней шифровки и анти-отладочных приемов.

Появились и первые известные мне отечественные вирусы: «Peterburg», «Voronezh» и ростовский «LoveChild».

1991

Популяция компьютерных вирусов непрерывно растет, достигая уже нескольких сотен. Растет и антивирусная активность: сразу два софтверных монстра (Symantec и Central Point) выпускают собственные антивирусные программы - Norton Anti-Virus и Central Point Anti-Virus. Следом появляются менее известные антивирусы от Xtree и Fifth Generation.

В апреле разразилась настоящая эпидемия файлово-загрузочного полиморфик-вируса «Tequila», а в сентябре подобная же «история» произошла с вирусом «Amoeba». Россию эти события практически не затронули.

Лето 1991: эпидемия вируса «Dir\_II», использовавшего принципиально новые способы заражения файлов (link-вирус).

В целом, год 1991 был достаточно спокойным - этакое затишье перед бурей, разразившейся в 1992-м.

1992

Вирусы для не-IBM-PC и не-MS-DOS практически забыты: «дыры» в глобальных сетях закрыти, ошибки исправлены, и сетевые вирусы-черви потеряли возможность для распространения. Все большую и большую значимость начинают приобретать файловые, загрузочные и файлово-загрузочные вирусы для наиболее распространенной операционной системы (MS-DOS) на самом популярном компьютере (IBM-PC). Количество вирусов растет в геометрической прогрессии, различные инциденты с вирусами происходят чуть ли не ежедневно. Развиваются различные антивирусные программы, выходят десятки кних и несколько регулярных журналов, посвященных вирусам. На этом фоне выделяются несколько основных моментов:

Начало 1992: первый полиморфик-генератор MtE, на базе которого через некоторое время появляется сразу несколько полиморфик-вирусов. MtE явился также прообразом нескольких последующих полиморфик-генераторов.

Март 1992: эпидемия вируса «Michelangelo» («March6») и связанная с этим истерия. Наверное, это первый известный случай, когда антивирусные компании раздували шумиху вокруг вируса не для того, чтобы защитить пользователей от какой-либо опасности, а для того, чтобы привлечь внимание к своему продукту, т.е. в целях извлечения коммерческой выгоды. Так одна американская антивирусная компания заявила, что 6-го марта будет разрушена информация более чем на пяти миллионах компьютеров. В результате поднявшейся после этого шумихи прибыли различных антивирусных фирм поднялись в несколько раз, а от вируса в дейтсвительности пострадали всего около 10.000 машин.

Июль 1992: появление первых конструкторов вирусов VCL и PS-MPC, которые увеличили и без того немаленький поток новых вирусов и, как и MtE в своей области, подтолкнули вирусописателей к созданию других, более мощных конструкторов.

Конец 1992: первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую страницу в вирусописательстве.

1993

Вирусописатели серьезно взялись за работу: помимо сотен рядовых вирусов, принципиально не отличающихся от своих собратьев, помимо целого ряда новых полиморфик-генераторов и конструкторов, помимо новых электронных изданий врусописателей появляется все больше и больше вирусов, использующих крайне необычные способы заражения файлов, проникновения в систему и т.д. Основными примерами являются:

«PMBS», работающий в защищенном режиме процессора Intel 80386.

«Strange» (или «Hmm») - сольное выступление на тему «стелс-вирус», однако выполненное на уровне аппаратных прерываний INT 0Dh и INT 76h.

«Shadowgard» и «Carbuncle», значительно расширившие диапазон алгоритмов компаньон-вирусов;

«Emmie», «Metallica», «Bomber», «Uruguay» и «Cruncher» - использование принципиально новых приемов «спрятывания» своего кода в зараженных файлах.

Весной 1993 Microsoft выпустил свой собственный антивирус MSAV, основой которого послужил CPAV от Central Point.

1994

Все большее значение приобретает проблема вирусов на компакт-дисках. Быстро став популярными, эти диски оказались одним из основных путей распространения вирусов. Зафиксировано сразу несколько инцидентов, когда вирус попадал на мастер-диск при подготовке партии компакт-дисков. В результате на компьютерный рынок были выпущены довольно большие тиражи (десятки тысяч) зараженных дисков. Естественно, что об их лечении говорить не приходится - их придется просто уничтожить.

В начале года в Великобритании появились два крайне сложных полиморфик-вируса - «SMEG.Pathogen» и «SMEG.Queeg» (до сих пор не все антивирусные программы в состоянии достичь 100%-го результата при их детектировании). Автор вирусов помещал зараженные файлы на станции BBS, что явилось причиной настоящей эпидемии и паники в средствах массовой информации.

Еще одну волну паники вызвало сообщение о якобы существующем вирусе «GoodTimes», распространяющем себя по сети Интернет и заражающем компьютер при получении электронной почты. Накакого такого вируса на самом деле не существовало, однако через некоторое время появился обычный DOS-вирус с текстом «Good Times», вирус этот получил название «GT-Spoof».

Активизируются правоохранительные органы: летом 1994 автор SMEG был «вычислен» и арестован. Примерно в то же самое время в той же Великобритании арестована целая группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

Появляются несколько новых достаточно необычных вирусов:

Январь 1994: «Shifter» - первый вирус, заражающий объектные модули (OBJ-файлы). «Phantom1» - эпидемия первого полиморфик-вируса в Москве.

Апрель 1994: «SrcVir» - семейство вирусов, заражающих исходные тексты программ (C и Pascal).

Июнь 1994: «OneHalf» - начало повальной эпидемии вируса, до сих пор являющегося самым популярным вирусом в России.

Сентябрь 1994: «3APA3A» - эпидемия файлово-загрузочного вируса, использующего крайне необычный способ внедрения в MS-DOS. Ни один антивирус не оказался готовым к встрече с подобного типа монстром.

В 1994 году (весна) перестал существовать один из антивирусных лидеров того времени - Central Point. Он был приобретен фирмой Симантек, которая до того уже успела «проглотить» несколько небольших фирм, занимавшихся антивирусными разработками - Peter Norton Computing, Certus International и Fifth Generation Systems.

1995

Ничего действительно заметного в области DOS-вирусами не произошло, хотя появляется несколько достаточно сложных вирусов-монстров типа «NightFall», «Nostradamus», «Nutcracker» и таких забавных вирусов, как «двуполый» вирус «RMNS» и BAT-вирус «Winstart». Широкое распространение получили вирусы «ByWay» и «DieHard2» - сообщения о зараженных компьютерах были получены практически со всего мира.

Февраль 1995: произошел инцидент с Microsoft: на диске, содержащем демонстрационную версию Windows95, обнаружен вирус «Form». Копии этого диска Microsoft разослал бета-тестерам, один из которых не поленился проверить диск на вирусы.

Весна 1995: аннонсирован альянс двух антивирусных компаний - ESaSS (ThunderBYTE anti-virus) и Norman Data Defence (Norman Virus Control). Эти компании, выпускающие достаточно сильные антивирусы, объединили усилия и приступили к разработке единой антивирусной системы.

Август 1995: один из поворотных моментов в истории вирусов и антивирусов: в «живом виде» обнаружен первый вирус для Microsoft Word («Concept»). Буквально за месяц вирус «облетел» весь земной шар, заполонил компьютеры пользователей MS-Word и прочно занял первое место в статистических исследованиях, проводимых различными компьютерными изданиями.

1996

Январь 1996: два достаточно заметных события - появился первый вирус для Windows95 («Win95.Boza») и эпидемия крайне сложного полиморфик-вируса «Zhengxi» в Санкт-Петербурге.

Март 1996: первая эпидемия вируса для Windows 3.x. Его имя - «Win.Tentacle». Этот вирус заразил компьютерную сеть в госпитале и нескольких других учреждениях во Франции. Интересность этого события состояла в том, что это был ПЕРВЫЙ Windows-вирус, вырвавшийся на свободу. До той поры (насколько мне известно) все Windows-вирусы жили только в коллекциях и электронных журналах вирусописателей, а в «живом виде» встречались только загрузочные, DOS- и Macro-вирусы.

Июнь 1996: «OS2.AEP» - первый вирус для OS/2, корректно заражающий EXE-файлы этой операционной системы. До этого в OS/2 встречались только вирусы, которые записывались вместо файла, уничтожая его или действуя методом «компаньон».

Июль 1996: «Laroux» - первый вирус для Microsoft Excel, к тому же пойманный в «живом виде» (практически одновременно в двух нефтедобывающих компаниях на Аляске и в ЮАР). Как и у MS-Word-вирусов, принцип действия «Laroux» основывается на наличии в файлах так называемых макросов - программ на языке Basic. Такие программы могут быть включены в электронные таблицы Excel так же, как и в документы MS-Word. Как оказалось, встроенный в Excel язык Basic также позволяет создавать вирусы. Этот же вирус в апреле 1997 стал причиной эпидемии в компьютерных фирмах Москвы.

Декабрь 1996: «Win95.Punch» - первый «резидентный» вирус для Win95. Загружается в систему как VxD-драйвер, перехватывает обращения к файлам и заражает их.

В целом год 1996 можно считать началом широкомасштабного наступления компьютерного андеграунда на операционную систему Windows32 (Windows95 и Windows NT) и на приложения Microsoft Office. За этот и следующий год появилось несколько десятков вирусов для Windows95/NT и несколько сотен макро-вирусов. Во многих их них вирусописатели применяли совершенно новые приемы и методы заражения, добавляли стелс- и полиморфик-механизмы и т.п. Таким образом компьютерные вирусы вышли на новый виток своего развития - на уровень 32-битных операционных систем. За два года вирусы для Windows32 повторили примерно все те же стадии, что ровно 10 лет до того прошли DOS-вирусы, однако на совершенно новом технологическом уровне.

1997

Февраль 1997: «Linux.Bliss» - первый вирус для Linux (разновидность юникса). Так вирусы заняли еще одну «биологическую» нишу.

Февраль-апрель 1997: Макро-вирусы перебрались и в Office97. Первые из них оказались всего лишь «отконвертированными» в новый формат макро-вирусами для Word 6/7, однако практически сразу появились вирусы, ориентированные только на документы Office97.

Март 1997: «ShareFun» - макро-вирус, поражающий MS Word 6/7. Для своего размножения использует не только стандартные возможности MS Word, но также рассылает свои копии по электронной почте MS-Mail.

Апрель 1997: «Homer» - первый сетевой вирус-червь, использующий для своего размножения File Transfer Protocol (ftp).

Июнь 1997: Появление первого самошифрующегося вируса для Windows95. Вирус, имеющий российское происхождение, был разослан на несколько BBS в Москве, что стало причиной эпидемии.

Ноябрь 1997: Вирус «Esperanto». Попытка создания (к счастью, неудачная) многоплатформенного вируса, который работает не только под DOS и Windows, но в состоянии заражать и файлы Mac OS (Макинтош).

Декабрь 1997: появилась новая форма вируса - черви mIRC. Оказалось, что наиболее популярная утилита Windows IRC (Internet Relay Chat), известная как mIRC, содержала «дыру», позволяющую вирусным скриптам передавать себя по IRC-каналам. В очередной версии IRC дыра была закрыта, и mIRC-черви канули в лету.

Основным антивирусным событием в 1997 году стало, конечно же, отделение антивирусного подразделения фирмы КАМИ в независимую компанию «Лаборатория Касперского», зарекомендовавшую себя на сегодняшний день как признанный технический лидер антивирусной индустрии. Начиная с 1994 года основной продукт компании - антивирусный сканер AntiViral Toolkit Pro (AVP) - стабильно показывает высокие результаты в многочисленных тестах, проводимых различными тестовыми лабораториями всего мира. Отделение в независимую компанию позволило по началу небольшой группе разработчиков стать первой по значимости антивирусной компанией на отечетсвенном рынке и достаточно заметной фигурой на ринке мировом. За короткие сроки были разработаны и выпущены версии для практически всех популярных платформ, предложены новые антивирусные решения, создана сеть международной дистрибуции и технической поддрежки.

В октябре 1997 года было подписано соглашение о лицензировании технологий AVP финской компанией DataFellows для использования в своей новой разработке FSAV (F-Secure Anti-Virus). До этого компания DataFellows была известна как производитель антивируса F-PROT.

Год 1997 также заметен по нескольким скандалам, разразившимся между основными производителями антивирусов в США и Европе. В начале года фирма McAfee объявила о том, что ее специалисты обнаружили «закладку» в программах одного из своих основных конкурентов - в антивирусе фирмы Dr.Solomon. Заявление от McAfee гласило, что если антивирус Dr.Solomon при сканировании обнаруживает несколько вирусов различных типов, то дальнейшая его работа происходит в усиленном режима. То есть если в обычных условиях на незараженных компьютерах антивирус от Dr.Solomon работает в обычном режиме, то при тестировании коллекций вирусов переключается в усиленный режим (по терминологии McAfee «cheat mode» - «режим обмана»), позволяющий детектировать вирусы, невидимые для Dr.Solomon при сканировании в обычном режиме. В результате при тестировании на незараженных дисках антивирус от Dr.Solomon показывает хорошие скоростные результаты, а при тестировании вирусных коллекций показывает неплохие результаты детектирования.

Через некоторое время Dr.Solomon нанес ответный удар, пришедшийся на некорректно построенную рекламную кампанию McAfee. Конкретно претензии предъявлялись тексту «The Number One Choice Worldwide. No Wonder The Doctor's Left Town». Одновременно с этим компания McAfee вела юридические тяжбы с другой антивирусной компанией Trend Micro по поводу нарушения патента на технологию сканирования данных, передаваемых по Интернет и электронной почте. В этот же конфликт c Trend Micro оказалась втянута фирма Symantec. Затем Symantec предъявил иск McAfee по обвинению в использовании кодов Symantec в продуктах McAfee. Ну и т.д.

Закончился год еще одним заметным событием, связанным с именем McAfee: фирмы McAfee Associates и Network General объявили об объединении в единую компанию Network Assotiates и о позиционировании усилий не только в области антивирусных защит, но и в разработке универсальных систем компьютерной безопасности, шифрования и сетевого администрирования. Начиная с этого момента вирусной и антивирусной истории McAfee следует читать как NAI.

1998

Вирусная атака на MS Windows, MS Office и сетевые приложения не ослабевает. Появляются вирусы, использующие все более сложные приемы заражения компьютеров и новые методы проникновения через компьютерные сети. Помимо вирусов на арену выходят также многочисленные троянские программы, ворующие пароли доступа в Интернет, и несколько утилит скрытого администрирования. Зафиксированы инциденты с зараженными CD-дисками: несколько компьютерных журналов распространяли на своей обложке диски с программами, зараженными Windows-вирусами «CIH» и «Marburg».

Начало года: Эпидемия целого семейства вирусов «Win32.HLLP.DeTroie», не только заражающих выполняемые файлы Windows32, но и способные передать своему «хозяину» информацию о зараженном компьютере. По причине использования специфических библиотек, присутствующих только во французской версии Windows, эпидемия затронула только франко-говорящие страны.

Февраль 1998: обнаружен еще один тип вируса, заражающий таблицы Excel - «Excel4.Paix» (или «Formula.Paix»). Данный тип макро-вируса для своего внедрения в таблицы Excel использует не обычную для вирусов область макросов, а формулы, которые, как оказалось, также могут содержать саморазмножающийся код.

Февраль-март 1998: «Win95.HPS» и «Win95.Marburg» - первые полиморфные Windows32-вирусы, обнаруженные к тому же «в живом виде». Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Март 1998: «AccessiV» - первый вирус для Microsoft Access. Причиной шумихи, как это было с вирусами «Word.Concept» и «Excel.Laroux», он не стал, поскольку все уже привыкли к тому, что приложения MS Office падают одно за другим.

Март 1998: Макро-вирус «Cross» - первый вирус, заражающий два различных приложения MS Office: Access и Word. Следом за ним появились еще несколько макро-вирусов, переносящих свой код из одного Office-проложения в другое.

Май 1998: вирус «RedTeam». Заражает EXE-файлы Windows, рассылает зараженные файлы при помощи электронной почты Eudora.

Июнь: эпидемия вируса «Win95.CIH», ставшая сначала массовой, затем глобальной, а затем повальной - сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии зарегистрировано на Тайване, где неизвестный хакер заслал зараженные файлы в местные Интернет-конференции. Оттуда вирус пробрался в США, где по недосмотру зараженными оказались сразу несколько популярных Web-серверов - они распространяли зараженные вирусом игровые программы. Скорее всего, именно эти зараженные файлы на игровых серверах и послужили причиной повальной эпидемии вируса, не ослабевавшей в течении всего года. По результатам рейтингов «популярности» вирус «подвинул» таких вирусных суперзвезд, как «Word.CAP» и «Excel.Laroux». Следует обратить внимание также на опасное проявление вируса: в зависимости от текущей даты вирус стирал Flash BIOS, что в некоторых случаях могло привести к необходимости замены материнской платы.

Август 1998: появление нашумевшего «BackOrifice» («Backdoor.BO») - утилиты скрытого (хакерского) администрирования удаленных компьютеров и сетей. Следом за «BackOrifice» появились несколько других аналогичных программ: «NetBus», «Phase» и прочие.

Также в августе появился первый вирус, заражающий выполняемые модули Java - «Java.StangeBrew». Данный вирус не представлял какой-либо опасности для пользователей Интернет, поскольку на удаленном компьтере невозможно использовать необходимые для размножения функции. Однако он проиллюстрировал тот факт, что атакованы вирусами также могут быть и приложения, активно используемые при просмотре Web-серверов.

Ноябрь 1998: «VBScript.Rabbit» - интернет-экспансия компьютерных паразитов продолжилась тремя вирусами, заражающими скрипты VisualBasic (VBS-файлы), которые активно применяются при написании Web-страниц. Как логическое следствие VBScript-вирусов стало появление полноценного HTML-вируса («HTML.Internal»). Становится достаточно очевидным, что усилия вирусописателей начинают концентрироваться вокруг сетевых приложений, и дело идет к появлению полноценного сетевого вируса-червя, использующего возможности MS Windows, Office и заражающего удаленные компьютеры, Web-сервера и/или активно распростряняющегося по электронной почте.

Произошли также заметные перестановки в антивирусном мире. В мае 1998 компании Symantec и IBM объявили об объединении своих усилий на антивирусном фронте: совместный продукт при этом распространяется фирмой Symantec под той же маркой Norton Anti-Virus, а IBM Anti-Virus (IBMAV) прекращает свое существование. На это моментально отреагировали основные конкуренты: Dr.Solomon и NAI (ранее - McAfee) тут же выпустили пресс-релизы с предложениями о льготном опдейте бывших пользователей IBMAV своими собственными антивирусами.

Не прошло и месяца, как прекратил свое существование и сам Dr.Solomon. Он был куплен компанией NAI (McAfee) за 640 миллионов долларов путем обмена акций. Данное событие вызвало шок в антивирусном мире: конфликт между двумя крупнейшими игроками антивирусного бизнеса закончился куплей/продажей, в результате которой с рынка исчез один из наиболее заметных и технологически сильных производителей антивирусного программного обеспеечения.

1999

Все на свете должно происходть медленно и неправильно, чтобы не сумел загордиться человек, чтобы человек был грустен и растерян. (Венедикт Ерофеев. «Москва - Петушки»)

# 3. Перспективы: что будет завтра и послезавтра

А что же будет дальше? И как долго вирусы будут нас беспокоить? - вопросы, который в той или иной мере беспокоит практически всех пользователей.

## 3.1. Что будет завтра?

Чего ожидать от компьютерного андеграунда в последующие годы? Скорее всего основными проблемами останутся: 1) полиморфик-DOS-вирусы, к которым добавятся проблемы полиморфизма в макро-вирусах и вирусах для Windows и OS/2; 2) макро-вирусы, которые будут находить все новые и новые приемы заражения и скрытия своего кода в системе; 3) сетевые вирусы, использующие для своего распространения протоколы и команды компьютерных сетей.

Пункт 3) находится пока только на самой ранней стадии - вирусы делают первые робкие попытки самостоятельно распространять свой код по MS Mail и пользуясь ftp, однако все еще впереди.

Не исключено, что появятся и другие проблемы, которые принесут немало неприятностей пользователям и достаточное количество неурочной работы разработчикам антивирусных программ. Однако я смотрю на будущее с оптимизмом: все проблемы, когда-либо встававшие в истории развития вирусов, были довольно успешно решены. Скорее всего так же успешно будут решаться и будущие проблемы, пока еще только витающие идеями в воспаленном разуме вирусописателей.

## 3.2. Что будет послезавтра?

Что будет послезавтра и как долго вообще будут существовать вирусы? Для того, чтобы ответить на этот вопрос следует определить, где и при каких условиях водятся вирусы.

Основная питательная среда для массового распространения вируса в ЭВМ, на мой взгляд, обязана содержать следующие необходимые компоненты:

1. незащищенность операционной системы (ОС);
2. наличие разнообразной и довольно полной документации по OC и «железу»;
3. широкое распространение этой ОС и этого «железа».

Слудует отметить, что понятие операционной системы достаточно растяжимое. Например, для макро-вирусов операционной системой являются редакторы Word и Excel, поскольку именно редакторы, а не Windows предоставляют макро-вирусам (т.е. программам на бейсике) необходимые ресурсы и функции.

Если в операционной системе присутствуют элементы защиты информации, как это сделано практически во всех ОС, вирусу будет крайне трудно поразить объекты своего нападения, так как для этого потребуется (как минимум) взломать систему паролей и привилегий. В результате работа, необходимая для написания вируса, окажется по силам только профессионалам высокого уровня (вирус Морриса для VAX - пример этому). А у профессионалов, на мой взгляд, уровень порядочности все-таки намного выше, чем в среде потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов еще более сократится.

Для массового производства вирусов также необходимо и достаточное количество информации о среде их обитания. Какой процент от числа системных программистов, работающих на мини-ЭВМ в операционках UNIX, VMS и т.д. знает систему управления процессами в оперативной памяти, полные форматы выполняемых файлов и загрузочных записей на диске? (т.е. информацию, необходимую для создания вируса). И следовательно, какой процент от их числа в состоянии вырастить настоящего полноценного зверя? Другой пример - операционная система Novell NetWare, достаточно популярная, но крайне слабо документированная. В результате мне пока не известно ни одного вируса, поразившего выполняемые файлы Novell NetWare, несмотря на многочисленные обещания вирусописателей выпустить такой вирус в ближайшее время.

Ну а по поводу широкого распространения ОС как необходимого условия для вирусного нашествия и говорить надоело: на 1000 программистов только 100 способны написать вирус, на эту сотню приходится один, который эту идею доведет до завершения. Теперь полученную пропорцию умножаем на число тысяч программистов - и получаем результат: с одной стороны 15.000 или даже 20.000 полностью IBM-совместимых вирусов, с другой - несколько сот вирусов для Apple-Macintosh. Такое же несоответствие пропорций наблюдается и в сравнении общего количества вирусов для Windows (несколько десяктов) и для OS/2 (несколько штук).

Приведенным выше трем условиям «расцвета» компьютерных вирусов удовлетворяют сразу несколько OS (включая редакторы), производимых фирмой Microsoft (DOS, Windows, Win95/NT и Word, Excel, Office97), что дает благодатную почву для существования самых разнообразных файловых и макро-вирусов. Удовлетворяют приведенным условиям также и стандарты разбиения жестких дисков. Результат - разнообразные варианты загрузочных вирусов, поражающих систему в момент ее загрузки.

Для того, чтобы прикинуть продолжительность нашествия компьютерных вирусов в какой-либо OC, надо оценить время сосуществования приведенных выше необходимых условий.

Довольно очевидно, что в обозримом будущем фирмы IBM и Apple не собираются уступать массовый рынок своим конкурентам (на радость Apple- и IBM-программистам), даже если для этого этим фирмам придется объединить усилия. Не представляется возможным и усечение потока информации по наиболее распространенным системам, так как это ударит по числу приложений для них, а следовательно, и по их «продаваемости». Остается только одно - защита ОС. Однако, защищенность ОС требует исполнения некоторых правил (паролей и т.п.), что приводит к ряду неудобcтв. Поэтому мне кажется маловероятным, что такие ОС станут популярными в среде обычных пользователей - секретарш, бухгалтеров, на домашних компьютерах, и т.д., и т.п., либо функции защиты будут отлючаться пользователем еще при установке ОС.

Исходя из вышесказанного можно сделать единственный вывод: вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются.

# 4. Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

1. среда обитания;
2. операционная система (OC);
3. особенности алгоритма работы;
4. деструктивные возможности.

По СРЕДЕ ОБИТАНИЯ вирусы можно разделить на:

1. файловые;
2. загрузочные;
3. макро;
4. сетевые.

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые длокументы, но и рассылает свои копии по электронной почте.

Заражаемая ОПЕРАЦИОННАЯ СИСТЕМА (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д. Макро-вирусы заражают файлы форматов Word, Excel, Office97. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ вирусов выделяются следующие пункты:

1. резидентность;
2. использование стелс-алгоритмов;
3. самошифрование и полиморфичность;
4. использование нестандартных приемов.

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

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

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

Использование СТЕЛС-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов OC на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ — запрет вызовов меню просмотра макросов. Один из первых файловых стелс-вирусов — вирус «Frodo», первый загрузочный стелс-вирус — «Brain».

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

Различные НЕСТАНДАРТНЫЕ ПРИЕМЫ часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре OC (как это делает вирус «3APA3A»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ вирусы можно разделить на:

1. безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
2. неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
3. опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
4. очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некотоорых типов винчестеров.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия. Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков (например, вполне безобидный на первый взгляд вирус «DenZuk» довольно корректно работает с 360K дискетами, но может уничтожить информацию на дискетах большего объема). До сих пор попадаются вирусы, определяющие «COM или EXE» не по внутреннему формату файла, а по его расширению. Естественно, что при несовпадении формата и расширения имени файл после заражения оказывается неработоспособным. Возможно также «заклинивание» резидентного вируса и системы при использовании новых версий DOS, при работе в Windows или с другими мощными программными системами. И так далее. Загрузочные вирусы; Макро-вирусы; Полиморфик-вирусы; Прочие «вредные программы»; Резидентные вирусы; Сетевые вирусы; Стелс-вирусы; Файловые вирусы; IRC-черви.

# 5. Методы борьбы с вирусами.

## 5.1. Методы обнаружения и удаления компьютерных вирусов

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

1. Анализ алгоритма вируса
2. Антивирусные программы
3. Восстановление пораженных объектов
4. Обнаружение неизвестного вируса

Профилактика заражения компьютера

## 5.2. DOCTOR WEB – одна из популярнейших антивирусных программ.

В последнее время стремительно растет популярность антивирусной программы Doctor Web. Dr.Web также, как и Aidstest относится к классу детекторов - докторов, но в отличие от последнего имеет так называемый "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. "Лечебная паутина", как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов, которые при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса. Dr.Web можно назвать антивирусом нового поколения по сравнению с Aidstest и его аналогами. В пользу этой программы говорит тот факт, что крупную лицензию ( на 2000 компьютеров) приобрело Главное управление информационных ресурсов при Президенте РФ, а второй по величине покупатель "паутины" - "Инкомбанк".

Управление режимами также как и в Aidtest осуществляется с помощью ключей. Пользователь может указать программе тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. В свою очередь можно тестировать либо только базовую память, либо, вдобавок, ещ\_ и расширенную (указывается с помощью ключа /H ). Как и Aidstest Doctor Web может создавать отчет о работе (ключ /P), загружать знакогенератор Кириллицы (ключ /R ), поддерживает работу с программно-аппаратным комплексом Sheriff ( ключ /Z ).

Но, конечно, главной особенностью "Лечебной паутины" является наличие эвристического анализатора, который подключается ключем /S. Баланса между скоростью и качеством можно добиться, указав ключу уровень эвристического анализа: 0 - минимальный, 1 - оптимальный, 2 - максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr.Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET. Для этого следует указать ключ /U (при этом распаковка файлов будет произведена на текущем устройстве) или /Uдиск: (где диск: - устройство, на котором будет производиться распаковка), если дискета, с которой запущен Doctor Web защищена от записи. Многие программы упакованы таким способом, хотя пользователь может и не подозревать об этом. Если ключ /U не установлен, то Doctor Web может пропустить вирус, забравшийся в запакованную программу.

Важной функцией является контроль заражения тестируемых файлов резидентным вирусом( ключ /V ). При сканировании памяти нет стопроцентной гарантии, что "Лечебная паутина" обнаружит все вирусы, находящиеся там. Так вот, при задании функции /V Dr.Web пытается воспрепятствовать оставшимся резидентным вирусам заразить тестируемые файлы.

Тестирование винчестера Dr.Web-ом занимает на много больше времени, чем Aidstest-ом, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно (с опцией /S2) проверять принесенные извне дискеты. Если информация на дискете находится в архиве (а в последнее время программы и данные переносятся с машины на машину только в таком виде; даже фирмы-производители программного обеспечения, например Borland, пакуют свою продукцию), следует распаковать его в отдельный каталог на жестком диске и сразу же, не откладывая, запустить Dr.Web, задав ему в качестве параметра вместо имени диска полный путь к этому подкаталогу. И все же нужно хотя бы раз в две недели производить полную проверку "винчестера" на вирусы с заданием максимального уровня эвристического анализа.

Так же как и в случае с Aidstest при начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, так как нельзя исключить, что последовательность байт, принятая в антивирусе за шаблон может встретиться в здоровой программе. Если по завершении тестирования Dr.Web выдаст сообщения о том, что нашел вирусы, нужно запустить его с опцией /P (если эта опция не была указана) для того, чтобы посмотреть, какой файл заражен. После этого нужно скопировать файл на дискету или на электронный диск и попытаться удалить, указав "Лечебной паутине" ключ /F. При неудачном лечении следует поступить так же, как в аналогичной ситуации, описаной выше для программы Aidstest.

Для ежедневной работы с дискетами можно посоветовать следующую конфигурацию: web <имя диска>/A/S2/V/O/U/H , где /A - проверять все файлы, /S2 - эвристический анализатор, /V - проверять заражение резидентным вирусом, /O - выводить сообщение OK для незараженных файлов, /U - проверять запакованные ( но не архивированные!) файлы, /H - тестировать верхнюю память.

Чтобы все время не набирать одну и ту же последовательность ключей, можно включить в меню пользователя (USER MENU) оболочки NORTON COMMANDER ( или ДОС-НОВИГАТОР, если используется последняя) пункты вызова Dr.Web и Aidstest, либо создать командный файл. Это не только сэкономит время, но и позволит уменьшить объем переменных окружения DOS, так как теперь не нужно будет указывать в команде PATH файла AUTOEXEC.BAT подкаталог с антивирусными программами (некоторые делают это для оперативного обращения к антивирусам).

# Заключение

При работе с современным персональным компьютером пользователя (а особенно начинающего) может подстерегать множество неприятностей: потеря данных, зависание системы, выход из строя отдельных частей компьютера и другие. Одной из причин этих проблем наряду с ошибками в программном обеспечении) и неумелыми действиями самого оператора ПЭВМ могут быть проникшие в систему компьютерные вирусы. Эти программы подобно биологическим вирусам размножаются, записываясь в системные области диска или приписываясь к файлам и производят различные нежелательные действия, которые , зачастую, имеют катастрофические последствия. Чтобы не стать жертвой этой напасти, каждому пользователю следует хорошо знать принципы защиты от компьютерных вирусов.

С давних времён известно, что к любому яду рано или поздно можно найти противоядие. Таким противоядием в компьютерном мире стали программы, называемые антивирусными. Данные программы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его , а также о других подозрительных действиях (например о попытках изменить установки CMOS). При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний. К преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению как к известным, так и неизвестным вирусам, тогда как детекторы пишутся под конкретные, известные на данный момент программисту виды. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода. Однако, программы-фильтры не могут отслеживать вирусы, обращающиеся непосредственно к BIOS, а также BOOT-вирусы, активизирующиеся ещё до запуска антивируса, в начальной стадии загрузки DOS, К недостаткам также можно отнести частую выдачу запросов на осуществление какой-либо операции: ответы на вопросы отнимают у пользователя много времени и действуют ему на нервы. При установке некоторых антивирусов-фильтров могут возникать конфликты с другими резидентными программами, использующими те же прерывания, которые просто перестают работать.

Наибольшее распространение в нашей стране получили программы-детекторы, а вернее программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса - Aidstest, Doctor Web, MicroSoft AntiVirus далее будут рассмотрены подробнее. Антивирусы-детекторы расчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ. Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов. Ревизоры - программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохранённой ранее в одном из файлов данных ревизора. При этом проверяется состояние BOOT-сектора, таблицы FAT, а также длина файлов, их время создания, атрибуты, контрольная сумма. Анализируя сообщения программы-ревизора, пользователь может решить, чем вызваны изменения: вирусом или нет. При выдаче такого рода сообщений не следует предаваться панике, так как причиной изменений, например, длины программы может быть вовсе и не вирус. Так был случай, когда один начинающий пользователь не на шутку перепугался, когда антивирус AVSP выдал ему сообщение об изменениях в файле CONFIG.SYS. Оказалось, что до этого на компьютер была осуществлена инсталяция менеджера памяти QEMM, который пишет свой драйвер в CONFIG.SYS.

К последней группе относятся самые неэффективные антивирусы - вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зарaженной.

# Список литературы

1. В.Э.Фигурнов "IBM PC для пользователя". Уфа, ПК "Дегтярёв и сын", 1993 г.
2. Ф.Файтс, П.Джонстон, М.Кратц "Компьютерный вирус: проблемы и прогноз". Москва, "Мир", 1993 г.
3. Н.Н.Безруков "Классификация компьютерных вирусов MS-DOS и методы защиты от них". Москва, СП "ICE", 1990 г.
4. Йорг Шиб "MS-DOS 6.22 за 5 минут". Москва, "Бином",1995 г.
5. Газета "Компьютерра" за 26 сентября 1994 г.
6. Документации на антивирусные программы.
7. Собственный опыт.