

Содержание

Введение	12
-----------------------	----

ГЛАВА 1 ❖

Общие сведения о компьютерных вирусах	15
--	----

1.1. Что такое «компьютерный вирус»	15
1.2. Несколько исторических замечаний	17
1.3. Какие бывают вирусы	24
1.3.1. Классификация по способу использования ресурсов	25
1.3.2. Классификация по типу заражаемых объектов	25
1.3.3. Классификация по принципам активации	25
1.3.4. Классификация по способу организации программного кода	26
1.3.5. Классификация вирусов-червей	27
1.3.6. Прочие классификации	27
1.4. О «вредности» и «полезности» вирусов.....	28
1.5. О названиях компьютерных вирусов.....	31
1.6. Кто и зачем пишет вирусы	35
1.6.1. «Самоутверждающиеся»	36
1.6.2. «Честолюбцы»	36
1.6.3. «Игроки»	39
1.6.4. «Хулиганы и вандалы».....	40
1.6.5. «Корыстолюбцы»	40
1.6.6. «Фемида» в борьбе с компьютерными вирусами	42
1.7. Общие сведения о способах борьбы с компьютерными вирусами	45

ГЛАВА 2 ❖

Загрузочные вирусы	49
---------------------------------	----

2.1. Техническая информация.....	49
2.1.1. Загрузка с дискеты.....	53
2.1.2. Загрузка с винчестера	56
2.2. Как устроены загрузочные вирусы	58
2.2.1. Как загрузочные вирусы получают управление	58
2.2.2. Как загрузочные вирусы заражают свои жертвы	59
2.2.3. Как вирусы остаются резидентно в памяти.....	60
2.2.4. Как заподозрить и «изловить» загрузочный вирус	60
2.3. Охотимся за загрузочным вирусом.....	62
2.3.1. Анализ вирусного кода	62
2.3.2. Разработка антивируса	66

4 ❖ Содержание

2.4. Редко встречающиеся особенности	70
2.4.1. Зашифрованные вирусы	70
2.4.2. Вирусы, не сохраняющие оригинальных загрузчиков	72
2.4.3. Механизмы противодействия удалению вирусов.....	74
2.4.4. Проявления загрузочных вирусов.....	77
2.4.5. Загрузочные вирусы и Windows.....	79
2.4.6. Буткиты.....	82
2.5. Советы по борьбе с загрузочными вирусами.....	85
2.5.1. Методы защиты дисков от заражения	86
2.5.2. Удаление загрузочных вирусов и буткитов «вручную»	87

ГЛАВА 3 ❖

Файловые вирусы в MS-DOS.....	89
3.1. Вирусы-«спутники»	89
3.2. «Оверлейные» вирусы.....	94
3.3. Вирусы, заражающие СОМ-программы	98
3.3.1. Внедрение в файл «жертвы»	98
3.3.2. Возврат управления «жертве»	102
3.4. Вирусы, заражающие EXE-программы	105
3.4.1. «Стандартный» метод заражения	107
3.4.2. Заражение в середину файла	109
3.4.3. Заражение в начало файла	110
3.5. Нерезидентные вирусы	111
3.5.1. Метод предопределенного местоположения файлов	112
3.5.2. Метод поиска в текущем каталоге	113
3.5.3. Метод рекурсивного обхода дерева каталогов	118
3.5.4. Метод поиска по «тропе»	119
3.6. Резидентные вирусы	122
3.6.1. Схема распределения памяти в MS-DOS	122
3.6.2. Способы выделения вирусом фрагмента памяти	126
3.6.3. Обработка прерываний	130
3.6.3.1. Перехват запуска программы	131
3.6.3.2. Перехват файловых операций	134
3.6.3.3. Перехват операций с каталогами	136
3.7. Вирусы-«невидимки»	137
3.7.1. «Психологическая» невидимость	140
3.7.2. Прямое обращение к системе	143
3.7.2.1. Метод предопределенных адресов	144
3.7.2.2. Метод трассировки прерывания	145
3.7.2.3. Прочие методы	149
3.7.3. Использование SFT	151

3.8. Зашифрованные и полиморфные вирусы	154
3.8.1. Зашифрованные и полиморфные вирусы для MS-DOS	155
3.8.2. Полиморфные технологии	168
3.9. Необычные файловые вирусы для MS-DOS.....	170
3.9.1. «Не-вирус» Eiscar	171
3.9.2. «Двуполюый» вирус	172
3.9.3. Файлово-загрузочные вирусы	173
3.9.4. Вирусы-«драйверы»	174
3.9.5. Вирусы с «неизвестной» точкой входа	175
3.9.6. Самый маленький вирус	176
3.10. Подробный пример обнаружения, анализа и удаления	179
3.10.1. Способы обнаружения и выделения вируса в чистом виде	179
3.10.2. Анализ вирусного кода	180
3.10.3. Пишем антивирус.....	183
3.11. MS-DOS-вирусы в эпоху Windows.....	184

ГЛАВА 4 ❖

Файловые вирусы в Windows.....

4.1. Системная организация Windows	186
4.1.1. Особенности адресации	187
4.1.1.1. Сегментная организация адресного пространства	188
4.1.1.2. Страничная организация адресного пространства	191
4.1.2. Механизмы защиты памяти	192
4.1.3. Обработка прерываний и исключений	193
4.1.4. Механизмы поддержки многозадачности	198
4.1.5. Распределение оперативной памяти	199
4.1.6. Файловые системы	203
4.1.7. Запросы прикладных программ к операционной системе	204
4.1.7.1. Системные сервисы в MS-DOS	204
4.1.7.2. Системные сервисы в Windows 3.X	205
4.1.7.3. Системные сервисы в Windows 9X	207
4.1.7.4. Системные сервисы в Windows NT	208
4.1.8. Конфигурирование операционной системы	209
4.1.8.1. Конфигурационные файлы Windows 3.X	209
4.1.8.2. Конфигурационные файлы и структуры Windows 9X	210
4.1.8.3. Конфигурационные файлы и структуры Windows NT	212
4.1.9. Исполняемые файлы Windows	213
4.2. Вирусы для 16-разрядных версий Windows	216
4.2.1. Формат файла NE-программы	217
4.2.1.1. Таблица описания сегментов	218
4.2.1.2. Таблица описания перемещаемых ссылок	219

4.2.1.3. Таблицы описания импорта	221
4.2.2. Организация вирусов для Windows 3X	221
4.2.3. Анализ конкретного вируса и разработка антивирусных процедур	225
4.3. Вирусы для 32-разрядных версий Windows	227
4.3.1. Формат файлов PE-программ	229
4.3.1.1. PE-программы на диске и в памяти	231
4.3.1.2. Таблица секций	234
4.3.1.3. Импорт объектов	236
4.3.1.4. Экспорт объектов	241
4.3.2. Где располагаются вирусы	243
4.3.2.1. Файловые «черви»	243
4.3.2.2. Вирусы-«спутники»	244
4.3.2.3. «Оверлейные» вирусы	245
4.3.2.4. Вирусы в расширенной последней секции	245
4.3.2.5. Вирусы в дополнительной секции	246
4.3.2.6. Вирусы, распределенные по секциям	247
4.3.2.7. Вирусы в файловых потоках NTFS	249
4.3.3. Как вирусы получают управление.....	250
4.3.3.1. Изменение адреса точки входа	250
4.3.3.2. Изменение кода в точке входа	251
4.3.3.3. Использование технологии EPO	251
4.3.4. Как вирусы обращаются к системным сервисам	252
4.3.4.1. Метод предопределенных адресов	253
4.3.4.2. Самостоятельный поиск адреса KERNEL32.DLL	258
4.3.4.3. Использование «нестандартных» сервисов	260
4.3.5. Нерезидентные вирусы	264
4.3.6. «Резиденты» 3-го кольца защиты	265
4.3.6.1. Вирусы – автономные процессы	266
4.3.6.2. «Полурезидентные» вирусы	266
4.3.6.3. Вирусы, заражающие стандартные компоненты Windows	266
4.3.6.4. Вирусы, анализирующие список процессов	268
4.3.7. «Резиденты» 0-го кольца защиты	269
4.3.7.1. Переход в 0-е кольцо защиты методом создания собственных шлюзов	269
4.3.7.2. Переход в 0-е кольцо защиты подменой обработчика исключений	270
4.3.7.3. Инсталляция в неиспользуемые буферы VMM	272
4.3.7.4. Инсталляция в динамически выделяемую системную память	273

4.3.7.5. Встраивание в файловую систему	274
4.3.8. Вирусы – виртуальные драйверы	278
4.3.8.1. VxD-вирусы	279
4.3.8.2. SYS-вирусы и WDM-вирусы	282
4.3.9. «Невидимость» Windows-вирусов	286
4.3.9.1. Маскировка присутствия в файле	287
4.3.9.2. Маскировка присутствия в памяти	289
4.3.9.3. Маскировка ключей Реестра	296
4.3.10. Полиморфные вирусы в Windows	296
4.3.11. Вирусы и подсистема безопасности Windows	301
4.4. Пример анализа и нейтрализации конкретного вируса	305
4.4.1. Первичный анализ зараженных программ	305
4.4.2. Анализ кода	307
4.4.3. Алгоритм поиска и лечения	307
4.4.4. Дополнительные замечания	308

ГЛАВА 5 ❖

Макровирусы	310
5.1. Вирусы в MS Word	310
5.1.1. Общие сведения о макросах	313
5.1.2. Вирусы на языке WordBasic	315
5.1.2.1. Проблема «локализации»	322
5.1.2.2. Активация без «автоматических макросов»	323
5.1.2.3. Копирование макросов без «MacroCopy»	324
5.1.2.4. Запуск бинарного кода	324
5.1.2.5. Обеспечение «невидимости»	325
5.1.3. Вирусы на языке VBA	326
5.1.4. О проявлениях макровирусов	333
5.1.5. Простейшие приемы защиты от макровирусов	336
5.1.5.1. Манипуляции с «NORMAL.DOT»	336
5.1.5.2. Удаление вируса средствами «Организатора»	336
5.1.5.3. Антивирусные макросы	337
5.1.5.4. Встроенная «защита» MS Word	339
5.2. Вирусы в других приложениях MS Office	342
5.2.1. Макровирусы в MS Excel	342
5.2.2. «Многоплатформенные» макровирусы	344
5.3. Полиморфные макровирусы	346
5.4. Прямой доступ к макросам	349
5.4.1. Формат структурированного хранилища	350
5.4.2. «Правильный» доступ к структурированному хранилищу	357
5.4.3. Макросы в Word-документе	358

5.4.3.1. Макросы на языке WordBasic	358
5.4.3.2. Макросы на языке VBA	361
5.4.3.3. Вид и расположение VBA-макросов	362
5.4.3.4. Поиск VBA-макросов	363
5.4.3.5. Распаковка VBA-текста макросов	364
5.4.3.6. Удаление VBA-макросов	366
5.5. Пример анализа и удаления конкретного макровируса	367
5.5.1. Получение и анализ исходного текста	367
5.5.2. Распознавание и удаление макровируса	370

ГЛАВА 6 ❖

Сетевые и почтовые вирусы и черви	371
6.1. Краткая история сетей и сетевой «заразы»	371
6.2. Архитектура современных сетей	375
6.2.1. Топология сетей	375
6.2.2. Семиуровневая модель ISO OSI	377
6.2.3. IP-адресация	378
6.2.4. Символические имена доменов	380
6.2.5. Клиенты и серверы. Порты	382
6.2.6. Сетевое программирование. Интерфейс сокетов	384
6.3. Типовые структура и поведение программы-червя	386
6.4. Как вирусы и черви распространяются	391
6.4.1. Черви в локальных сетях	392
6.4.2. Почтовые вирусы	398
6.4.2.1. Первые почтовые вирусы. Интерфейс MAPI	401
6.4.2.2. Прямая работа с почтовыми серверами	408
6.4.3. «Интернет»-черви	414
6.5. Как черви проникают в компьютер	417
6.5.1. «Социальная инженерия»	423
6.5.2. Ошибки при обработке почтовых вложений	427
6.5.3. Ошибки в процессах SVCHOST и LSASS	429
6.5.4. Прочие «дыры»	435
6.5.5. Брандмауэры	438
6.6. Как черви заражают компьютер	442
6.7. Пример обнаружения, исследования и удаления червя	445
6.7.1. Проявления червя	445
6.7.2. Анализ алгоритма работы	448
6.7.2.1. Установка в памяти	448
6.7.2.2. Борьба с антивирусами	449
6.7.2.3. Модификация Реестра	451
6.7.2.4. Поиск адресов	451

6.7.2.5. Распространение по электронной почте	451
6.7.3. Методы удаления	452
6.8. Современные сетевые вирусы и черви.....	454
6.8.1. Модульное построение	456
6.8.2. Множественность способов распространения	457
6.8.3. Борьба червей с антивирусами	458
6.8.4. Управляемость. Ботнеты.....	458

ГЛАВА 7 ❖

Философские и математические аспекты	461
7.1. Строгое определение вируса	461
7.1.1. Модели Ф. Коэна	462
7.1.2. Модель Л. Адлемана	469
7.1.3. «Французская» модель	472
7.1.4. Прочие формальные модели	475
7.1.4.1. Модель китайских авторов Z. Zuo и M. Zhou	475
7.1.4.2. Векторная модель Д. Зегжды	475
7.1.4.3. Модели на основе абстрактных «вычислителей»	476
7.2. «Экзотические» вирусы	478
7.2.1. Мифические вирусы	479
7.2.2. Batch-вирусы	482
7.2.3. Вирусы в исходных текстах	486
7.2.4. Графические вирусы	490
7.2.5. Вирусы в иных операционных системах	492
7.2.5.1. Вирусы в UNIX-подобных системах	492
7.2.5.2. Вирусы для мобильных телефонов.....	501
7.2.6. Прочая вирусная «экзотика»	506
7.3. Распространение вирусов.....	508
7.3.1. Эпидемии сетевых червей	508
7.3.1.1. Простая SI-модель экспоненциального размножения	510
7.3.1.2. SI-модель размножения в условиях ограниченности ресурсов	514
7.3.1.3. SIS-модель примитивного противодействия	516
7.3.1.4. SIR-модель квалифицированной борьбы	517
7.3.1.5. Прочие модели эпидемий	519
7.3.1.6. Моделирование мер пассивного противодействия	521
7.3.1.7. Моделирование «контрчервя»	522
7.3.2. Эпидемии почтовых червей, файловых и загрузочных вирусов	527
7.3.3. Эпидемии мобильных червей	530
7.4. Обнаружение вирусов	532

7.4.1. Анализ косвенных признаков	533
7.4.2. Простые сигнатуры	535
7.4.3. Контрольные суммы	541
7.4.4. Вопросы эффективности	544
7.4.4.1. Выбор файловых позиций	545
7.4.4.2. Фильтр Блума	547
7.4.4.3. Метод половинного деления	548
7.4.4.4. Разбиение на страницы	549
7.4.5. Использование сигнатур для детектирования полиморфиков	551
7.4.5.1. Аппаратная трассировка	552
7.4.5.2. Эмуляция программ	556
7.4.5.3. Противодействие эмуляции	560
7.4.5.4. «Глубина» трассировки и эмуляции	563
7.4.6. «Рентгеноскопия» полиморфных вирусов	564
7.4.7. Метаморфные вирусы и их детектирование	567
7.4.7.1. Этап «выделения и сбора характеристик»	569
7.4.7.2. Этап «обработки и анализа»	571
7.4.8. Анализ статистических закономерностей.....	578
7.4.9. Эвристические методы детектирования вирусов	580
7.4.9.1. Выделение характерных признаков	582
7.4.9.2. Логические методы	586
7.4.9.3. Синтаксические методы	588
7.4.9.4. Методы на основе формулы Байеса	588
7.4.9.5. Методы, использующие искусственные нейронные сети	590
7.4.10. Концепция современного антивирусного детектора	592
7.5. Борьба с вирусами без использования антивирусов	596
7.5.1. Файловые «ревизоры»	596
7.5.2. Политики разграничения доступа	597
7.5.3. Криптографические методы	601
7.5.4. Гарвардская архитектура ЭВМ	604
7.6. Перспективы развития и использования компьютерных вирусов.....	605
7.6.1. Вирусы как «кибероружие»	606
7.6.2. Полезные применения вирусов	613
ЗАКЛЮЧЕНИЕ	623
Литература	625
ПРИЛОЖЕНИЕ ❖	
Листинги вирусов и антивирусных процедур	630

1. Листинги компьютерных вирусов.....	630
1.1. Листинг загрузочного вируса Stoned.AntiExe	630
1.2. Листинг вируса Eddie, заражающего программы MS-DOS.....	634
1.3. Листинг вируса Win16.Wintiny.b, заражающего NE-программы	637
1.4. Листинг вируса Win32.Varum.1536, заражающего PE-программы	639
2. Исходные тексты антивирусных процедур	641
2.1. Процедуры рекурсивного сканирования каталогов	641
2.2. Процедуры детектирования и лечения вируса Boot.AntiExe.....	642
2.3. Процедуры детектирования и лечения вируса Eddie.651.a.....	642
2.4. Процедуры детектирования и лечения вируса Win.Wintiny.b.....	644
2.5. Процедуры детектирования и лечения вируса Win32.Varum.1536	645
2.6. Процедуры детектирования и лечения вирусов Macro.Word.Wazzu.gw и Macro.Word97.Wazzu.gw	646
2.7. Скрипт антивируса AVZ для детектирования и лечения почтового червя E-Worm.Avrton.a	651
Предметный указатель.....	653

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

А. и Б. Стругацкие. «Обитаемый остров»

Введение

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

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

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

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

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

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

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

Нужна ли такая книга? Представляется, что просто необходима.

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

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

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

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

Наконец, изучать мир компьютерных вирусов просто очень интересно!

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

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

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

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

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

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

ГЛАВА 1

Общие сведения о компьютерных вирусах

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

Что же представляют собой компьютерные вирусы на самом деле?

1.1. Что такое «компьютерный вирус»

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

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

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

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

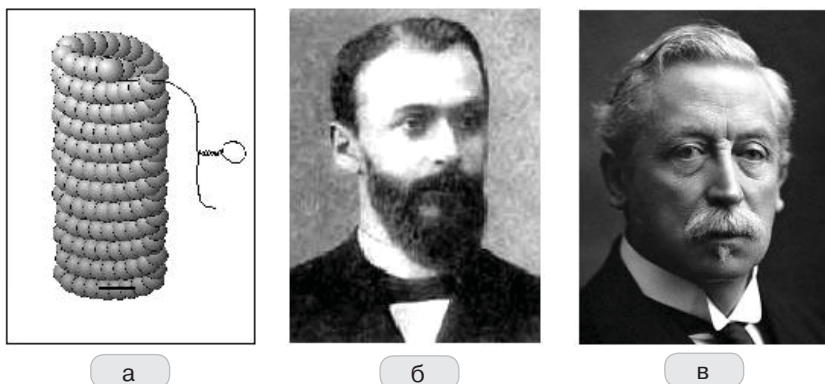


Рис. 1.1 ❖ «Настоящий» вирус и его первооткрыватели:
а) вирус «табачной мозаики»; б) Д. И. Ивановский; в) М. Бейеринг

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

Итак, компьютерный вирус – это:

программа, способная к несанкционированному созданию своих функционально идентичных копий.

В данном определении рассмотрим подробнее три ключевых понятия.

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

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

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

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

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

Класс троянских программ нами рассматриваться не будет.

1.2. Несколько исторических замечаний

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

А. и Б. Стругацкие. «Хромая судьба»

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

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

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

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

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

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

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

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

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

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

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

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

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

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

К 1990 г. во всем мире было создано всего около сотни вирусов, причем каждый новый распространялся практически беспрепятственно, вызывая более или менее широкую эпидемию. Связано это было прежде всего с недостаточной информированностью пользователей и неразвитостью средств антивирусной защиты. Но вскоре ситуация изменилась. С одной стороны, пользователи наконец-то поняли опасность бесконтрольного распространения вирусов, многие из которых содержали вредоносные фрагменты. С другой – начала набирать обороты индустрия антивирусного программного обеспечения. В нашей стране активно использовалась условно-бесплатная антивирусная программа AidsTest Д. Н. Лозинского, несколько менее популярен был пакет «Доктор Касперский» Е. В. Касперского. За рубежом лидировали комплект Scan/Clean от John McAfee, Findvirus от Alan Solomon и Norton Antivirus от Peter Norton Computing (впоследствии эта торговая марка стала собственностью фирмы Symantec). Впрочем, последний антивирус мог и «не родиться», поскольку буквально парой лет ранее, в конце 1980-х годов, Питер Нортон публично и громогласно заявлял о мифичности вирусной угрозы и сравнивал ее с угрозой крокодилов, живущих в нью-йоркской канализации. Но, к счастью, быстро сообразил «что почем» и благословил развитие антивируса, названного его именем¹.

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

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

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

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

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

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

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

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru