6. АТАКИ СИСТЕМЫ СНАРУЖИ

6.1 ВИРУСЫ

6.1.1 Понятие вируса

Вирус — это программа, которая может размножаться, присоединяя свой код к другой программе

География развития «вирусописательства»

- США, Европа — начало 80-х гг.;
- Болгария, Индия — середина 80-х гг.;
- Россия (тогда ещё СССР) — конец 80-х гг.;
- Китай, Тайвань, другие страны Азии — начало и середина 90-х гг.

Классификация вирусов

- по способу размножения;
- по способу действия;
- по уровню наносимого вреда.

6.1.2 Сценарии нанесения ущерба вирусами

Вы действительно хотите форматировать жесткий диск?

OK

ПРИВЕТ ОТ КОМПАНИИ GENERAL SHULER!

ДЛЯ ПРИОБРЕТЕНИЯ КЛЮЧА ДЕШИФРАЦИИ К ВАШЕМУ ЖЕСТКОМУ ДИСКУ, ПОЖАЛУЙСТА. ВЫШЛИТЕ $100 В МЕЛКИХ НЕМАРКИРОВАННЫХ КУПЮРАХ НА А/Я 2154. ПАНАМА-СИТИ. ПАНАМА. СПАСИБО. МЫ РАДЫ СОТРУДНИЧАТЬ С ВАМИ.

```
main( ) {while (1) fork( );}
```

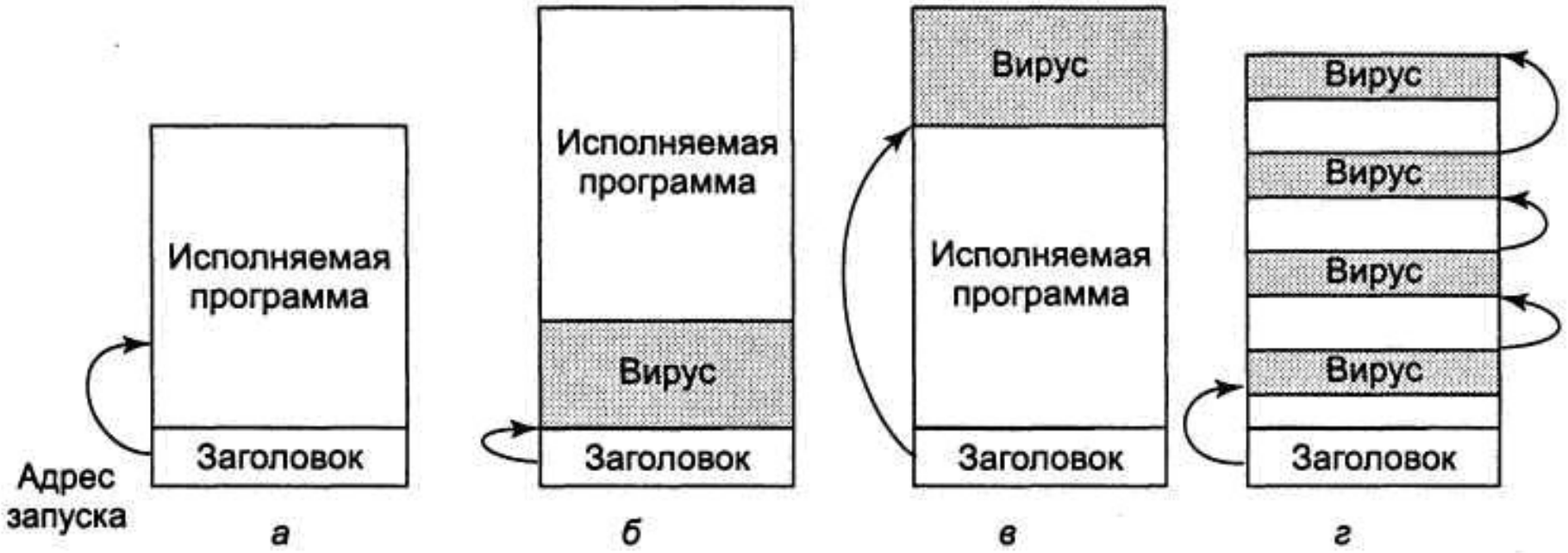
6.1.3 Вирусы-компаньоны

6.1.4 Вирусы, заражающие исполняемые файлы

Рекурсивная процедура, ищущая исполняемые файлы в системе UNIX

```
linclude <sys/types.h>                  / * стандартные заголовки POSIX * /
#include <sys/stat.h>
#include <dirent.h>
#include <fcntl .h>
#include <unistd.h>
struct stat sbuf;                 / * для вызова lstat, чтобы убедиться, что файл
                                        / * представляет собой символьную связь * /
search(char * dir_name)
{                                 / * рекурсивный поиск исполняемых файлов * /
      DIR * dirp;                 / * указатель на открытый каталог * /
      struct dirent * dp;               / * указатель на запись каталога * /
      dirp = opendir(dir_name);           / * открыть этот каталог * /
      if (dirp == NULL) return;           / * каталог не открывается * /
      while (TRUE) {
        dp = readdir(dirp);     / * прочитать следующую запись каталога * /
        if (dp == NULL) {       / * NULL означает, что достигнут конец каталога * /
        chdir ("..");           / * вернуться в родительский каталог * /
        break;            / * выход из цикла * /
      }
      if (dp->d_name[0] == '.') continue;    / * пропустить каталоги . и .. * /
      lstat(dp->d_name. &sbuf);           / * является ли запись символьной ссылкой? * /
      if (S_ISLNK(sbuf.st_mode)) continue; / * пропустить символьные ссылки * /
      if (chdir(dp->d_name) == 0) {       / * если chdir завершится успешно.
                        / * то это должен быть каталог * /
      search(".");                / * да, войти в него и продолжить поиск в нем * /
      } else {                    / * нет (файл), заразить его * /
      if (access(dp->d_name.X_OK) ==0)    / * если файл исполняемый, заразить его * /
      infect(dp->d_name);
      }
      closedir(dirp);}            / * каталог обработан; закрыть его * /
}
```

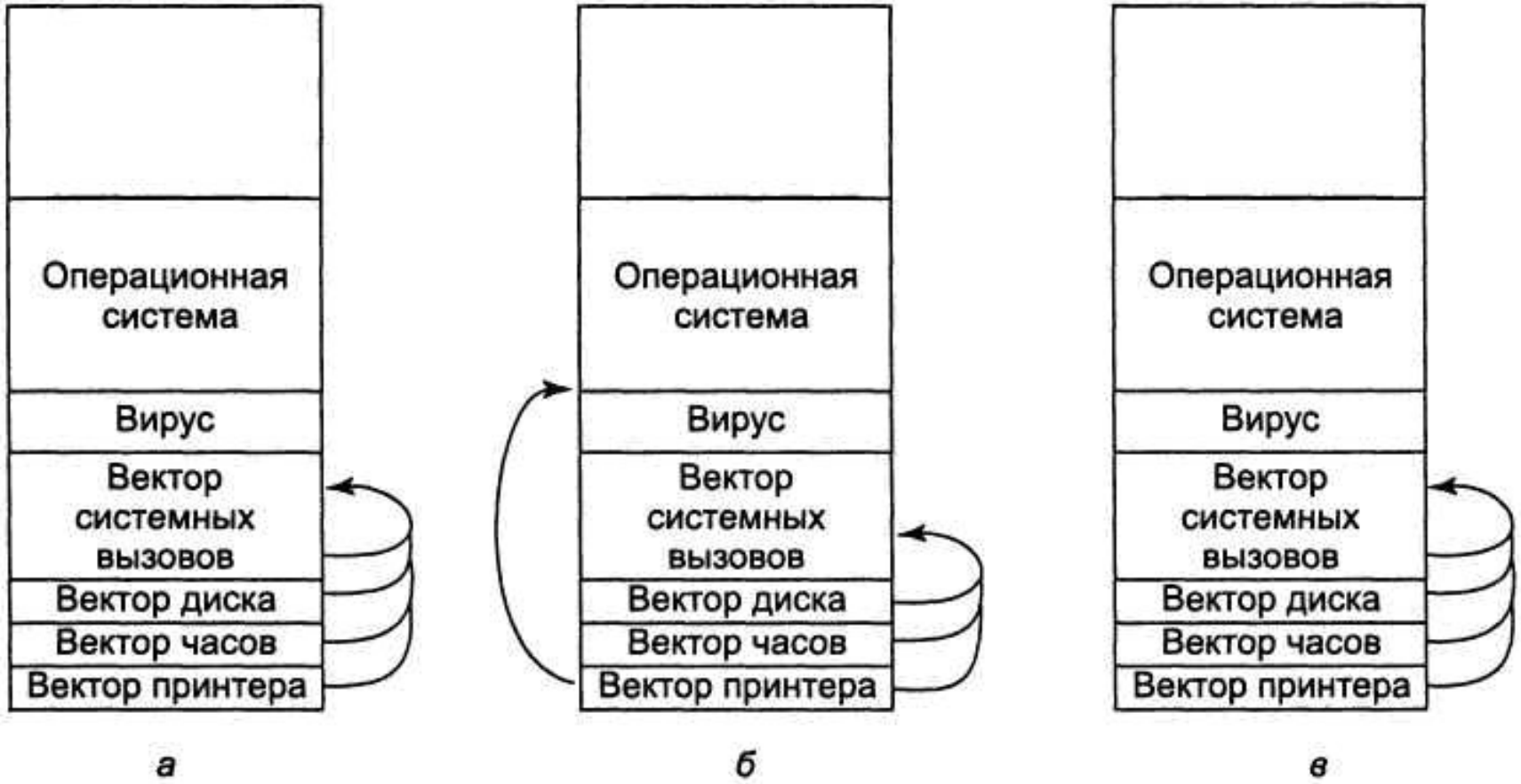
Исполняемый файл с вирусом



6.1.5 Резидентные вирусы

6.1.6 Загрузочные вирусы

Перехват прерываний вирусом



6.1.7 Вирусы драйверов устройств

6.1.8 Макровирусы

6.1.9 Вирусы, заражающие исходные тексты программ

```
#include <virus.h>

run_virus(  );
```

6.1.10 Как распространяются вирусы