

М.ПРОКУДИН,
626440, Тюменская обл.,
г. Нижневартовск-5,
ул. 60 лет Октября, 88 — 59.

ИЗУЧАЕМ “ЗАЩИЩЕННЫЕ” ПРОГРАММЫ

Хочу поделиться с читателями “РЛ” методикой снятия двух типов защиты от копирования с программ в формате ROM для ПК “Вектор-06Ц”. Для этого необходимы программы COPY V2.1 и монитор-отладчик V2.5 (они продавались вместе с ПК), а также необходимо, чтобы в ПЗУ начального загрузчика была штатная прошивка считывания программ в формате ROM. При разработке метода я исходил из того, что все программы располагаются в области памяти, начиная с адреса 0000 до адреса 7FFF.

Необходимо только вытащить данные из памяти, не сбрасывая программу в работу.

Наиболее просто снимается защита с программ, не изменяющих формат первоначальной загрузки. Для программ, начинающихся с первого блока, необходимо выполнить следующие операции:

1. Загрузить монитор-отладчик V2.5 (M-O);
2. Сбросить в работу в режиме 1;
3. Нажать кнопку УС и, не отпуская ее, кнопки ВВОД, БЛК;
4. Загрузить программу, с которой необходимо снять защиту;
5. Нажать УС и, не отпуская, БЛК, СБР;
6. Вывести на магнитную ленту (МЛ) в формате ROM программу директивой O>1,NN,0, где NN — число блоков в программе (блок — 256 байт).

Немного сложнее снимается защита с программ, начинающихся с нулевого блока. Для этого необходимо выполнить следующие операции:

1. Загрузить M-O;
2. Сбросить в работу в режиме 1;
3. Вывести на МЛ блоки в формате ROM директивами:
 - а) O>0,1,0;
 - б) O>94,0C,0;
 - в) O>E0,20,0;
4. Нажать УС и, не отпуская, ВВОД, БЛК;
5. Загрузить программу, с которой необходимо снять защиту;
6. Нажать УС и, не отпуская, ВВОД, БЛК;
7. Загрузить нулевой блок M-O (пункт 3а);
8. Нажать УС и, не отпуская, БЛК, СБР;
9. Вывести на МЛ в формате MON программу с адреса 0100 и по конечный адрес (NNNN) программы со смещением 0100 директивой W 0100,NNNN,0100;
10. Нажать кнопки ВВОД и БЛК;
11. Загрузить COPY V2.1;
12. Сбросить в работу;
13. Начать копировать программу (пункт 5);
14. После считывания трех-четырех блоков нажать кнопку УС и, не отпуская ее, кнопки ВВОД, БЛК;
15. Загрузить программу пункт 3а;
16. Нажать УС и, не отпуская, ВВОД, БЛК;
17. Загрузить программу пункт 3б;
18. Нажать УС и, не отпуская, ВВОД, БЛК.;
19. Загрузить программу пункт 3в;
20. Нажать УС и, не отпуская, БЛК,СБР;
21. Переместить область памяти с адреса 0800 по адрес 08FF директивой M 0800,08FF,0100.
22. Считать программу пункт 9 директивой RW;

23. Вывести на МЛ программу в формате ROM директивой O>1,NN,FF, где NN — число блоков в программе.

Сложнее снимается защита с программ, которые изменяют формат первоначального загрузчика, например, программы фирмы “COMAN”.

Необходимо выполнить следующие операции:

1. Загрузить программу, с которой необходимо снять защиту, не сбрасывая ее в работу;
2. Нажать УС и, не отпуская, ВВОД, БЛК;
3. Загрузить программу, пункт 3а (см. выше);
4. Нажать УС и, не отпуская, ВВОД, БЛК;
5. Загрузить программу, пункт 3б (см. выше);
6. Нажать УС и, не отпуская, ВВОД, БЛК;
7. Загрузить программу, пункт 3а (см. выше);
8. Нажать УС и, не отпуская, БЛК, СБР;
9. Записать программу на МЛ в формате MON с адреса 0100 и по конечный адрес (NNNN) со смещением 0100 директивой W 0100,NNNN,0100;
10. Нажать ВВОД, БЛК;
11. Загрузить M-O.
12. Набрать программу:


```
7F00 01 00 01 11 FF 00 2100
7F08 00 7F 02 03 23 7B 957A
7F10 9C D2 09 7F C3 14 7F00
```
13. Записать программу на МЛ директивой O>1, 7F, 0;
14. Нажать ВВОД, БЛК;
15. Записать программу, с которой снимаем защиту, не сбрасывая ее в работу;
16. Нажать УС и, не отпуская, ВВОД, БЛК;
17. Загрузить программу, пункт 13;
18. Нажать УС и, не отпуская, БЛК, СБР;
19. Нажать УС и, не отпуская, ВВОД, БЛК;
20. Загрузить программу, пункт 3а (см. выше);
21. Нажать УС и, не отпуская, ВВОД, БЛК;
22. Загрузить программу, пункт 3б (см. выше);
23. Нажать УС и, не отпуская, ВВОД, БЛК;
24. Загрузить программу, пункт 3в (см. выше);
25. Нажать УС и, не отпуская, БЛК, СБР;
26. Загрузить программу, пункт 9 директивой RW;
27. Вывести на МЛ программу в формате ROM директивой O>1, NN, FF, где NN — число блоков в программе.

В некоторых программах фирмы “COMAN” необходимо перед выполнением пункта 27 в нулевых адресах программы дописать 3 байта для организации стека с адреса 7FFF (31 FF 7F), т.к. у этих программ организация стека происходит в измененном загрузчике.

После выполнения всех этих операций записанные программы будут копироваться любым COPY.

Гонорар прошу перевести в фонд развития журнала.

ПОПРАВКА

В программе “Программатор для ZX-SPECTRUM”, “РЛ”, N2, 93г. имеются неточности. В строке 2 пропущена закрывающая кавычка, в строке 5030 — знак возведения в степень ↑. Правильная запись:
2 POKE 23658,8: CLEAR 31999: INK 5: PAPER 0: BORDER 0: CLS:
LOAD “” CODE 32000
5030 LET t=t+16↑(4-y)*(CODEw\$(y)-48-7*(CODEw\$(y)>57)).

- Огромный выбор программ для “Спектр”, “Радио-86РК”, “Электроника БК-0010”, “Вектор”, “Орион-128”. Куплю интересные программы. 671205, Кабанский р-н, Каменск, Рабочая, 67.
- Вышло наложенным платежом радиодетали 6П45С, УН8,5/1,2, К174ПС1, ТВС90ЛЦБ, САТТ-Г, САТТ-Ш, конденсаторы К50-6, К50-35, КТ369А, КТ363АМ и др. Отвечу на письмо с вложенным конвертом. 210027, г.Витебск, а/я 38, Андреев П.И.
- Куплю новый или б/у принтер, но не ранее 91г. выпуска. Оплата 5 — 6 тыс. в зависимости от типа принтера. 454138, г.Челябинск, Комсомольский пр-т, 78 А — 205, Бровкин Д.И.