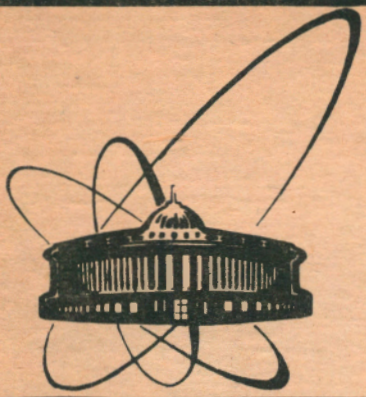

сообщения
объединенного
института
ядерных
исследований
дубна

Р11-90-313

М.В.Чижов

ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

1990

В последнее время среди программных продуктов всё чаще стали встречаться программы, "заражённые" компьютерным вирусом. При вызове этих программ они, в свою очередь, могут заражать другие программы и, таким образом, вирус может распространяться очень быстро. Среди большого разнообразия существующих вирусов встречаются как безобидные, так и очень опасные вирусы, способные испортить или уничтожить огромное количество информации на гибких и жёстких дисках.

Вирусы распространяются путём присоединения к выполнимым модулям программ в .COM, .EXE, .OVL или .SYS файлах. Они изменяют точку входа в оригинальной программе на начало своей процедуры и после её выполнения передают управление оригинальной программе. Явным признаком заражения этих файлов является увеличение их длин.

В настоящий момент написано уже много различных программ, обеспечивающих обнаружение и, в некоторых случаях, удаление известных вирусов, а также резидентных программ, осуществляющих контроль за их распространением. К сожалению, число вирусов с каждым годом непрерывно увеличивается. Они становятся всё более изощрёнными и обходят уже известные защиты. Более того, существует довольно широкий класс вирусов, которые размещаются в Boot Record'е и загружаются в оперативную память раньше всех программ, в том числе и программ, осуществляющих защиту.

На наш взгляд, это наиболее опасные вирусы, так как они получают доступ ко всем ресурсам компьютера ещё до загрузки системных и прикладных программ. Эти вирусы размещаются в системных областях диска и не всегда можно определить,

является ли их содержимое оригинальным или содержит тело процедуры вируса.

Наиболее прямой и эффективный способ защиты от этих вирусов заключается в инсталляции защитной программы ещё на уровне BIOS'а. Для этого необходимо данную программу оформить как его расширение. В соответствии со стандартом IBM PC /1/ расширение BIOS'а может быть размещено в пределах 1 Мбайта выше адреса C0000, не перекрывая другие расширения и сам BIOS. Оно определяется по двум первым байтам: 055h и 0AAh. Затем следует байт, указывающий длину модуля расширения в блоках по 512 байт. Программа инициализации расширения должна начинаться сразу же после этого заголовка и заканчиваться внешним возвратом для передачи управления программе BIOS'а. Сумма байтов расширения по модулю 256 должна равняться нулю.

В данном конкретном случае защиты Boot Record'а жёсткого диска от заражения необходимо инсталлировать программу, которая запретит запись в интересующую нас область диска. Структура программы довольно проста и полностью аналогична расширению BIOS'а жёсткого диска для IBM PC-XT. Она состоит из двух частей: программы инициализации и программы обработки прерываний. Первая программа перенаправляет вектор прерывания функций BIOS'а, связанный с дисковыми операциями, на вторую программу обработки прерываний и устанавливает для этих операций новый вектор прерываний. Вторая программа обеспечивает защиту при попытке записи в Boot Record. Её блок-схема имеет вид

Затем после инсталляции данной программы можно использовать разнообразные программы защиты для предохранения от вирусов областей диска с File Allocation Table, системными и пользовательскими программами. Поэтому её использование будет эффективно предохранять компьютер лишь в сочетании с другими программами защиты от не менее опасных вирусов других типов.

Для того чтобы физически инсталлировать расширение BIOS'а в компьютер, необходимы либо свободные панельки под постоянную память на системной плате, либо дополнительная плата с декодировщиком адреса и постоянной памятью. В постоянную память заносится выполнимый код программы защиты в соответствии с описанным выше стандартом.

В персональном компьютере "Правец-16" имеются шесть панелек под микросхемы постоянной памяти ёмкостью 8 Кбайт каждая с начальными адресами F4000h, F6000h, F8000h, FA000h, FC000h и FE000h. Микросхема, располагающаяся с начального адреса F4000h, играет роль расширения BIOS'а для клавиатурного драйвера, выполненного, однако, без учета вышеописанного стандарта и по сути являющегося непосредственным продолжением BIOS'а. Таким образом, BIOS, занимающий самые старшие адреса, не может функционировать один без данного "расширения". Остальные места занимают микросхемы с кассетным БЕЙСИКом. Автором была выполнена модификация BIOS'а /2/, в результате которой освободилось место с начальным адресом F4000h. Именно это место используется под расширение BIOS'а с программой защиты Boot Record'а от вирусов.

Для тех компьютеров, которые не имеют свободных панелек под расширение BIOS'а, была разработана и изготовлена небольшая плата. Она содержит лишь две микросхемы с матрицами постоянной памяти, одна из которых является дешифратором адреса, а другая содержит программу защиты. Это самый минимальный набор дешёвых микросхем, которые требуются для поддержки данной функции. В качестве дешифратора используется микросхема P556PT11 либо с открытым коллектором - P556PT4. Собственно для расширения BIOS'а выбрана дешёвая микросхема P556PT17 или с открытым коллектором - P556PT5, которая

содержит 512 байт памяти. Для микросхем с открытыми коллекторами на плате предусмотрены контакты для коллекторных резисторов на выходные линии. С помощью перемычки возможен выбор одного из четырёх начальных адресов инсталляции расширения BIOS'а: C8000h, D0000h, D8000h и E0000h. Это необходимо для бесконфликтной инсталляции платы в персональный компьютер. Данная плата может быть установлена в любой свободный разъём на IBM-совместимом персональном компьютере.

Эта простая программа или её модификации могут более надёжно защитить ваш компьютер от всевозможных вирусов, распространяющихся через Boot Record, чем существующие известные сложные системы защиты. Их известность и распространённость не способствуют сохранению тайны защиты. Поэтому борьба с большим разнообразием вирусов будет эффективной лишь в том случае, если использовать против них также большое число простых программ защиты.

В заключение автор благодарит начальника группы ремонта малых ЭВМ В.А.Карамышева за предоставленную возможность использовать материальную базу группы, помощь и поддержку в работе.

ЛИТЕРАТУРА

1. Technical Reference for the IBM Personal Computer XT Part Number 6936763.
2. М.В.Чижов. Модификация основной системы ввода-вывода (BIOS) ПЭВМ "Правец-16", рацпредложение ОИЯИ 128-ОКИП,1989.

Рукопись поступила в издательский отдел
4 мая 1990 года.

Чижов М.В. Р11-90-313

Защита от компьютерных вирусов

Предложена защита от вирусов в Boot Record'е. Специально для ПК "Правец-16" с модифицированным BIOSом и компьютеров, имеющих свободные панельки под его расширение, запрограммирован чип, осуществляющий эту защиту. Сделана небольшая плата, выполняющая такую же защитную функцию для любого IBM-совместимого компьютера. Данная разработка обеспечивает более надежную защиту от вирусов этого типа, чем существующие программные продукты.

Работа выполнена в Лаборатории теоретической физики ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна 1990

Перевод автора

Chizhov M.V. P11-90-313

Protection of Your Computer from Viruses

A virus protection for Boot Record is proposed. First: an EPROM, providing a protection for PC "Pravetz-16" with modified BIOS and for personal computers with free sockets for additional ROM modules, is programmed. Second: a small-sized card providing the virus protection for all IBM compatible computers is made. These devices assure a safer protection from Boot Record viruses than the existing program products.

The investigation has been performed at the Laboratory of Theoretical Physics, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna 1990