

# Phrack RU issue 019

Русская версия Phrack, выпуск 019. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; Unix/Linux, BSD, Windows NT и администрирование систем; социальная инженерия, carding, физический доступ и практические схемы.

Материалы выпуска: Содержание; Утилиты DCL для хакера VMS; Понимание системы цифрового мультимплексирования (Часть 2); Форматирование номеров социального страхования; Система назначения и управления объектами (FACS); Редакционная статья Phrack о «микробэшинге»; Phrack World News; Phrack World News.

Больше крутых материалов в моём телеграм канале [@grogrigs](#)

# Содержание

**Автор:** Crimson Death

Добро пожаловать в девятнадцатый выпуск Phrack! Вы заметите, что он не такой объёмный, как предыдущий, — но этот месяц ознаменован SummerCon, и на него уже строятся планы. Если вам интересно, загляните в PWN за подробностями. Кроме того, нам нужны авторы: если у вас есть материал или вы знаете того, у кого он есть, — свяжитесь со мной. Следующий выпуск Phrack снова выйдет в полном объёме, но поскольку сейчас лето, все мы немного сбавили темп. Не волнуйтесь — Phrack по-прежнему будет выходить каждый месяц. Что ж, до встречи на SummerCon!

Crimson Death

Sysop of The Forgotten Realm

---

| № | Материал                                  | Автор            | Размер |
|---|-------------------------------------------|------------------|--------|
| 1 | Phrack Inc.<br>Содержание                 | Crimson Death    | 02k    |
| 2 | DCL Utilities for VMS<br>Hackers          | The Mentor       | 23k    |
| 3 | Digital Multiplexing<br>Systems (Часть 2) | Control C        | 18k    |
| 4 | Social Security Number<br>Formatting      | Shooting Shark   | 03k    |
| 5 | Facility Assignment &<br>Control Systems  | Phantom Phreaker | 11k    |
| 6 | Phrack Editorial on<br>Microbashing       | The Nightstalker | 06k    |
| 7 | Phrack World News<br>XVIV (Часть 1)       | Knight Lightning | 04k    |
| 8 | Phrack World News<br>XVIV (Часть 2)       | Epsilon          | 06k    |

# Утилиты DCL для хакера VMS

**Автор:** The Mentor

*Особая благодарность Silver Spy за то, что в своё время познакомил меня с DCL!*

---

Любой, кто проводит время, взламывая VAX-машины (под словом «взламывая» я имею в виду не только попытку проникнуть внутрь — я имею в виду *что-то делать*, когда уже внутри!), замечает, что командный язык DCL чрезвычайно мощен. Я собрал подборку утилит, которые не только должны оказаться полезными хакеру, но и служат хорошим примером программирования на DCL.

Были приняты все меры для того, чтобы пользовательское окружение оставалось неизменным от момента запуска файла до выхода. Все постоянные изменения сессии задокументированы.

## Краткий обзор DCL

Существует множество материалов по DCL (лучшее место для поиска информации — файлы справки VMS), поэтому я не буду учить вас программировать на нём. Чтобы воспользоваться приведённым ниже кодом, выделите нужный раздел в вашем любимом текстовом редакторе, загрузите его в файл и назовите файл `.COM`. Если вы видите файл с расширением `.COM` — это файл DCL. DCL-файлы выполняются командой:

```
$@FILENAME
```

или, если файл нужно запустить как отдельный процесс:

```
$SPAWN/NOWAIT @FILENAME
```

## Содержание

1. **CD.DOC** — документация к CD.COM (единственный документационный файл в наборе).
2. **CD.COM** — утилита смены каталога, схожая с командой `CD` в PC, но более мощная. `$SET DEFAULT` — настоящая головная боль!
3. **HUNT.COM** — ищет указанного пользователя на заданном узле. Полезно для оповещения о присутствии системного администратора.
4. **ALARM.COM** — будильник. Если логи проверяются в 8 утра — вероятно, вы захотите выйти раньше.
5. **CGO.COM** — включён, потому что короткий. Позволяет скомпилировать, скомпоновать и запустить программу на C одной командой.

У меня есть ещё около 300 страниц COM-файлов. Если вам что-нибудь нужно — напишите мне. Я постараюсь помочь. Меня можно найти на Forgotten Realm, или можно позвонить на нехакерскую (местную для меня) IBM-игровую BBS, если сообщение срочное (The Bastille — 512/353-0590, 300/1200, 24 ч. Это не лучшая хакерская доска в мире, но почта приходит ежедневно...).

Также, если программирование такого рода вас интересует — дайте знать! Я рассматриваю возможность поднять доску для обсуждения программирования (компиляторы, ИИ/экспертные системы, операционные системы и т.д.). Если получу достаточно положительных откликов — запущу. Оставляйте почту на упомянутых системах.

The Mentor

---

## CD.COM — версия 5.0 — команда смены каталога VMS

Подкаталоги — удобная функция многих компьютеров, но воспользоваться ими не всегда легко. Команды VMS для работы с подкаталогами несколько неочевидны даже для PC-программистов, привыкших к каталогам.

Решение? CD.COM — команда смены каталога, работающая почти так же, как команды CD и PROMPT в PC-DOS:

```
CD                - Показывает ваш домашний каталог, текущий каталог
                  и имя узла. (Похоже на VMS SHOW DEFAULT, но лучше.)

CD dir_name       - Переходит в каталог [dir_name].
CD [dir_name]     (То же, что SET DEFAULT [dir_name].)

CD .sub_name      - Переходит в подкаталог [.sub_name].
CD [.sub_name]    (То же, что SET DEFAULT [.sub_name].)

CD \              - Переходит в ваш домашний (корневой) каталог,
CD HOME           то есть каталог, в котором вы находитесь при входе.
CD SYS$LOGIN      (То же, что SET DEFAULT SYS$LOGIN.)

CD ..             - Переходит в каталог, расположенный выше текущего.
CD [-]            (То же, что VMS SET DEFAULT [-].)

CD ..sub_name     - Переходит «горизонтально» из одного подкаталога
CD [-.sub_name]   в другой. (То же, что SET DEFAULT [-.sub_name].)

CD *              - Выбирает подкаталог для перехода из списка.

CD .              - Сбрасывает текущий каталог.

CD ?              - Показывает инструкцию по использованию CD.
```

У команды VMS SET DEFAULT есть недостаток: можно сменить каталог на несуществующий. CD решает это изящнее: вы остаётесь в том же каталоге, что и были, и появляется сообщение:

```
[dir_name] Directory does not exist!
```

PC-DOS позволяет отображать текущий каталог в приглашении командной строки. (Если вы ещё не видели эту функцию — попробуйте команду PC-DOS PROMPT \$P\$G.) CD.COM будет изменять приглашение при каждой смене каталога, если вы добавите в файл LOGIN.COM следующую строку:

```
DEFINE SYS$PROMPT "ON"
```

Без этой строки приглашение не изменяется. Вместо этого имя домашнего (корневого) каталога, текущего каталога и имя узла отображаются при каждом выполнении команды CD.

Поскольку VMS допускает приглашение не длиннее 32 символов, если переход в подкаталог делает приглашение слишком длинным, CD автоматически убирает часть каталогов высшего уровня, чтобы приглашение оставалось коротким, и отображает \* в качестве одного из символов приглашения.

CD позволяет использовать имена каталогов, определённые командой DEFINE. Например, если вы посещаете один из курсов доктора Смита CS3358, можно определить каталог его заданий следующим образом:

```
DEFINE SMITH "DISK$CS:[CS.SMITH.3358]"
```

Тогда CD SMITH перенесёт вас в этот каталог. Попробуйте! Некоторые каталоги уже определены системой. Команда SHOW LOGICAL подскажет некоторые из этих системных каталогов, если хотите

Как и в PC-DOS, каталоги и подкаталоги VMS имеют древовидную структуру. Системный корневой каталог для вашего диска называется [000000], и в нём содержатся имена всех подкаталогов диска. Каталоги воображаемого пользователя CS335825305 были бы расположены так:

```

                                [000000]
                                .   .   .   .
Каталоги CS3358:                .   .   .   .
                                *
... [CS3358251]    [CS3358252]    [CS3358253]    [CS3358254] ...
                                .   .   .
Каталоги CS3358253:            .   .   .
                                *
... [CS3358253.04HOPE]    [CS3358253.05JONES]    [CS3358253.06KEY] ...
                                .   .
Каталоги CS335825305:         .   .
                                *   *
                                [CS3358253.05JONES.MAIL]    [CS3358253.05JONES.BULL]

```

CREATE/DIR [.sub\_name]

VMS также позволяет использовать символы ` вместо [ и ]` для указания имён каталогов. CD полностью это поддерживает.

```

$! CD.COM v6.09
$! The Ultimate Change Directory Command.
$!
$ hdir      = f$trnlrm("SYS$LOGIN")           ! Home Directory
$ ndir      = f$edit(p1,"UPCASE")             ! New Directory
$ odir      = f$environment("DEFAULT")        ! Old Directory
$ prompton  = (f$edit(f$trnlrm("SYS$PROMPT"),"UPCASE") .eqs. "ON")
$!
$ if (ndir .eqs. "") then goto DISPLAY ! No Dir
$ if (ndir .eqs. "**") then goto DIRSEARCH ! Search for Dirs
$ if (ndir .eqs. "?") then goto HELP ! Instructions
$!
$ PARSE:
$ length    = f$length(ndir)                  ! Fix up ndir
$ if (f$location("@",ndir) .eq. 0) .or. -
    (f$location("$",ndir) .eq. 0) then ndir = f$extract(1, length - 1, ndir)
$ right     = f$location("]",ndir) + 1
$ if (right .gt. length) then right = f$location(">", ndir)
$ if (right .le. length) then ndir = f$extract(0, right, ndir)
$!
$ if (f$trnlrm(ndir) .eqs. "") then goto CASESYM ! Not Logical Name
$ ndir      = f$trnlrm(ndir)                  ! Logical Name
$ goto PARSE
$!
$ CASESYM:
$ if ("'"&ndir'" .eqs. "") then goto CASE0 ! Not Symbol
$ ndir      = 'ndir'                          ! Symbol
$ goto PARSE
$!
$ CASE0:
$ len_ndir  = f$length(ndir)                  ! Regular Dir
$ if (f$location("[", ndir) .lt. len_ndir) .or. -
    (f$location("<", ndir) .lt. len_ndir) then goto SETDIR
$!

```

```

$ CASE1:                                     ! Home Dir
$ if ((ndir .nes. "HOME") .and. (ndir .nes. "\")) then goto CASE2
$     ndir = hdir
$     goto SETDIR
$!
$ CASE2:                                     ! . . . .dir
$ if (f$location(".", ndir) .nes. 0) then goto CASE3
$     if (ndir .eqs. "..") then ndir = "-"
$     if (f$extract(0, 2, ndir) .eqs. "..") -
$         then ndir = "-" + f$extract(1, len_ndir - 1, ndir)
$     ndir = "[" + ndir + "]"
$     if (ndir .eqs. "[.]") then ndir = odir
$     goto SETDIR
$!
$ CASE3:                                     ! :
$ if (f$location(":", ndir) .ge. len_ndir) then goto CASE4
$     left = f$location(":", ndir) + 1
$     symbol = f$extract(left, 1, ndir)
$     if (symbol .eqs. ":") then goto CASE3B      ! :: Node
$     if ((symbol .eqs. "[" .or. (symbol .eqs. "<")) then goto SETDIR
$     ndir = f$extract(0, left, ndir) + "[" -
$         + f$extract(left, len_ndir - left+1, ndir) + "]"
$     goto SETDIR
$!
$ CASE3B:                                     ! NODE::nothing
$ if (f$length(ndir)-1 .gt. left) then goto CASE3C
$     ndir = ndir + "[000000]"
$     goto SETDIR
$!
$ CASE3C:                                     ! NODE::directory
$ if ((f$location("[", ndir) - f$location("<", ndir)) .ne. 0) -
$     then goto SETDIR
$
$     ndir = f$parse(ndir,,, "NODE") + "[" + f$parse(ndir,,, "NAME") + "]"
$     goto SETDIR
$!
$ CASE4:                                     ! dir
$ ndir = "[" + ndir + "]"
$!
$ SETDIR:
$ set default 'ndir'
$ if (f$parse("") .eqs. "") then goto DIRERROR
$!
$ DISPLAY:
$ if ((ndir .nes. "") .and. prompton) then goto NODISPLAY
$     hnode = f$getsyi("NODENAME")
$     cnode = f$parse(f$trnlnm("SYS$DISK"),,,, "NODE") - ":"
$     if (cnode .eqs. "") then cnode = hnode
$     cdir = f$environment("DEFAULT")
$     write sys$output " "
$     write sys$output "         Home Node: ", hnode
$     write sys$output "         Home Directory: ", hdir
$     if (cdir .eqs. hdir) .and. (cnode .eqs. hnode) then goto DISPSKIP
$     write sys$output "         Current Node: ", cnode
$     write sys$output "         Current Directory: ", cdir
$ DISPSKIP:
$     write sys$output " "
$!
$ NODISPLAY:
$ ndir = f$environment("DEFAULT")
$ if .not. prompton then goto END
$!
$ if (f$length(ndir) .ge. 32) then goto TOOLONG
$!
$ SETPROMPT:
$ set prompt = 'ndir' " "
$!
$ END:
$ exit
$!
$ DIRERROR:

```

```

$ write sys$output " "
$ write sys$output "          ", ndir, " Directory does not exist!"
$ write sys$output " "
$ set default 'odir'
$ ndir = odir
$ goto NODISPLAY
$!
$! Prompt Problems-----
$!
$ TOOLONG:
$! Prompt is too long. Get rid of everything to the left of [ or <. If that
$! doesn't work, get rid of a subdirectory at a time. As a last resort,
$! set the prompt back to $.
$!
$ left      = f$location("[", ndir)
$ len_ndir = f$length(ndir)
$ if (left .ge. len_ndir) then left = f$location("<", ndir)
$ if (left .gt. 0) .and. (left .lt. len_ndir) -
    then ndir = f$extract(left, len_ndir - left, ndir)
$!
$ STILLTOOLONG:
$ if (f$length(ndir) .lt. 32) then goto SETPROMPT
$ left      = f$location(".", ndir) + 1
$ len_ndir = f$length(ndir)
$ if left .ge. len_ndir then ndir = "$ "
$ if left .ne. len_ndir -
    then ndir = "[" + f$extract(left, len_ndir - left, ndir)
$ goto STILLTOOLONG
$!
$! Wildcard Directory-----
$!
$ DIRSEARCH:
$ error_message = f$environment("MESSAGE")
$ on control_y then goto DIREND
$ on control_c then goto DIREND
$ set message/nosev/nofac/noid/notext
$ write sys$output " "
$ dispct = 1
$ direct = 0
$ pauseflag = 1
$!
$ DIRLOOP:
$ userfile = f$search("*.dir")
$ if (userfile .eqs. "") .and. (direct .ne. 0) then goto DIRMENU
$ if (userfile .eqs. "") then goto DIRNONE
$ dispct = dispct + 1
$ direct = direct + 1
$ on severe then $ userprot = "No Priv"
$ userprot = f$file_attributes(userfile, "PRO")
$ if userprot .nes. "No Priv" then userprot = " "
$ userfile'direct' = "[" + f$parse(userfile, ,, "NAME") + "]"
$ userprot'direct' = userprot
$ lengthflag = (f$length(userfile'direct') .gt. 18)
$ if lengthflag then write sys$output -
$ f$fao(" !3SL !34AS ", direct, userfile'direct'), userprot'direct'
$ if (.not. lengthflag) then write sys$output -
$ f$fao(" !3SL !20AS ", direct, userfile'direct'), userprot'direct'
$ if (dispct .lt. 8) then goto DIRLOOP
$ direct = direct + 1
$ userfile'direct' = ""
$ direct = direct + 1
$ userfile'direct' = ""
$ if pauseflag then goto DIRMENU
$ dispct = 0
$ goto DIRLOOP
$!
$ DIRMENU:
$ write sys$output " "
$ if (userfile .eqs. "") then goto DIRMENU2
$ write sys$output "      M      More subdirectories"
$ if pauseflag then -

```

```

$      write sys$output "      N      More subdirectories/No pause"
$!
$ DIRMENU2:
$      write sys$output "      R      Re-Display subdirectories"
$      write sys$output "      Q      Quit (default)"
$
$ DIRINQUIRE:
$ write sys$output " "
$ inquire dirchoice " Select One"
$ write sys$output " "
$!
$ if (dirchoice .gt. 0)      .and. -
    (dirchoice .le. direct) then goto DIRCASEDIGIT
$ dirchoice = f$edit(dirchoice,"UPCASE")
$ if (dirchoice .eqs. "") .or. -
    (dirchoice .eqs. "Q") then goto DIRCASEBLANK
$ if (dirchoice .eqs. "M") .or. -
    (dirchoice .eqs. "N") then goto DIRCASEMORE
$ if (dirchoice .eqs. "R") then goto DIRCASERED
$!
$ DIRCASEERROR:
$ if (direct .eq. 1) then write sys$output -
    " Select 1 to change to the ", userfile1, " subdirectory. "
$ revdirect = direct
$ if (dispct .eq. 8) then revdirect = revdirect - 2
$ if (direct .gt. 1) then write sys$output -
    " Valid subdirectory selections are 1 through ", revdirect, " (Octal)."
$ goto DIRINQUIRE
$!
$ DIRCASEDIGIT:
$ if (userfile'dirchoice' .eqs. "") then goto DIRCASEERROR
$ ndir = userfile'dirchoice'
$ goto DIREND
$!
$ DIRCASEBLANK:
$ write sys$output " Subdirectory not changed."
$ write sys$output " "
$ goto DIREND
$!
$ DIRCASEMORE:
$ dispct = 0
$ if (dirchoice .eqs. "N") then pauseflag = 0
$ if (userfile .nes. "") then goto DIRLOOP
$ write sys$output " No more subdirectories to display."
$ goto DIRINQUIRE
$!
$ DIRCASERED:
$ dispct = 1
$ DISPLOOP:
$ if (userfile'dispct' .eqs. "") then goto DISPDONT
$ lengthflag = (f$length(userfile'dispct') .gt. 18)
$ if lengthflag then write sys$output -
    f$fao(" !3SL !34AS ", dispct, userfile'dispct'), userprot'dispct'
$ if (.not. lengthflag) then write sys$output -
    f$fao(" !3SL !20AS ", dispct, userfile'dispct'), userprot'dispct'
$ DISPDONT:
$ dispct = dispct + 1
$ if (dispct .le. direct) then goto DISPLOOP
$ goto DIRMENU
$!
$ DIRNONE:
$ write sys$output "No subdirectories to choose, or no directory privileges."
$ write sys$output " "
$ goto DIREND
$!
$ DIREND:
$ set message 'error_message'
$ on control_y then exit
$ on control_c then exit
$ if (ndir .eqs. "**") then goto DISPLAY
$ goto PARSE

```



```

$!
$!-Help-----
$!
$  HELP:
$  type sys$input

          CD.COM  Version 6  VMS Change Directory Command

          Usage:  CD command/directory

CD          Display home directory,          CD ..        Change directory to the
             current directory, node.         CD [-]        dir above current dir.

CD \         Change directory to your         CD ..sub      Change directory to a
CD HOME      SYS$LOGIN directory.             CD [-.sub]    "sideways" subdirectory.

CD dir       Change directory to the          CD *          Display/select the
CD [dir]     [dir] directory.                 available subdirectories.

CD .sub      Change directory to the          CD .          Reset current directory.
CD [.sub]    [.sub] subdirectory.             CD ?          Display CD instructions.

          CD :== @SYS$LOGIN:CD.COM             DEFINE SYS$PROMPT "ON"
          To make CD available from            To have the VMS $ prompt
          any directory you change to.         display the current directory.

                                By The Mentor

$  goto END

```

## Код HUNT.COM

```

$ ! HUNT.COM
$ ! By The Mentor
$ ! Updated by: The Mad Mexican
$ ! Usage: SPAWN/NOWAIT @HUNT
$ !
$ ! Searches SHOW USER output for a specified user,  strobes at given
$ ! intervals considering the severity of the hunt at which time output
$ ! is generated and process terminates.  If user loggs in then output
$ ! is generated and process terminates.  May check both nodes if a set
$ ! host is called.  Also supports a file with the names to be hunted for.
$ !
$ ! *** NOTE ***   This is set up for a two-node system with NYSSA
$ !                being the default node and TEGAN being the alternate
$ !                node (Circuit Breaker and some others will recognize
$ !                the nodes as my 'home' ones.)  You will need to
$ !                slightly modify the code to reflect the nodename(s)
$ !                of whatever system you are using...
$ !
$ !
$ !
$ say="write sys$output"
$ on control then goto door
$ monitored_node = "'NODE'"
$ say "Monitoring node '"monitored_node'".  <HIT RETURN>"
$ severity_of_hunt:
$ inquire selection "Severity of HUNT, 1 being the most urgent: 1-2-3"
$ if selection.ge.2 then goto selection_2
$ delay="wait 00:00:20"
$ loop_count=40
$ goto begin_process
$ selection_2:
$ if selection.eq.3 then goto selection_3
$ delay="wait 00:01:00"
$ loop_count=8
$ goto begin_process
$ if selection.gt.3 then goto severity_of_hunt
$ delay="wait 00:02:30"

```

```

$ loop_count=20
$ begin_process:
$ if monitored_node.eqs."TEGAN" then goto search_file_tegan
$ if f$search("nyssa.dat9") .nes. "" then goto file_exist
$ goto continue
$ search_file_tegan:
$ if f$search("tegan.dat9") .nes. "" then goto file_exist
$ continue:
$ say "hit <RETURN>"
$ inquire/nopunctuate choice9 "Who are we hunting for? "
$ if choice9 .eqs. "" then exit
$ count = 0
$ bell_sound[0,8]=%X07
$ top:
$ sho user/output='monitored_node'.dat9
$ purge 'monitored_node'.dat9
$ set message/nofac/noid/notext/nosev
$ search 'monitored_node'.dat9 'choice9'
$ a=$severity
$ if a .eqs. "1" then goto found_user
$ set message 'temp_msg9'
$ count = count + 1
$ if count .ge. 'loop_count' then goto give_up
$ delay
$ goto top
$ file_exist:
$ say "ERROR - Could not create temporary data file."
$ say "Please delete or rename '"NODE'.DAT9"
$ exit
$ found_user:
$ say bell_sound
$ say "'choice9' is now online on node '"monitored_node'."
$ say bell_sound
$ goto door
$ give_up:
$ say " "
$ say "'choice9' has not yet logged in on '"monitored_node'."
$ door:
$ say bell_sound
$ say "HUNT routine has terminated on node '"monitored_node'."
$ delete/noconfirm/nolog 'monitored_node'.dat9;*
$ set message 'temp_msg9'
$ exit

```

## Код ALARM.COM

```

$ ! ALARM.COM
$ ! By The Mentor
$ ! Usage: SPAWN/NOWAIT @ALARM
$ ! Strobes f$time() every 5 seconds until specified time
$ ! is met at which time output is generated and process terminates.
$ CLR = " "
$ count = 0
$ PID = F$PID(CONTEXT)
$ TERMINAL = F$GETJPI('PID',"TERMINAL")
$ DEVICE = F$GETDVI(TERMINAL,"DEVTYPE")
$ IF DEVICE .EQS. 110 THEN CLR = "[H[2J" ! VT220
$ IF DEVICE .EQS. 98 THEN CLR = "[H[2J" ! VT102
$ IF DEVICE .EQS. 96 THEN CLR = "[H[2J" ! VT100
$ IF DEVICE .EQS. 64 THEN CLR = "HJ" ! VT52
$ CLS = "WRITE SYS$OUTPUT CLR"
$ DATE = F$CVTIME(F$TIME())
$ NODE = F$GETSYI("NODENAME")
$ bell[0,8]=%X07
$ ON CONTROL THEN GOTO DOOR
$ say = "write sys$output"
$ say f$cvtime(,,"TIME")
$ say " "

```

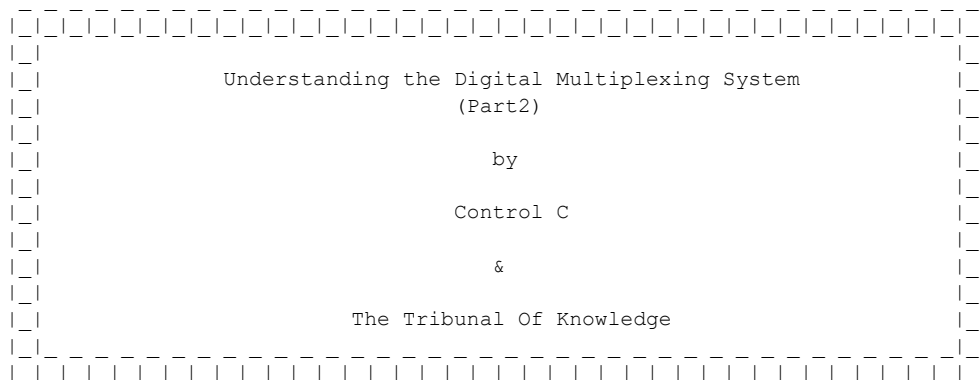


Вот и всё. Надеюсь вернуться в следующем выпуске с другими программами. И помните: программисты, свяжитесь со мной!

The Mentor

День благодарения, 1987

# Понимание системы цифрового мультиплексирования (Часть 2)



**Автор:** Control C & The Tribunal Of Knowledge

Некоторые из вас, возможно, помнят мой файл о цифровом мультиплексировании в Phrack 10. Это обещанная вторая часть, которую я откладывал примерно полтора года. Файл был готов ещё в мае 87-го, но я решил выпустить его только сейчас. Итак, вот он!

Коммутаторы DMS впервые появились в 1979 году. С тех пор они претерпели множество изменений, чтобы обеспечить совместимость с самыми разными типами оборудования. DMS способен взаимодействовать с SP-1, #5 XBar, 1ESS, 2ESS, 3ESS, 4ESS, NX1D, NX1E, TSD, SXS, ETS4, NO. 1 EAC, NO. 2 EAX, NO. 3 EAX, TSPS, CAMA/3CL boards, Stromberg Carlson Turret of ONI и Visual Indicators, Modified North Electric TSD for ONI, Stromberg Carlson (CAMA operator Position — ONI/ANI), AE #31 Switchboard, Co-located NT/AE switchboard I/C, O/G, UDC data poller of OM, DACS (Directory Assistance Charging System), NT #144 LTD, WECO #14 LTD, WECO #16 LTD, CALRS (Centralized Automated Loop Reporting System), Badger 612A, AE #1 и #21 LTD, AE #30, SC #14 LTD, Lordel MITS70 line Test System, Porta System Line Test Unit, Pulsar II IMTS, Teradyne loop test unit, а также WECO MLT 1 (Mechanized Loop Testing System).

## Общеканальная межстанционная сигнализация

Общеканальная межстанционная сигнализация (Common Channel Interoffice Signaling, CCIS) — это метод сигнализации и реализации сервисов сетевого уровня. CCIS обеспечивает надёжные, кристально чистые каналы передачи сигнальных данных между сетью и коммутационными узлами. Метод сигнализации CCIS использует оборудование передачи данных, отдельное от голосовых транков.

## Общеканальная межстанционная сигнализация № 6

Основой системы CCIS является международный стандарт № 6 Международного консультативного комитета по телефонии и телеграфии (CCITT), который задействован в полную меру в сети хранимых программ управления (Stored Program Control, SPC) компании AT&T.

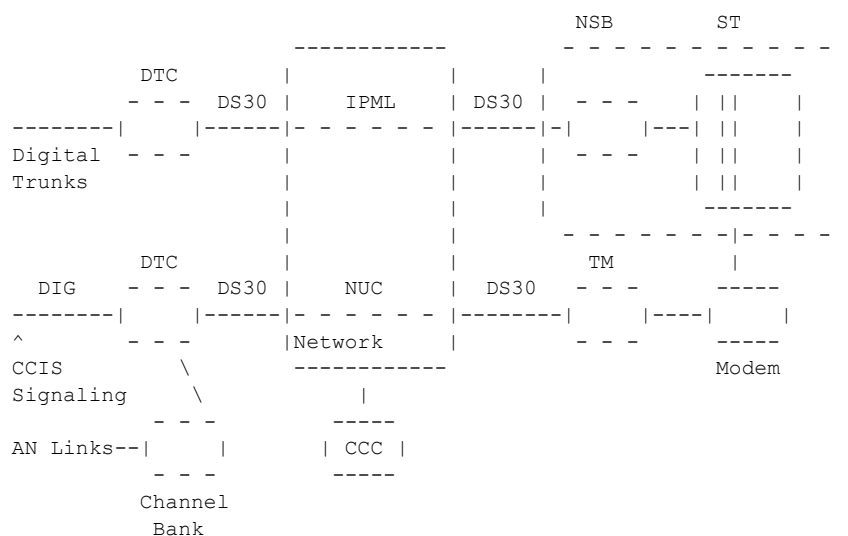
Сеть CCIS6 состоит из ряда сигнальных регионов, в каждом из которых функционирует пара взаимосвязанных пунктов транзита сигнализации (Signal Transfer Points, STP). Коммутационные системы, подключённые к CCIS6 и соединённые со STP, называются обслуживающими узлами

(Serving Offices, SO).

Полосовая сигнализация (CCIS-BS) применяется для транковой сигнализации на межстанционных транках типа «intertoll», использующих сеть CCIS.

Прямая сигнализация (CCIS-DS) используется для обмена сигналами между коммутационными машинами SPC и сетевой точкой управления (Network Control Point, NCP). В настоящее время CCIS6 поддерживает расширенный INWATS с функцией проверки исходящего офиса (OSO), проверку данных вызывающей карты (CCV), механизированный сервис вызывающих карт (MCCS) и проверку биллингового номера (BNS). CCIS6 совместима с DMS-100/200, DMS-200, а также DMS-100/200 или DMS-200 с TOPS.

### Схема CCIS6:



### Аббревиатуры:

- **DIG** — Digital (Цифровой)
- **AN** — Analog (Аналоговый)
- **DTC** — Digital Trunk Controller (Цифровой контроллер транков)
- **MSB** — Message Switch Buffer (Буфер коммутатора сообщений)
- **ST** — Signaling Terminal (Сигнальный терминал)
- **TM** — Trunk Module (Модуль транков)
- **NUC** — Nailed-Up Connection (Постоянное соединение)
- **IPML** — Inter-Peripheral Message Link (Межпериферийный канал передачи сообщений)

### Общеканальная межстанционная сигнализация № 7

Общеканальная сигнализация (CCS) № 7, или CCIS7, — это система CCS, основанная на стандарте CCITT № 7. CCIS7/CCS7 на коммутаторе DMS состоит из двух частей: части переноса сообщений (Message Transfer Part, MTP) и временной части пользователя телефонии. Они совместимы с DMS-100, DMS-200, DMS-100/200 и DMS-100/DMS-100/200 с TOPS.

CCIS7 не разграничивает полосовую и прямую сигнализацию. Для маршрутизации обратно к коммутатору CCIS7 использует коды точек назначения/происхождения (DPC/OPC).

CCIS7 поддерживает автоматический сервис вызывающих карт (ACCS), расширенный INWATS, службы локальной сигнализации и возможности прямого набора сервисных номеров.

## **Равный доступ (Equal Access)**

Тандемный узел доступа (Access Tandem, AT) DMS-200 выполняет функцию концентрации и распределения трафика для межрегиональных (interLATA) вызовов, поступающих в локальную зону доступа и транспортировки (Local Access and Transport Area, LATA) или исходящих из неё. Это предоставляет межрегиональным операторам (IC) доступ к нескольким оконечным офисам внутри LATA. Система поддерживает коды доступа межрегиональных операторов (10xxx), набор 10xxx и 950-YXXX, автоматическое определение номера (ANI) для всех вызовов, контроль ответа, равнодоступный автоматический учёт сообщений (AMA) для исходящих и входящих вызовов, а также сигнализацию операторских служб.

DMS-100 EA обеспечивает прямой и тандемный коммутируемый доступ к межрегиональным операторам внутри LATA как для исходящих, так и для входящих вызовов. Он предоставляется в трёх вариантах:

### **Оконечный офис с равным доступом (EAEO)**

DMS-100 Equal Access End Office (EAEO) обеспечивает прямое соединение с точками присутствия (Point of Presence, POP) межрегиональных и международных операторов (IC/INC) внутри LATA.

### **Тандемный узел доступа совместно с EAEO**

DMS-200 Access Tandem (AT), применяемый вместе с оконечным офисом с равным доступом (EAEO), позволяет тандемной коммутации транков соединяться с точками присутствия IC/INC внутри LATA.

Соединение EAEO с IC/INC через DMS-200 AT использует так называемую двухступенчатую перекрывающую выходную импульсную передачу, которая сокращает время установления соединения. На первом этапе AT выдаёт импульсом цифры OZZ + XXX для идентификации набранного IC/INC и выбора исходящего транка. Затем устанавливается соединение от IC/INC до EAEO через AT. На втором этапе цифры, включающие ANI и вызываемый номер, передаются через DMS-200 AT к IC/INC.

Запись AMA о завершении вызова в формате AT&T формируется DMS-200 для всех EAEO. Запись AMA о завершении вызова создаётся для каждого вызова, достигшего этапа захвата транка от IC/INC и получения сигнала «wink» от DMS-200 AT.

### **Тандемный узел доступа с оконечным офисом без равного доступа**

DMS-200 AT, работающий с оконечным офисом без равного доступа, обеспечивает тандемную транковую связь с точкой присутствия IC/INC внутри LATA. Для установления соединения — подключения оконечного офиса Feature Group B (FGB) или Feature Group C (FGC) к IC/INC через DMS-200 AT — используется стандартная сигнализация Bell Central Automatic Message Accounting (CAMA). Тандемный узел доступа использует цифры XXX кода доступа 950-YXXX, выданные импульсом оконечным офисом FGB, для идентификации IC/INC и подключения к исходящему транку.

## **Механизированный сервис вызывающих карт (MCCS)**

Мошеннические действия с кредитными картами, выставление счёта на третий номер, перехват оплаты вызовов, а также нарастающая автоматизация операторских сервисов непосредственно привели к внедрению механизированного сервиса вызывающих карт (MCCS) на платформах DMS-200/TOPS и в удалённых и головных центрах централизации операторов (ОС).

MCCS использует CCIS для передачи запросов и ответов к DMS-200/TOPS и от него. Обработанные оператором вызовы по кредитным картам и прямой ввод данных кредитной карты абонентами через DTMF-телефоны обслуживаются с помощью специальных механизмов MCCS. Оба способа — обработка оператором и прямой ввод данных кредитной карты — позволяют сократить количество операторов.

Проверка биллингового номера (BNS) расширяет возможности оператора по обработке вызовов с оплатой третьим лицом и переводом оплаты, используя CCIS для проверки номера в базе данных валидации на наличие ограничений выставления счёта (например, третий номер является «крепостью»). Эта функция естественным образом снижает мошенническое использование сервиса оплаты вызовов третьим лицом.

Общеканальная межстанционная сигнализация — прямая сигнализация (CCIS-DS), на которой построен MCCS, используется для передачи сообщений к множеству возможных центров проверки биллинга (BVC) и от них. Сообщения, передаваемые в BVC в рамках MCCS, включают биллинговый номер и персональный идентификационный номер (PIN). В BNS сообщения содержат специальный биллинговый номер (оплата третьим лицом или перевод оплаты). Ответные сообщения от BVC включают данные о действительности номера, ограничениях биллинга (при их наличии) и код офиса учёта доходов (RAO).

## **Вспомогательная система операторских служб (AOSS)**

DMS-200 Auxiliary Operator Services System (AOSS) используется преимущественно для служб справочной информации и перехвата, которые не входят в пакет TOPS. AOSS аналогична TOPS и сосуществует с ней на транзитной системе DMS-200.

К основным преимуществам AOSS относятся: предоставление службы справочной информации в современных условиях, выполнение административных функций позиций AOSS силами системы технического обслуживания DMS-200 Toll, экономия на транках за счёт совмещения транкинга для вызовов 1+ и 0+, управление трафиком справочной службы методами TOPS, создание встроенной системы обучения, не требующей дополнительного оборудования и снижающей затраты на подготовку персонала.

## **Интегрированная деловая сеть (IBN)**

Интегрированная деловая сеть (Integrated Business Network, IBN) — это коммерческая концепция, разработанная для малого и крупного бизнеса с целью предоставления современных возможностей УАТС (PBX) и Centrex. Операционная компания может использовать IBN для поддержания и укрепления своих конкурентных позиций на действующих коммутаторах DMS-100 и DMS-100/200. Используя коммутатор DMS-100, операционная компания может поддерживать различные деловые функции наряду с существующим местным/транзитным трафиком.

Сервисы IBN могут быть подключены к Centrex-Central Office (CO) или Centrex-Customer Unit (CCU) посредством дополнительных программных модулей и незначительных аппаратных улучшений.



Текущие функции IBN включают: масштабируемую систему на до 30 000 линий, возможности сетевого взаимодействия, городской сервис для коммутатора DMS-100 и удалённых узлов для любой абонентской станции, детализацию сообщений станции (SMDR), которая предоставляет клиентам IBN записи о вызовах. Эти записи могут использоваться для системного анализа, управления и распределения затрат по станциям. SMDR может применять записи LAMA, если узел IBN оснащён оборудованием LAMA, централизованными функциями обслуживания и администрирования диспетчерской связи, а также прямым входящим набором (DID).

## Электронная коммутируемая сеть (ESN)

Электронная коммутируемая сеть разработана для удовлетворения телекоммуникационных потребностей крупных многоузловых корпораций. ESN строится на базе цифровой деловой коммуникационной системы SL-1 или SL-100 с функциями сетевого взаимодействия, либо на основе узла DMS-100 IBN. SL-1 рассчитана на 30–5000 линий. SL-100 и узлы DMS-100 IBN могут обслуживать от нескольких тысяч до 30 000 линий.

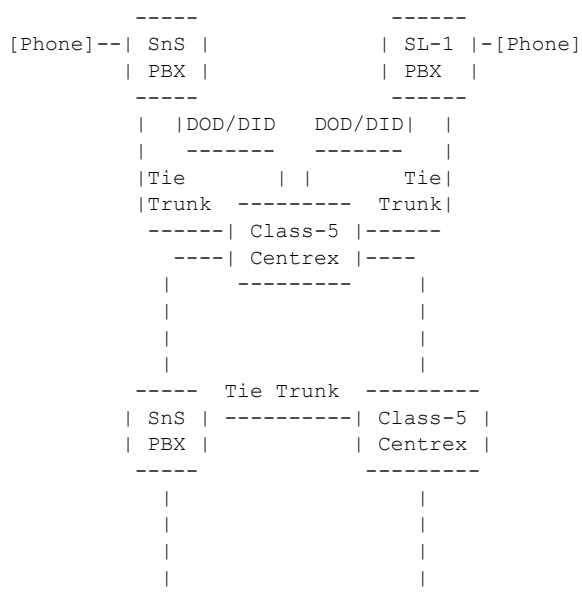
Узел DMS-100 IBN или SL-100 может дистанционно обслуживать множество объектов с головного сайта. Это обеспечивается соединением через цифровые передающие средства, установленные в виде удалённых модулей на площадке абонента.

## Специализированная служба общего пользования (SCCS)

DMS-250 Specialized Common Carrier Service (SCCS) обеспечивает возможность преобразования аналогового сигнала в цифровой (A/D) и цифрового в аналоговый (D/A), необходимого при работе с аналоговыми цепями. DMS-250 также способен коммутировать голосовые и цифровые каналы.

DMS-250 принимает информацию в аналоговом или цифровом виде и с помощью временного обмена слотами коммутирует её с любого входного порта на временно адресованный и подключённый выходной порт. Информация может быть или не быть преобразована обратно в аналоговый вид.

## Схема обычной частной телекоммуникационной сети:



|          |       |  |       |  |          |
|----------|-------|--|-------|--|----------|
| [Phone]- | Small |  | SL-1  |  | -[Phone] |
|          | PBX   |  |       |  |          |
| -----    |       |  | ----- |  |          |

## Сотовая мобильная радиосвязь

Сотовая система состоит из двух основных компонентов: сотового коммутатора и оборудования базовых станций.

### Системы сотовой коммутации

Сотовый коммутатор выполняет три основные функции: аудиокоммутацию, управление базовыми станциями и системное администрирование.

Коммутаторы DMS предоставляют три базовые реализации сотовой коммутации: автономную, комбинированную и удалённую.

Автономная коммутация осуществляется мобильной телефонной станцией (Mobile Telephone Exchange, MTX), сопряжённой с одним или несколькими оконечными офисами 5-го класса. Соединение выполняется по транкам DID/DOD. В зависимости от потребностей зоны обслуживания MTX может быть представлена в следующих вариантах: MTX — для городских зон, MTXC — для пригородных зон, MTXM — для сельской местности.

Комбинированная коммутация интегрируется в DMS-100 посредством аппаратных дополнений и сотового программного обеспечения. Комбинированная коммутация призвана обеспечить простой и экономически эффективный способ внедрения сотовых сервисов в существующий узел.

Удалённая коммутация реализуется путём объединения удалённого центра коммутации (Remote Switching Center, RSC) с контроллером базовой станции (Cell Site Controller, CSC). Данная комбинация обслуживается либо автономным, либо комбинированным коммутатором. Удалённая коммутация предназначена для обслуживания пригородных центров, удалённых районов или небольших населённых пунктов и обеспечивает дополнительную гибкость для расширяющихся систем.

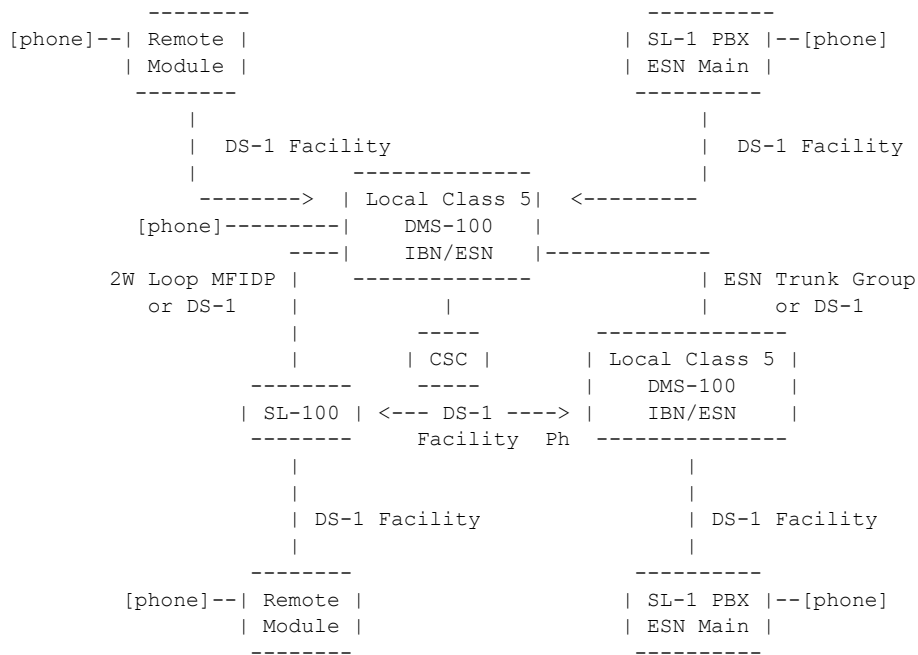
Все перечисленные типы сотовых коммутаторов способны балансировать нагрузку между различными базовыми станциями. Например, если нагрузка на одну станцию достигает программируемого порога перегрузки, вызовы перенаправляются на ближайшие станции с достаточной пропускной способностью.

### Оборудование базовых станций

Оборудование базовой станции состоит из CSC и радиооборудования. CSC управляется сотовым коммутатором и, в свою очередь, управляет радиооборудованием и задачами технического обслуживания. CSC совместима с любым сотовым коммутатором MTX благодаря удалённому кластерному контроллеру (Remote Cluster Controller, RCC).

Радиооборудование включает автономные радиоканальные блоки (Radio Channel Units, RCU), антенны, многоканальные передающие устройства и объединители приёмников.

Благодаря различному программному обеспечению RCU способен выполнять голосовые, навигационные и тестовые функции. Автономная конструкция позволяет размещать RCU на удалении от CSC. Каждый RCU оснащён встроенными схемами для расширенного тестирования радиочасти системы.



---

*Конец файла*  
**5-23-87**

Если у вас есть вопросы, свяжитесь со мной или с любым другим членом ТОК!

Control C  
 !ТОК! (1987)

# Форматирование номеров социального страхования

**Автор:** Shooting Shark, 21 июня 1988 г.

Некоторые виды компьютерного мошенничества, например создание фиктивных записей в платёжных базах данных, требуют генерации поддельного номера социального страхования (SS#). Многие работодатели пытаются выявить «фантомные» номера, прогоняя их через верификационные программы. В этой статье я покажу, как обойти такую проверку, сформировав правдоподобно выглядящий SS#.

Для начала — несколько общих правил:

- Средние две цифры SS# могут быть нечётными или чётными, если номер был выдан после 1965 года. Все номера, выданные до 1965 года и имеющие средние цифры 10 и выше, должны быть чётными.
- На сегодняшний день ни один SS# не был выдан с первой цифрой 8 или 9. Очень мало номеров выше 595 было задействовано, поэтому соблюдайте осторожность. Диапазон 700–729 был выдан Агентством по пенсионному обеспечению железнодорожников давным-давно, а значит, такие номера принадлежат пожилым людям. Номера в диапазоне 596–626 ещё не назначены (насколько мне известно), однако 596–599 зарезервированы для Пуэрто-Рико, 600–601 — для Аризоны, а 602–626 — для Калифорнии.

Следующий шаг необходим лишь в том случае, если требуется, чтобы место выдачи (и, вероятно, штат рождения или проживания) совпадало с SS#. В таком случае обратитесь к следующей таблице:

| Первые три цифры<br>=====                            | Регион<br>=====                                                                  |         |                |
|------------------------------------------------------|----------------------------------------------------------------------------------|---------|----------------|
| 000                                                  | Иностранный обмен, туристы и т.д. (многие студенты колледжей имеют такие номера) |         |                |
| 001–003                                              | Нью-Гэмпшир                                                                      | 004–007 | Мэн            |
| 008–009                                              | Вермонт                                                                          | 010–034 | Массачусетс    |
| 035–039                                              | Род-Айленд                                                                       | 040–049 | Коннектикут    |
| 050–134                                              | Нью-Йорк                                                                         | 135–158 | Нью-Джерси     |
| 159–211                                              | Пенсильвания                                                                     | 212–220 | Мэриленд       |
| 221–222                                              | Делавэр                                                                          | 223–231 | Вирджиния      |
| 232–236 (кроме<br>SS# начинающихся<br>с "232 30"...) | Западная Вирджиния                                                               |         |                |
| 232 30                                               | Северная Каролина                                                                |         |                |
| 237–246                                              | Северная Каролина                                                                | 247–251 | Южная Каролина |
| 252–260                                              | Джорджия                                                                         | 261–267 | Флорида        |
| 589–595                                              | Флорида                                                                          | 268–302 | Огайо          |
| 303–317                                              | Индиана                                                                          | 318–361 | Иллинойс       |
| 362–386                                              | Мичиган                                                                          | 387–399 | Висконсин      |
| 400–407                                              | Кентукки                                                                         | 408–415 | Теннесси       |
| 416–424                                              | Алабама                                                                          | 425–428 | Миссисипи      |
| 587–588                                              | Миссисипи                                                                        | 429–432 | Арканзас       |
| 433–439                                              | Луизиана                                                                         | 440–448 | Оклахома       |
| 449–467                                              | Техас                                                                            | 468–477 | Миннесота      |
| 478–485                                              | Айова                                                                            | 486–500 | Миссури        |
| 501–502                                              | Северная Дакота                                                                  | 503–504 | Южная Дакота   |
| 505–508                                              | Небраска                                                                         | 509–515 | Канзас         |
| 516–517                                              | Монтана                                                                          | 518–519 | Айдахо         |
| 520                                                  | Вайоминг                                                                         | 521–524 | Колорадо       |
| 525                                                  | Нью-Мексико                                                                      | 585     | Нью-Мексико    |

|         |                                                 |         |                    |
|---------|-------------------------------------------------|---------|--------------------|
| 526-527 | Аризона                                         | 528-529 | Юта                |
| 530     | Невада                                          | 531-539 | Вашингтон          |
| 540-544 | Орегон                                          | 545-573 | Калифорния         |
| 574     | Аляска                                          | 575-576 | Гавайи             |
| 577-579 | Вашингтон, О.К.                                 | 580     | Виргинские острова |
| 580-584 | Пуэрто-Рико                                     |         |                    |
| 586     | Гуам, Американское Самоа и Филиппинские острова |         |                    |
| 700-729 | Пенсионный фонд железнодорожников               |         |                    |

Пример: если вы Стэн Сиснерос, проживающий в Бёрлинггейме, Калифорния, и вы родились в 1970 году, ваш SS# мог бы быть 546-28-4197.

# Система назначения и управления объектами (FACS)

**Автор:** Phantom Phreaker

## Введение

Система назначения и управления объектами (Facility Assignment and Control System, FACS) — это интегрированная сетевая компонентная система, о которой большинство фрикеров и хакеров знает из старого файла под названием «FACS FACTS», написанного Sharp Razor. Хотя тот файл содержит точное описание системы FACS, ему недостаёт детализации и объёма. Данная статья предоставит точную информацию о системе FACS и предназначена для настоящего энтузиаста телекоммуникаций (то есть эта статья не для тех, кто пользуется кодами и называет это «фрикингом», и не для тех, кто считает, что фрикинг — это просто «бесплатные звонки»). Надеюсь, что фриеры и хакеры по всему миру, желающие понять, как работает телефонная сеть, извлекут пользу из этой информации. Любое злонамеренное использование данной информации строго запрещено. Содержимое этого файла предназначено исключительно в информационных и образовательных целях.

## Общее описание

FACS можно охарактеризовать как многофункциональную систему назначения объектов внешней кабельной инфраструктуры и центрального офиса. Для тех, кто незнаком с этими терминами: внешняя кабельная инфраструктура (outside plant) — это часть телефонной сети, проходящая от офиса телефонной компании (например, конечного офиса пятого класса, EO) до абонента, включая смотровые люки и точки распределения/доступа, такие как интерфейсы обслуживаемых зон (Serving Area Interfaces, SAI) — большие уличные шкафы с двустворчатыми дверями, позволяющие ремонтным бригадам обслуживать, тестировать и получать доступ к множеству абонентских линий в данном районе.

FACS состоит из пяти компонентных систем (подсистем), часть из которых также используется как самостоятельные системы (то есть в районе, где FACS не применяется, COSMOS можно рассматривать как автономную систему).

Компонентные системы:

- **PREMIS** — PREmise Information System (Информационная система объекта)
- **SOAC** — Service Order Analysis & Control (Анализ и управление заявками на обслуживание)
- **LFACS** — Loop Facility Assignment and Control System (Система назначения и управления объектами абонентской линии)
- **COSMOS** — COmputer System for Main Frame OperationS (Компьютерная система для операций с главным коммутационным оборудованием)
- **WM** — Work Manager (Диспетчер работ)

FACS используется многими подразделениями и рабочими центрами в сети местной телефонной компании (BOC). Далее в статье будет приведён общий пример взаимодействия с телефонной компанией.

## **PREMIS**

PREMIS поддерживает процесс переговоров с клиентом (то есть пока клиент общается с представителем службы BOC, PREMIS — это компьютерная система, к которой имеет доступ представитель) и процесс подготовки заявки на обслуживание (Service Order, SO; SO — это, по сути, запрос на предоставление услуги). PREMIS — компьютерная система хранения и поиска информации, предназначенная для поддержки Центра обслуживания жилых абонентов (Residence/Residential Service Center, RSC), а в ряде случаев — Центра обслуживания корпоративных клиентов (Business Service Center, BSC). RSC обслуживает частных абонентов, BSC — корпоративных.

PREMIS обеспечивает быстрый и удобный доступ к проверке адреса клиента для нумерованных и нenumерованных адресов (информация хранится по номеру телефона, а не по адресу), к статусу телефонной услуги по адресу (подключён ли телефон, отключён, ожидает подключения, ожидает отключения, отключён за неуплату и т.д.), к назначению телефонных номеров для клиентов (PREMIS может сформировать список доступных телефонных номеров в заданной АТС; свободные номера поступают из COSMOS) и к данным о назначении объектов для исходящих заявок.

Следующие функции PREMIS доступны представителям службы и имеют особое значение для центра назначения абонентских линий (LAC):

### **Переговоры с клиентом:**

- Проверка служебного адреса клиента по механизированному справочнику улиц (Street Address Guide, SAG).
- Проверка статуса клиента по механизированному файлу адресов объектов, позволяющая выявить потенциальные условия создания помех (Interfering Station, IS).
- Назначение новых телефонных номеров через файл доступных телефонных номеров (TN).

### **Подготовка заявки на обслуживание:**

- Предоставление данных SAG.
- Обеспечение правильного написания адреса.

PREMIS, насколько мне известно, не имеет прямых коммутируемых подключений, так что не питайте особых надежд. Тем не менее могут существовать другие способы доступа к информации в PREMIS.

## **SOAC**

Система SOAC обеспечивает взаимодействие FACS с процессором заявок на обслуживание BOC (Service Order Processor, SOP). SOP — это система, в которую представители службы вводят данные заявок; SOP передаёт введённые данные в систему SOAC. Система SOAC интерпретирует и проверяет эти входные данные.

SOAC формирует Запросы на назначение (Assignment Requests, AR), которые отправляются в LFACS и COSMOS (см. соответствующие разделы) для запроса назначения объектов внешней кабельной инфраструктуры (OSP) и центрального офиса соответственно.

SOAC получает Ответы на запросы назначения (AR Responses, ARR) от LFACS и WM/COSMOS, объединяет эти данные и форматирует результат в раздел назначения универсальной заявки на обслуживание (Universal Service Order, USO). Эта USO возвращается в SOP после обработки в SOAC.

SOAC возвращает в SOP информацию о статусе и уведомления об ошибках. Статусная информация сообщает представителю службы, введшему данные в SOP, может ли FACS

обработать данную заявку. Уведомления об ошибках отправляются обратно в SOP, когда часть заявки содержит ошибку.

SOAC ведёт учёт статуса и управляющей информации по всем запросам заявок, а также входного образа и конкретных данных, полученных в ходе обработки. Эта информация вместе с входным образом и результатами обработки именуется данными ожидающего назначения.

Заявки не всегда проходят через SOAC автоматически. SOAC может проанализировать заявку и определить, требуется ли ручная помощь; если да, в LAC направляется уведомление о Запросе на ручную помощь (Request for Manual Assistance, RMA). Сотрудники LAC используют SOAC, а при необходимости и другие системы FACS — COSMOS/WM и LFACS — для завершения назначения по этой заявке.

SOAC также может получать выходные данные системы COSMOS от определённых команд. Одной из таких команд может быть команда IJR, переводящая схему в статус «под угрозой» (jeopardy). Статус «под угрозой» означает, что назначение, по всей видимости, будет (или уже является) отстающим от графика выполнения. Пример (показаны сообщения COSMOS):

```
WC% IJR
H ORD nxxxxxxxxx/TN nxx-xxxx/JR nx
RMK NEED TIE PR FOR nxx
-
**ORDER nxxxxxxxxx          HAS BEEN GIVEN JEOPARDY STATUS
  CKTID: TN nxx-xxxx
**JEOPARDY REASON: nx       mm-dd-yy hh:mm
OUTPUT SENT TO SOAC
**IJR COMPLETED   mm-dd-yyy   hh:mm
```

Строка H — это номер заявки, где n может быть буквой, а x — цифрой. TN — затронутый телефонный номер, JR — причина угрозы (Jeopardy Reason), представляющая собой код из одной буквы и одной цифры, RMK — примечание (ReMark); в данном случае требуется соединительная пара. Блок, начинающийся и заканчивающийся двумя звёздочками, — это вывод COSMOS; остальная информация не требует пояснений.

## LFACS

Система LFACS ведёт инвентарный учёт объектов внешней петлевой инфраструктуры: кабелей (CA), кабельных пар (CP), распределительных терминалов, точек соединения, кросс-коммутационных терминалов и подобных вещей, которые должен знать серьёзный фрикер. Кстати, если хотите получить очень хорошую информацию о внешней петлевой инфраструктуре, поищите статью Phucked Agent 04 в первом выпуске технического журнала LOD/H. Это превосходные файлы, и я рекомендую каждому фрикеру прочитать их, если ещё не читали. LFACS также назначает объекты внешней петлевой инфраструктуры для AR, полученных от SOAC в результате активности клиентских заявок. Процесс назначения автоматизирован для 95% запросов на обслуживание.

LFACS предоставляет компьютеризированную версию DPAC и ECCR (карточек назначения выделенных объектов — Dedicated Plant Assignment Cards — и записей об обменных кабельных проводниках — Exchange Cable Conductor Records), которые ранее существовали в виде физических документов, хранившихся в LAC. В DPAC содержится информация, например, о распределительном терминале жилой единицы и выделенных петлевых объектах жилой единицы; ECCR содержит данные о выборе пар, счётчике добавления/разрыва, переносе линии и станции, а также информацию о рабочих нарядах (WO). Часть этой информации может использоваться бюро полевой помощи LAC для содействия бригадам внешней инфраструктуры в получении необходимых сведений.



Когда условия для автоматического ответа LFACS на AR от SOAC не выполнены, в LAC генерируется уведомление RMA. Соответствующие сотрудники LAC взаимодействуют с LFACS, а при необходимости — с SOAC и WM/COSMOS для завершения процесса назначения.

## COSMOS

О COSMOS написано немало, поэтому я не буду подробно останавливаться на этой системе, так как многие уже знакомы с ней.

COSMOS ведёт базу данных инвентаризации объектов центрального офиса (таких как TN, CP, OE, CS, BL — телефонный номер, кабельная пара, офисное оборудование, класс обслуживания, мостовой разъединитель соответственно) и назначает эти объекты для AR, полученных от SOAC в результате активности клиентских заявок.

COSMOS помогает Центру сетевого администрирования (Network Administration Center, NAC) и Центру управления кроссировками (Frame Control Center, FCC) в управлении и эксплуатации главного распределительного фрейма (MDF) и оборудования центрального офиса (COE), а также объектов и цепей центрального офиса. COSMOS выполняет назначение телефонных номеров, линейного оборудования, управление использованием/повторным использованием перемычек, управление точками тестирования (TP), управление работами на фрейме и другие подобные функции.

Когда условия для ответа COSMOS на AR от SOAC не выполнены, в LAC генерируется RMA (как и в случае с другими системами, описанными в этой статье). LAC может затем использовать WM/COSMOS, SOAC и LFACS для завершения назначения.

## WM

WM обеспечивает связь между одним комплектом систем SOAC/LFACS и одной или несколькими системами COSMOS. Все входные данные в COSMOS из LAC направляются через WM. WM обеспечивает коммутацию сообщений, управление нагрузкой и другие функции для LAC.

---

-EOF-

RC:LINE;CHNG!/ORD 1/TN LOD-LOD-LODH/ESM YES/ESX YES/ESL YES/RC:TRK!/TNN \$LOD\$.

---

Надеюсь, что информация, изложенная в этой статье, оказалась интересной для всех читателей. Я не включил столько информации, сколько мог бы, — часть конфиденциальных сведений была намеренно опущена, поскольку их раскрытие могло бы вызвать проблемы. Моя личная благодарность адресована замечательным людям, разработавшим систему FACS, а также всем телефонным компаниям, ибо без вас не было бы телефонных фрикеров. Спасибо, что открываете нам доступ к своим сетям, пусть этот доступ и берётся, а не даётся. Попробуйте как-нибудь нанять фрикера — это может оказаться полезным.

Замечание для энтузиастов телекоммуникаций и компьютеров, прочитавших эту статью: НЕ ЛОМАЙТЕ НИЧЕГО! ЕСЛИ ВЫ НЕДОСТАТОЧНО ОТВЕТСТВЕННЫ, ЧТОБЫ ИСПОЛЬЗОВАТЬ ЭТИ ДАННЫЕ РАЗУМНО И БЕЗ ЗЛОУПОТРЕБЛЕНИЙ — НЕМЕДЛЕННО УНИЧТОЖЬТЕ ЭТУ СТАТЬЮ И ДЕЛАЙТЕ ВИД, ЧТО НИКОГДА ЕЁ НЕ ЧИТАЛИ.

---

*Это была презентация THE LEGION OF DOOM! (C) 1988+*

# Редакционная статья Phrack о «микробэшинге»

**Автор:** The Nightstalker

---

Я развлекался идеей написать историю Революции Микрокомпьютеров — глазами человека, пережившего её изнутри, пожалуй, с воспоминаниями телекоммуникационного энтузиаста в качестве приправы.

Однако, поразмыслив, я решил воспользоваться этой трибуной, чтобы обратиться к проблеме, которая беспокоила меня уже давно. Я имею в виду явление, которое можно назвать «микробэшингом».

По моему мнению, это серьёзная проблема в МикроПодполье.

Для справки: мне 36 лет, я копаюсь с компьютерами — мейнфреймами, мини-ЭВМ и микрокомпьютерами — с 1976–1977 годов. В своё время я собрал Altair 8800 и написал то, что, возможно, было первой программой для пиратства программного обеспечения. (Нечто, массово копировавшее на бумажную ленту Altair BASIC Билла Гейтса.) Ещё я собрал TV Typewriter по схемам Дона Ланкастера и 100-бодный модем в дополнение к нему. К слову, сейчас я пользуюсь компьютером Commodore 64: у меня есть модем на 1200 бод, два дисководов, приличный принтер и цветной монитор. Ради записи: я продал Apple IIe, чтобы купить C64. Я ни разу не пожалел об этом решении.

И вот найдутся те, кто прочитает последнее предложение и скажет себе: «Чёртов коммодоровец! Он ПРОДАЛ Apple ради Коммодора? Что за идиот!» Тогда я мог бы ответить пользователю Apple IIe, думающему так: «Бедняга! Ты потратил кучу денег на IIe! Плюс ещё кучу на платы расширения, чтобы он умел то, что в моём C64 встроено с завода? Ну дела! Некоторым людям нужны нянечки!»

Вот это, уважаемые читатели, и есть микробэшинг. Таким образом, за несколько минут этот гипотетический диалог породил взаимную неприязнь, если не откровенную враждебность. Какая трата времени и сил! У нас обоих мощные компьютеры, о существовании которых я не мог даже мечтать 12 (12!) лет назад. В моём Altair было 16 килобайт ОЗУ, и я считал это верхом крутизны! У большинства людей в их самодельных микро стояло лишь 4–8 килобайт. У меня даже был дисковод! Огромный монстр весом в 20 фунтов, работавший с односторонними 8-дюймовыми дисками объёмом всего 120 килобайт. Вся система вместе с TeleType (моим терминалом-принтером) стоила около 5000 долларов в ценах 1977 года — примерно 15 000 долларов в ценах 1988-го. (Мой маленький C64, полная стоимость которого меньше 1000 долларов, просто уничтожает тот Altair с TeleType.)

## Каковы корни микробэшинга?

Я не уверен, но вот некоторые мысли.

**Статус**, я уверен, играет главную роль в микробэшинге. C64/128 всегда будет стоить меньше эквивалентной системы на Apple IIe. «Мой компьютер стоит дороже твоего! Значит, мой компьютер лучше! Вот!» По такой логике мой старый Altair за 5000/15000 долларов лучше большинства машин Apple. Явная нелепость, не правда ли? (Я заметил, что среди владельцев Mac Plus, SE и II, а также пользователей //gs теперь формируется субкультура «Долой IIe». Должен признаться, я испытываю от этого извращённое удовольствие. Теперь другой человек оказался в той же шкуре, не так ли?)

**Конформизм**, особенно среди подростков и молодых взрослых, тоже может быть фактором. «Все серьёзные люди используют Apple. Только геймеры используют дешёвые игрушки из K-Mart. Если у

тебя нет Apple — ты никто!» Давление конформизма — мощная вещь.

Мой приятель из отдела вычислительного обслуживания Гарварда держит Mac II на рабочем столе в офисе и Mac Plus дома. У другого друга — клон Zenith AT в кабинете в корпорации Mitre в Мэриленде и Apple ][+ дома. У хорошего знакомого, редактора крупного издания на дисковых носителях, есть //gs, подаренный Apple. Все эти парни — мощные пользователи компьютеров. Гарвардец — их UNIX-гуру. Человек из Мэриленда — государственный служащий GS-13, работающий на BBC в качестве универсального специалиста по MS-DOS/ADA, который только что вложил миллион долларов в финансирование исследований по распределённым вычислениям в Лос-Аламосе. Последний — редактор раздела Apple в этом издании. Ни один из них не тратит ни секунды на то, чтобы уничижительно отзываться о моём C64. Если эти люди считают меня коллегой, равным (а они так и считают!), и им всё равно, какой компьютер я использую, — почему некоторые пользователи //e тратят время и энергию на унижение C64?

**Третьим фактором** может быть тайное подозрение: «Ёлки! Если C64 умеет всё это, зачем я потратил столько денег на Apple?» Вина и самосомнение могут быть мощным двигателем микробэшинга. «Если я буду достаточно унижать Коммодоров, может, другие люди тоже купят Apple, и тогда я не буду единственным, у кого он есть». Психологи называют это «переносом» — перенесением негативных чувств и сомнений в себе на что-то другое с последующим унижением этого другого. Ветхий Завет именует это «козлом отпущения».

---

Полагаю, что в итоге я пытаюсь сказать следующее: давайте все повзрослеем и прекратим эту глупую перепалку и мелкие уколы. Никто не выигрывает, а проигрываем мы все. Мы теряем время, информацию, дисковое пространство на BBS, общение и удовольствие! Мне не нравится видеть, как пользователь Apple нападает на Commodore. Мне также не нравится видеть, как пользователь C64 нападает на пользователя TI, — так же как мне не нравится наблюдать, как этот пользователь TI издевается над владельцем Adam. Неужели вы думаете, что нам нечем больше заняться, чем раздувать из мухи слона применительно к нашим компьютерам?

У меня — есть. Если мы не можем вести себя лучше, чем детсадовский ребёнок, ноющий из-за игрушки, то, может быть, мы и не заслуживаем этих мощных инструментов, стоящих на наших столах.

---

*Написано THE NIGHTSTALKER, июнь 1988 г.*

# Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN
PWN      >>>>>--* Phrack World News *--<<<<< PWN
PWN                        Issue XVIV/1          PWN
PWN
PWN                        Created by Knight Lightning PWN
PWN      Written and compiled by Knight Lightning PWN
PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

**Автор:** Knight Lightning

---

## Проект «Феникс»

---

Что такое «Проект Феникс»?

**Феникс** (fe/niks), сущ. Уникальная мифическая птица редкостной красоты, по преданию живущая 500–600 лет, сжигающая себя дотла и восстающая из пепла в юношеской свежести, чтобы прожить новый жизненный цикл.

**Проект** (proj/ekt), сущ. Нечто задуманное, разработанное или спланированное. Крупное или масштабное начинание. Долгосрочное задание.

---

Зачем нужен «Проект Феникс»?

1 июня 1987 года Metal Shop Private, казалось, навсегда ушла в небытие без каких-либо шансов на возрождение, однако идеалы и сообщество, сформировавшееся вокруг этого знаменитого очага знаний, продолжали жить. 19–21 июня 1987 года мир фрикеров и хакеров пережил SummerCon'87 — событие, объединившее значительную часть сообщества: кто-то присутствовал на конвенте лично, кто-то — духовно. 22 июля 1987 года сообщество фрикеров и хакеров было разгромлено в результате общенационального удара со стороны всевозможных охранных структур и правоохранительных органов — так было запущено в действие уничтожение сообщества в том виде, в каком мы его знали. Несмотря на события 22 июля 1987 года, PartyCon'87 состоялся в запланированные сроки — 26–28 июля 1987 года — как очевидное последнее собрание оставшихся на континенте свободных хакеров; им ещё не было известно, что мир, который они стремились защитить, уже уничтожен. С 1 августа 1987 года все первоначальные участники и сотрудники Metal Shop Triad и Phrack Inc. приняли решение исчезнуть в надежде вернуться однажды, когда всё будет как прежде...

## ТОТ ДЕНЬ НАСТАЛ...

Начинается новое тысячелетие, и всё начинается 22 июля 1988 года. Символично, что годовщина разрушения сообщества фрикеров и хакеров совпадёт с днём его возрождения.

Объявляем SummerCon'88 в (где же ещё?) Сент-Луисе, штат Миссури!

Знание — ключ к будущему, и оно свободно. Телекоммуникационная и охранные отрасли больше не смогут удерживать право на обучение, право на исследование и право на знание. Новая эпоха наступила, и с использованием всех доступных **ЗАКОННЫХ** средств молодёжь сегодняшнего дня сможет учить молодёжь завтрашнего.

---

SummerCon'88 — это праздник нового начала. В настоящее время ведётся подготовка к тому, чтобы конвент этого года был вдвое интереснее прошлогоднего, и чем больше участников, тем грандиознее он будет. Никто не отстранён от участия в торжествах, и распространение нелегальной информации не является частью этого конвента (вопреки мнению San Francisco Examiner — они, кстати, даже не присутствовали на прошлом). Все желающие принять участие в конвенте этого года должны немедленно написать Crimson Death, чтобы мы могли лучше спланировать мероприятие с учётом точного числа участников.

Гостиничные номера, приобретённые для SummerCon'88, предназначены исключительно для приглашённых гостей. Специалисты по безопасности и сотрудники правоохранительных органов, желающие присутствовать, должны как можно скорее связаться с оргкомитетом для получения официального приглашения на конвент.

Приносим извинения за короткое уведомление в этом году...

:Knight Lightning — «Будущее вечно»

# Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN
PWN      >>>>>==* Phrack World News *==<<<<< PWN
PWN              Issue XVIV/2 PWN
PWN
PWN              Created by Knight Lightning PWN
PWN              Written and compiled by Epsilon PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

**Автор:** Epsilon (составитель), Knight Lightning (создатель)

---

## Doc Holiday в юридических неприятностях

Однажды ночью Doc Holiday 713 решил наведаться на свою АТС. Здание было окружено забором с колючей проволокой наверху. Он перелез через забор без труда и обошёл периметр здания в поисках камер видеонаблюдения. Убедившись, что камер нет, он решил войти через чёрный ход. К своему удивлению, чёрный ход оказался незаперт [Что ж, по крайней мере ему не предъявили обвинение во взломе и проникновении, правда? — Epsilon], и он вошёл в здание. Немного осмотревшись — мимо ящиков с тест-сетями и кабелями — он заскучал и направился в комнату с терминалами и большой панелью управления. Инструкции по работе с терминалом были приклеены скотчем сбоку стола, и он их опробовал. Он с удовольствием поотслеживал телефонные линии и проверил тональный набор других абонентов, после чего решил покинуть здание.

На выходе он наткнулся на ящик с надписью примерно «Коммутационный блок». Он не стал заглядывать внутрь — торопился уйти — и предпочёл забрать ящик домой, чтобы там осмотреть. Когда он открыл дверь, чтобы выйти, он заметил фонарик, мелькающий в темноте. Он испугался и поставил ящик на землю [Кстати, дверь, через которую он вошёл, находилась наверху лестничного пролёта сзади здания, снаружи. — Epsilon]. Ящик не устоял на месте и скатился по ступенькам, скорее всего повредив то, что было внутри. Он попытался сбежать вниз по лестнице и перелезть через забор, но обнаружил, что снаружи его ждут полицейские. Он бросился бежать. Полицейский крикнул ему остановиться и пригрозил стрелять — и он лёг на землю. Его задержали и доставили в полицейский участок.

Выяснилось, что полиция знала о его местонахождении, потому что он сработал бесшумную сигнализацию — предположительно, ещё при входе в здание.

На участке его допрашивали. Устав от этого, он заявил, что уходит. Когда он направился к выходу, полицейский схватил его и коленом сломал ему ребро. После некоторых уговоров Дос всё же был доставлен в больницу.

Сейчас он дома и ожидает слушания. Этот инцидент, по всей видимости, не скажется на его хакерской деятельности.

*Информация предоставлена Doc Holiday*

---

## The Disk Jockey... Задержан!

The Disk Jockey, которого все мы знали, был арестован в прошлую пятницу по 22 статьям о пособничестве мошенничеству и ряду других обвинений. В данный момент он находится под стражей, залог составляет 150 000,00 долларов [Да, всё верно. Сто пятьдесят тысяч долларов. — Epsilon].

По имеющимся сведениям, причиной инцидента послужил некий «фрикер» по прозвищу White Lightning (616), который сообщил в службу безопасности Sprint, что The Disk Jockey незаконно пользовался их услугами.

Сейчас он ожидает даты судебного заседания и недоступен для комментариев.

*Информация предоставлена Compaq (219)*

---

## SummerCon '88

Мы, команда Phrack Inc., с гордостью представляем SummerCon '88. Конвенция состоится в Westport Ramada Inn в Сент-Луисе, штат Миссури, в выходные 22 июля. Ожидается, что мероприятие пройдёт с пятничного полудня до воскресного полудня. Если вы планируете присутствовать, свяжитесь с нами через аккаунты Phrack или через Phrack In. VMS по номеру (800)331-8477, \* #, доб. 6660. На этом CON не приветствуется распространение незаконной информации. Спасибо.

*Информация предоставлена Knight Lightning*

---

## PWN Коротко

---

Первый шаг так называемого The Phoenix Project — возрождения хак/фрик-сообщества — уже сделан. Этот первый шаг — публичная образовательная BBS, посвящённая обучению общества основам телекоммуникаций и компьютерных систем. Доска называется The Phoenix Project, номер: (512)754-8182. Размещение незаконной информации на этой системе запрещено. Наш SysOp — The Mentor. Спасибо, и звоните, если интересно.

*Информация предоставлена The Mentor*

---

По слухам, в хак/фрик-сообществе формируется новая группа. Она ищет около восьми опытных участников с разнообразными интересами. Если вы считаете себя подходящим кандидатом и заинтересованы — свяжитесь с Doc Holiday на любой BBS, где он присутствует. Спасибо.

---

Control C из 313 **не был** задержан, вопреки расхожему мнению. Это — большая путаница, и мы расскажем, как она возникла, в одном из следующих выпусков. До тех пор, пожалуйста, не распространяйте этот слух.

---