Phrack RU issue 027

Русская версия Phrack, выпуск 027. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; Unix/Linux, BSD, Windows NT и администрирование систем; сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура.

Материалы выпуска: Содержание; Работа с IBM VM/SP CP; Введение в MIDNET; Список NUA для сетей Datex-P и X.25; COSMOS — Компьютерная система для обслуживания мейнфреймов. Часть вторая; Исследование сети DECNET; Становление хакера; Отправка поддельной почты в Unix; Служба почтовой инспекции; Phrack World News; Phrack World News — Мировые новости Phrack; Один из «хитрых хакеров» Клиффорда Столла мёртв (самоубийство?).

Больше крутых материалов в моём телеграм канале @grogrigs

Содержание

Автор: Taran King и Knight Lightning

20 июня 1989 года

Приветствуем вас на страницах 27-го выпуска Phrack Inc. Мы работали под давлением — через каких-то пару дней стартует SummerCon '89. Приносим извинения за то, что этот выпуск так долго выходил: летние каникулы повлекли за собой куда больше обязанностей и плотный распорядок дня, с которым нам никогда не приходилось иметь дело во время учёбы. И всё же, думаем, вы согласитесь: выпуск того стоил.

В этом номере мы представляем обновлённый список NUA и Datex-P от Oberdaemon из Швейцарии, а также седьмую главу «Саги о будущем трансцендентном» (учитывая, что файлы о SPAN и NSFnet являлись главами 5 и 6). Кроме того, публикуется вторая часть материала о COSMOS, написанного King Arthur.

Прежде чем перейти к основному содержанию выпуска, хотим сделать несколько замечаний относительно безопасности и доступа Phrack Inc. в Интернет.

Благодаря одному другу мы в Phrack Inc. узнали об одном из главных методов, которые Агентство национальной безопасности (АНБ) применяет для слежки за глобальными сетями.

В определённые сообщения, рассылаемые некоторыми государственными ведомствами, включены специальные номера телефонов — в частности, WATS (800)-номера. Пока эти сообщения распространяются по всему континенту через различные системы сетевой почты и передачи файлов, они проходят через несколько станций слежения. Все эти станции выполняют одну функцию — в терминах Unix она называется «grep».

Grep расшифровывается как G>lobal R>egular E>xpression search and P>rint (глобальный поиск и вывод по регулярному выражению). Grep выполняет простое сопоставление строк. Каждое вхождение таких специальных 800-номеров в почтовом сообщении (или их пакете) помечается, записывается, и запись пересылается на определённые станции слежения в разведывательные органы.

Вот сети, в которых, по нашим достаточно обоснованным предположениям, подобная практика применяется:

• **USEnet**: Электронная почта проверяется лишь в отдельных местах, однако ВСЕ новости (включая alt и любые другие нестандартные группы новостей) помечаются единственным правительственным доменом на базе SUN-3, название которого мы не называем.
• **ARPAnet**: Всё письма, проходящие через стандартный интернет-контроллер BBN (Bolt, Bernack and Neumann — ответвление от Кембриджа/MIT), будут помечены, однако контроллер записывает лишь TCP/IP-адреса источника и получателя. Но стоит учесть, что речь идёт о ***ВСЕХ*** списках рассылки DARPA — тогда масштаб становится очевиден. Причина, по которой более подробная информация НЕ записывается, состоит в том, что эта сеть — единственное АВТОРИЗОВАННОЕ место, где подобные сообщения с горячими WATS-номерами должны появляться. Что это означает, вы поймёте чуть позже.
• **BITnet**: Крупный IBM-мейнфрейм с незадействованными циклами каналов ввода-вывода без труда справится со сканированием почты одной из наиболее открыто доступных «бесплатных» сетей.
• **Fidonet**: Секретная служба просматривает её в поисках данных кредитных карт и других нарушений. Им не составит труда заодно проверять и наличие (800)-номеров.

• **W.Union**: Все международные телексные линии сканируются на предмет большого числа признаков — прежде всего информации, связанной с наркотиками. Указанные телефонные номера тоже внесены в их список.

У нас есть и другие подозрения, но пока мы их придержим.

Другая новость столь же тревожна, поскольку касается нас напрямую. Мы временно лишаемся сетевого доступа. С 27 июня 1989 года по 28 августа 1989 года у нас не будет доступа к нашим учётным записям на мейнфрейм-системе UMCVMB. Просим не пытаться написать нам по адресам там вплоть до 28 августа 1989 года. Впрочем, у каждой тучи есть серебряная подкладка — и этот случай не исключение. Для тех, кто работает с сетями и хочет прислать файлы в Phrack Inc. в этот период, мы с гордостью представляем нашего друга и соратника — Hatchet Molly. С ним можно связаться по адресу `TK0GRM2@NIU.BITNET` и/или `TK0GRM2%NIU.BITNET@CUNYVM.CUNY.EDU`.

Итак, выпиваем за ещё один великолепный выпуск Phrack Inc.!

```
Taran King                          Knight Lightning

                    Hatchet Molly
                 TK0GRM2@NIU.BITNET
          TK0GRM2%NIU.BITNET@CUNYVM.CUNY.EDU
```

Работа с IBM VM/SP CP

(IBM Virtual Machine System Product — управляющая программа)

Автор: Taran King

18 мая 1989 года

Цель данной статьи — разобраться в устройстве управляющей программы (CP) системы IBM VM/SP. По сути, CP — это отдельный уровень VM/CMS (в полноэкранных редакторах уровень CP отображается в правом нижнем углу экрана; в построчных редакторах надпись "CP" появляется перед командной строкой и после нажатия Enter). Задача CP — управление реальными ресурсами системы. Любая команда, требующая доступа к чему-либо за пределами вашей виртуальной машины, должна передаваться через CP. Если CMS не распознаёт введённую вами команду, она автоматически передаётся в CP.

Обычно пользователь попадает на уровень CP после сбоя программы или после разрыва соединения. Перейти в режим CP можно также нажатием клавиши PA1, которая является функциональной клавишей. В режиме онлайн PA1 переключает между CP и CMS; при повторном входе после разрыва соединения PA1 можно использовать наряду с командой BEGIN, о которой рассказывается ниже.

Как правило, VM/CMS-системы хорошо оснащены справочными файлами. Если что-то из изложенного покажется вам неясным, из режима CMS введите HELP CP XXX, где XXX — интересующая вас CP-команда.

В начале статьи я привожу таблицу IBM-определённых классов и типов функций из руководства IBM VM/SP CP. По ней можно определить, какими привилегиями обладает пользователь с тем или иным назначенным классом.

```
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
IBM-Defined      Function         User &
   Class           Type          Functions
~~~~~~~~~~~      ~~~~~~~~       ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     A               O           Operations:  The primary sysop can issue all
                                 class A commands.  The class A user controls
                                 the VM/SP system.  Class A is assigned to the
                                 user at the VM/SP system console during IPL.
                                 The primary sysop is responsible for the
                                 availability of the VM/SP system and its
                                 communication lines and resources.  In
                                 addition, the class A user controls system
                                 accounting, broadcast messages, virtual
                                 machine performance options, and other
                                 command operands that affect the overall
                                 performance of the VM/SP.  The sysop controls
                                 operation of the real machine using the
                                 system control panel and console device.
                                 NOTE:  The class A sysop who is automatically
                                 logged on during CP initialization is
                                 designated as the primary sysop.

     B               R           Resource:  The system resource operator can
                                 issue all class B commands.  The class B user
                                 controls allocation and deallocation of all
                                 the real resources of the VM/SP system,
                                 except those controlled by the primary sysop
                                 and spooling operator.

     C               P           Programmer:  The system programmer can issue
                                 all class C commands.  The class C user
```

```
                                updates certain functions of the VM/SP
                                system.  The system programmer can modify
                                real storage in the real machine.

      D              S          Spooling:  The spooling operator can issue
                                all class D commands.  The class D user
                                controls spool data files and specific
                                functions of the system's unit record
                                equipment.

      E              A          Analyst:  The system analyst can issue all
                                class E commands.  The class E user displays
                                the contents of real storage, performs the
                                functions required to generate saved systems
                                and discontiguous saved segments, and
                                controls the collecting and recording of
                                performance measurement data.  This class of
                                user can display specified real storage areas
                                on the virtual operator's console or on a
                                spooled virtual printer, but cannot modify
                                real storage.

      F              C          Customer Engineer:  The service
                                representative can issue all class F
                                commands.  The class F user obtains, and
                                examines, in detail, certain data about input
                                and output devices connected to the VM/SP
                                system.  The service representative can
                                establish extensive recording mode for one
                                I/O device at a time and can cause the
                                recording of repressible machine check errors
                                to be initiated or resumed.

      G              G          General:  The general user can issue all
                                class G commands.  The class G user controls
                                functions associated with the execution of
                                his virtual machine.  A general user cannot
                                display or modify real storage.

     ANY            ANY         The ANY classification is given to certain CP
                                commands that are available to any user.
                                These are primarily for the purpose of
                                gaining and relinquishing access to the VM/SP
                                system.

  ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
```

Ниже приведён перечень доступных команд с кратким описанием их назначения, формата и соответствующего IBM-определённого класса с типом функции.

---

* (звёздочка)

Из CP можно использовать команду для добавления комментария в журнал терминальной консоли или на экран терминала. Иными словами, введите и следом — любую строку символов, которую вы хотите видеть на экране.

Класс привилегий: ANY
Тип функции: N/A

#CP

Эта команда используется для выполнения CP-команды из среды команд виртуальной машины без предварительного сигнала перехода в командную среду CP. Это означает, что при наборе `#CP` CP получает команду непосредственно, тогда как `CP` лишь ставит команду в очередь CP.

Класс привилегий: ANY
Тип функции: ANY

ACNT

Команда ACNT используется для создания учётных записей для вошедших в систему пользователей и сброса учётных данных. Кроме того, она закрывает спул-файл, в котором накапливаются учётные записи.

Класс привилегий: A
Тип функции: O

ADSTOP

Команда ADSTOP используется для остановки выполнения виртуальной машины в заданной точке виртуальной инструкции. После слова ADSTOP можно указать переменную hexloc — шестисимвольное шестнадцатеричное представление виртуального адреса инструкции, на которой должно остановиться выполнение. Параметр OFF команды ADSTOP отменяет любую ранее установленную точку останова.

Класс привилегий: G
Тип функции: G

ATTN

Команда ATTN используется для выставления в очередь прерывания по вниманию на вашей виртуальной консоли.

Класс привилегий: G
Тип функции: G

AUTOLOG

Эта команда позволяет пользователю войти в любую виртуальную машину, описанную в директории.

Класс привилегий: A, B
Тип функции: O

BACKSPAC

Команда BACKSPAC используется для перезапуска или перепозиционирования текущего вывода на реальном перфораторе или принтере.

Класс привилегий: D
Тип функции: S

BEGIN (или B)

Команда BEGIN, введённая без параметров из режима CP, возвращает пользователя в режим CMS в том месте, где он находился до разрыва соединения или перехода в CP. За командой BEGIN также может следовать шестнадцатеричный адрес, указывающий точку, с которой следует продолжить выполнение, если пользователь хочет начать с другого места.

Класс привилегий: G
Тип функции: G

CHANGE (или CH)

Команда CHANGE используется совместно с подкомандами и переменными. Как правило, переменная "name" имеет длину от 1 до 4 символов. Ниже перечислены подкоманды с описанием функций и форматов:

• **READER или RDR** — изменяет спул-файлы считывателя.
• **PRINTER или PRT** — изменяет спул-файлы принтера.
• **PUNCH или PCH** — изменяет спул-файлы перфоратора.
• **CLASS c1** — задаёт существующий класс, где c1 — односимвольное буквенно-цифровое поле от A до Z или от 0 до 9.
• **spoolid** — идентификационный номер спул-файла, подлежащего изменению.
• **FORM form1** — буквенно-цифровое имя формы длиной от 1 до 8 символов для выбора изменяемых файлов (form1).
• **ALL** — изменяет все ваши спул-файлы.
• **HOLD** — запрещает печать, перфорацию или считывание файла до его освобождения.
• **NOHOLD** — снимает с указанного файла статус HOLD пользователя.
• **DIST dist** — изменяет дистрибутивный код на переменную "dist".
• **COPY(*)nnn** — задаёт количество копий файла для спулинга; действительно только для файлов принтера или перфоратора. "nnn" — число от 1 до 255; символ "*" используется в случае применения принтера 3800, чтобы копии изготавливались внутри принтера.
• **FLASH name nnn** — указывает, что наложение форм, содержащееся в принтере 3800, должно быть суперпозиционировано на определённые страницы вывода. "nnn" — число от 0 до 255, означающее количество суперпозиционируемых копий.
• **MODIFY name (n)** — позволяет изменять текст, запрещая вывод информации или добавляя метки к выводу. "n" выбирает ключевое слово в CHARS для текста модификации копии.
• **CHARS name1 (name2(name3(name4)))** / **CHARS name1(CH names2(CH names3(CH names4)))** — задаёт таблицу размещения символов при печати файла. Допускается до 4 имён.

• **FCB name** — управляет вертикальным интервалом вывода на странице.
• **FORM form2** — изменяет имя спул-формы файла на form2.
• **NAME fn (ft)** — присваивает идентификатор спул-файлу в формате CMS (имя файла и тип файла).
• **NAME dsname** — присваивает идентификатор спул-файлу в формате, отличном от CMS, где "dsname" — от 1 до 24 символов, подходит для OS- или DOS-файлов.

Класс привилегий: S, G
Тип функции: D, G

CLOSE (или C)

Команда CLOSE завершает спулинг на любом виртуальном спулированном устройстве с единичной записью или консольном устройстве. После буквы C или слова CLOSE используются следующие подкоманды:

• READER или RDR
• PRINTER или PRT
• PUNCH или PCH
• FORM form1
• HOLD
• NOHOLD
• DIST dist
• NAME fn (ft)
• NAME dsname
• **vaddr** — виртуальный адрес (cuu) закрываемого устройства.
• **CONSOLE** — закрывает спул-файл консоли виртуальной машины, преобразуя его в спул-файл принтера.
• **PURGE** — закрывает и немедленно уничтожает выходные спул-файлы виртуальной машины. Выходной файл не создаётся.
• **CHAIN** — действительна только для VM/SP HPO Release 4.2 и PRPQ улучшений спул-файлов Profs. Указывает, что файл перфоратора должен быть сцеплен.

Класс привилегий: G
Тип функции: G

COMMANDS (или COMM)

Используйте COMMAND для получения списка команд и кодов диагностики, разрешённых к использованию.

Класс привилегий: ANY
Тип функции: ANY

COUPLE

Команда COUPLE логически соединяет ваше виртуальное недикатированное устройство с канальной связью (channel-to-channel) с виртуальным устройством другого пользователя того же типа или с другим вашим виртуальным устройством того же типа. Формат команды: `COUPLE vaddr1 TO userid vaddr2`. Переменная vaddr1 — ваш виртуальный адрес; переменные userid vaddr2 идентифицируют userid и виртуальный адрес подключаемого пользователя.

Класс привилегий: G
Тип функции: G

CP

Команду CP можно ставить перед обрабатываемой командой, хотя это не обязательно. Как правило, команда CP используется из режима CMS для постановки CP-функций в очередь путём набора `CP` .

Класс привилегий: ANY
Тип функции: ANY

CPTRAP

Команда CPTRAP создаёт reader-файл из выбранной таблицы трассировки, интерфейса CP и записей интерфейса виртуальной машины для диагностики проблем.

Класс привилегий: C
Тип функции: P

DCP

Эта команда отображает содержимое реальных областей хранения на терминале.

Класс привилегий: C, E
Тип функции: P

DEFINE (или DEF)

Команда DEFINE в CP используется для изменения конфигурации виртуальной машины или режима работы канала. Существует ОЧЕНЬ много подкоманд, применяемых вместе с DEFINE, таких как RDR, PRT, PCH и других. Если вам нужны подробности, воспользуйтесь справкой (HELP CP DEF) — это почти 600 строк детального описания каждой подкоманды.

Класс привилегий: B, G
Тип функции: R, G

DETACH (или DET)

Команда DETACH используется для удаления виртуального устройства из виртуальной машины. Подкоманды:

• **vaddr (vaddr...)** — используется для отключения нескольких адресов; vaddr — виртуальный адрес (cuu) отключаемого устройства.
• **vaddr-vaddr** — используется для отключения диапазона адресов.
• **CHANNEL c** — отключает реальный адрес канала.

Класс привилегий: B, G
Тип функции: R, G

DIAL

Команда DIAL логически подключает коммутируемую, выделенную, локально подсоединённую или удалённую BSC-терминал (Binary Synchronous Communications) к ранее вошедшей в систему многопользовательской виртуальной машине. Формат: `DIAL userid (vaddr)`, где userid — идентификатор пользователя для подключения, а vaddr — необязательный виртуальный адрес.

Класс привилегий: ANY
Тип функции: ANY

DISABLE

Команда DISABLE запрещает низкоскоростным коммуникационным линиям доступ к системе.

Класс привилегий: A, B
Тип функции: R

DISCONN (или DISC)

Команда DISCONNECT используется для отключения терминала от системы при продолжении работы виртуальной машины. Параметры DISC HOLD или DISC HO указывают, что коммуникационная линия не должна отключаться, что позволяет избежать повторного набора номера при следующем входе.

Класс привилегий: ANY
Тип функции: ANY

DISPLAY (или D)

Команда DISPLAY позволяет отображать компоненты виртуальной машины на вашем терминале. В зависимости от переменной, следующей за D или DISPLAY, можно отобразить: виртуальные области хранения, ключи хранения, регистры общего назначения, регистры с плавающей точкой, управляющие регистры, векторные регистры, VAC (счётчик векторной активности), VSR (регистр векторного статуса), VMR (регистр векторной маски), PSW (слово состояния программы), CAW (слово адреса канала) и CSW (слово состояния канала).

Класс привилегий: G
Тип функции: G

DMCP

Эта команда печатает содержимое реальных областей хранения на виртуальном спулированном принтере пользователя.

Класс привилегий: C, E
Тип функции: P

DRAIN

Команда DRAIN останавливает операции спулинга на устройствах считывания указанного реального устройства после завершения обработки текущего файла.

Класс привилегий: D
Тип функции: S

DUMP (или DU)

Команда DUMP печатает содержимое различных компонентов виртуальной машины на виртуальный спулированный принтер. В зависимости от переменной после DUMP или DU, распечатываются: виртуальное PSW (слово состояния программы), регистры общего назначения, регистры с плавающей точкой, управляющие регистры, ключи хранения и виртуальные области хранения.

Класс привилегий: G
Тип функции: G

ECHO (или EC)

По умолчанию равна 1; команда ECHO переводит терминал в режим эха, при котором любая введённая строка передаётся обратно на терминал в неизменном виде указанное количество раз в соответствии со значением переменной, следующей непосредственно за словом ECHO или EC.

Класс привилегий: G

Тип функции: G

ENABLE

Используйте команду ENABLE для включения ранее отключённых или нераспознанных устройств, чтобы пользователи могли получить доступ к системе.

Класс привилегий: A, B
Тип функции: R

EXTERNAL (или EXT)

Команда EXTERNAL позволяет пользователю имитировать внешнее прерывание виртуальной машины и вернуть управление этой машине. Шестнадцатеричный код после слова EXTERNAL или EXT связывается с внешним прерыванием; по умолчанию используется число 40, соответствующее кнопке внешнего прерывания на системной консоли.

Класс привилегий: G
Тип функции: G

FLUSH

Команда FLUSH останавливает и немедленно уничтожает с переводом в статус ожидания текущий вывод на указанном устройстве с единичной записью.

Класс привилегий: D
Тип функции: S

FORCE

Эта команда принудительно выполняет выход любого пользователя из системы.

Класс привилегий: A
Тип функции: O

FREE

Используйте команду FREE для снятия системного статуса ожидания с набора спул-файлов указанного пользователя.

Класс привилегий: D

Тип функции: S

HALT

Команда HALT завершает любую активную программу канала на указанном реальном устройстве.

Класс привилегий: A
Тип функции: O

HOLD

Команда HOLD помещает спул-файлы пользователя в системный статус ожидания.

Класс привилегий: D
Тип функции: S

INDICATE (или IND)

Команда INDICATE позволяет отобразить на терминале использование основных системных ресурсов и конкуренцию за них. Переменные после слова INDICATE или IND выводят следующие данные:

• **LOAD** — показывает количество пользователей в очереди 1 и очереди 2, использование реального хранилища и соотношение активных пользователей к обслуживаемым. Возвращаемые значения характеризуют рабочую нагрузку на систему.
• **USER** — отображает объём системных ресурсов, использованных вашей виртуальной машиной в текущем терминальном сеансе.

Класс привилегий: A, E, G
Тип функции: O, A, G

IPL (или I)

Как правило, используется для возврата в CMS с помощью команды `IPL CMS` или `I CMS`. Команда IPL имитирует функцию начальной загрузки программы для виртуальной машины. Подкоманды:

• **vaddr** — виртуальный адрес (cuu) устройства, содержащего загружаемое ядро.
• **cylno** — цилиндр с данными IPL (по умолчанию 0).
• **nnnnn** — адрес блока с данными IPL (по умолчанию 0).
• **CLEAR** — обнуляет виртуальное пространство хранения перед загрузкой операционной системы.
• **NOCLEAR** — оставляет содержимое виртуального пространства хранения неизменным до загрузки программы.
• **STOP** — останавливает виртуальную машину в ходе процедуры IPL непосредственно перед загрузкой начального PSW.

• **ATTN** — генерирует прерывание по вниманию виртуальной машины в ходе процедуры IPL.
• **PARM p1 (p2...)** — передаёт до 64 байт данных в регистры общего назначения виртуальной машины начиная со старшего байта регистра 0.
• **systemname** — имитирует функцию IPL при загрузке именованной системы, сохранённой ранее.

Класс привилегий: G
Тип функции: G

LINK

Команда LINK используется для подключения к вашей конфигурации виртуальной машины устройства, связанного с другой виртуальной машиной, на основании информации из записи директории этого пользователя. Формат: `LINK TO userid vaddr1 AS vaddr2 (mode) ((PASS=) password(1)).`

Класс привилегий: G
Тип функции: G

LOADBUF

На принтере 1403 команда LOADBUF загружает универсальный набор символов (UCS) с указанным образом печатной ленты или цепи. На принтерах 3203, 3211, 3212, 4245 или 4248 загружает UCS или буфер управления формой (FCB) с указанным образом. На принтере 3289 модели 4 загружает в буфер смещения шрифтов (FOB) образ ленты и FCB.

Класс привилегий: D
Тип функции: S

LOADVFCB

Эта команда задаёт образ буфера управления формой для различных виртуальных спулированных принтеров. Переменные, следующие за ней:

• **vaddr**
• **FCB** — обязательное зарезервированное ключевое слово, означающее буфер управления формой.
• **name** — имя, определённое системой.
• **INDEX (nn)** — задаёт начальную позицию печати под номером nn для принтера 3211.

Класс привилегий: G
Тип функции: G

LOCATE

Используйте команду LOCATE для поиска адресов управляющих блоков CP, связанных с конкретным пользователем, устройством пользователя или реальным системным устройством.

Класс привилегий: C, E
Тип функции: P

LOCK

Эта команда безвозвратно фиксирует в памяти выбранные страницы реального хранилища.

Класс привилегий: A
Тип функции: O

LOGOFF (или LOGOUT, или LOG)

Используется для завершения сеанса виртуальной машины и отключения виртуальной машины от системы. Параметр HOLD (то есть `LOG HOLD`) позволяет сохранить соединение, чтобы при следующем входе не требовался повторный набор номера на коммутируемой линии.

Класс привилегий: ANY
Тип функции: ANY

LOGON (или LOGIN, или L)

Очевидно, команда LOGIN или LOGON используется для идентификации пользователя в системе и получения к ней доступа. После слов LOGIN, LOGON или L введите свой userid — идентификатор, назначенный вам в системе. Если в системе не включено подавление пароля, пароль можно ввести сразу после userid. ПРИМЕЧАНИЕ: если в системе включено подавление пароля (то есть вводимый пароль не отображается на экране), при попытке ввести пароль в той же строке, что и userid, вы получите системное сообщение об ошибке. Параметр NOIPL, следующий за паролем и userid, указывает, что IPL-устройство или имя из директории не должны использоваться для автоматической загрузки IPL.

Класс привилегий: ANY
Тип функции: ANY

MESSAGE (или MSG, или M)

Используйте команду MESSAGE для передачи текста сообщения указанному userid или основному системному оператору. `MSG userid msgtext` отправляет msgtext пользователю, указанному после userid. Если вместо userid указан символ `*`, текст отправляется самому себе. Если вместо userid указано слово OPERATOR, текст сообщения отправляется основному системному оператору независимо от его userid.

Класс привилегий: A, B, ANY
Тип функции: O, ANY

MIGRATE

Команда MIGRATE активирует стандартные процедуры миграции страниц/таблицы подкачки или принудительно переносит страницы конкретного пользователя на вторичное устройство, даже если этот пользователь в данный момент активен.

Класс привилегий: A
Тип функции: O

MONITOR

Для инициирования или переопределения функции, генерируемой системой, либо для прекращения регистрации событий, происходящих в реальной машине, используйте команду MONITOR.

Класс привилегий: A, E
Тип функции: O

MSGNOH

Команда MSGNOH позволяет служебной виртуальной машине отправлять сообщения указанным пользователям без стандартного заголовка, присущего команде MESSAGE.

Класс привилегий: B
Тип функции: R

NETWORK

Команда NETWORK позволяет загружать, выгружать и управлять работой контроллеров 3704 или 3705, а также управлять работой контрольной программы 3725 в режиме эмуляции 270x (EP). Кроме того, она обеспечивает управление удалёнными устройствами 3270 через линии BSC.

Класс привилегий: A
Тип функции: O

NOTREADY (или NOTR)

Команда NOTREADY заставляет виртуальное устройство, указанное после NOTREADY по адресу cuu, выглядеть так, как если бы оно перешло из состояния готовности в состояние неготовности.

Класс привилегий: G
Тип функции: G

ORDER (или ORD)

ORDER используется для упорядочивания закрытых спул-файлов пользователя в определённом порядке по типу устройства. К таким спул-файлам относятся файлы READER, PRINTER и PUNCH; их можно сортировать по CLASS, FORM и идентификатору спула.

Класс привилегий: D, G
Тип функции: S, G

PER

PER позволяет отслеживать определённые события в ходе выполнения программы на виртуальной машине пользователя. Эта команда может контролировать: выборку и выполнение инструкции, выполнение успешной инструкции ветвления, выполнение инструкции, изменяющей конкретный регистр общего назначения, и выполнение инструкции в виртуальной машине, изменяющей хранилище.

Класс привилегий: A, B, C, D, E, F, G
Тип функции: G

PURGE (или PUR)

Используйте команду PURGE для удаления из системы ваших собственных закрытых спул-файлов до их распечатки или перфорации на спулирующих устройствах, либо до их считывания пользователем. В спецификациях спул-файлов указываются файлы READER, PRINTER и PUNCH, а также параметр ALL, уничтожающий все перечисленные выше файлы.

Класс привилегий: D, G
Тип функции: S, G

QUERY (или Q)

Также доступна в режиме CMS; команда QUERY используется для определения статуса системы и конфигурации машины. Несмотря на огромное количество подкоманд QUERY, ниже перечислены элементы, которые можно запросить. Для получения подробной информации рекомендую использовать команду HELP CP QUERY — это весьма исчерпывающий текст (более 1000 строк).

• Время, использованное вами в течение терминального сеанса.

• Количество закрытых входных и выходных спул-файлов вашей виртуальной машины.
• Текущие настройки цвета и/или расширенного выделения для консоли виртуальной машины.
• Текущие настройки функций команды SET.
• Текущие настройки функций команды TERMINAL.
• Статус всех устройств виртуальной машины.
• Режим работы канала: блочный мультиплексор или селектор.
• Список всех пользователей, подключённых к заданному виртуальному адресу, с их адресами устройств и режимами доступа.
• Отображение дополнительного пользователя (secuser), указанного в директиве CONSOLE.
• Идентификация и атрибуты спул-файлов PRINTER, PUNCH и READER виртуальной машины.
• Идентификатор виртуального процессора.
• Режим работы процессора установки VM/SP HPO: однопроцессорный (UP), режим подключённого процессора (AP) или многопроцессорный (MP).
• Userid и идентификатор системы.
• Список элементов набора трассировки PER.
• Сообщения журнала дня.
• Имена пользователей, вошедших в систему.
• Количество пользователей, вошедших в систему или подключённых к ней.

ПРИМЕЧАНИЕ: существуют и другие операнды команды QUERY, доступные при наличии необходимого класса привилегий.

Класс привилегий: A, B, C, D, E, F, G
Тип функции: O, R, P, S, A, C, G

QVM

Используйте эту команду для запроса перехода из среды VM/SP в собственный режим для конкретной виртуальной машины.

Класс привилегий: A
Тип функции: O

READY

В формате `READY vaddr` эта команда используется для выставления в очередь прерывания «конец устройства» для указанного виртуального устройства.

Класс привилегий: G
Тип функции: G

REPEAT

Используйте команду REPEAT для увеличения количества копий выходного файла или для перевода текущего выходного файла в статус ожидания с увеличением или без увеличения числа создаваемых копий.

Класс привилегий: D
Тип функции: S

REQUEST (или REQ)

Просто используйте команду REQUEST для генерации прерывания по вниманию на виртуальной консоли.

Класс привилегий: G
Тип функции: G

RESET

Также в формате `RESET vaddr`, эта команда используется для очистки всех ожидающих прерываний указанного виртуального устройства.

Класс привилегий: G
Тип функции: G

REWIND (или REW)

Команда REWIND используется для перемотки реального ленточного устройства, подключённого к виртуальной машине по указанному виртуальному адресу, в формате `REWIND vaddr`.

Класс привилегий: G
Тип функции: G

SAVESYS

Эта команда позволяет сохранить виртуальное пространство хранения машины вместе с регистрами и PSW в их текущем состоянии. Используется в процессе создания именованных систем.

Класс привилегий: E
Тип функции: A

SCREEN (или SCRE)

Используйте команду SCREEN для изменения расширенного цвета и/или параметров расширенного выделения для консоли виртуальной машины. Команду можно выполнить с любого

поддерживаемого IBM терминала или из PROFILE EXEC, поскольку SCREEN не зависит от типа устройства. Однако SCREEN действительна только при наличии функции расширенного цвета на контроллере терминала.

Вы можете назначить расширенный цвет и параметры выделения шести отдельным областям экрана: области ввода, области системного статуса и области вывода, включающей три подобласти: вывод CP, вывод виртуальной машины и область повторного отображения ввода. Физические характеристики экранов информационных дисплеев 3270 различаются в зависимости от модели.

Поскольку эта команда в основном применима для пользователей, работающих не через коммутируемые линии, я решил не описывать подробно все доступные переменные команды SCREEN. Ещё раз рекомендую использовать HELP CP SCREEN для получения деталей.

Класс привилегий: G
Тип функции: G

SEND

Используя средство «Единый образ одной консоли» (SCIF), команда SEND передаёт команды и ответы на сообщения для консоли дополнительного пользователя на отключённые виртуальные машины для выполнения. Формат: `SEND (CP) userid (text).`

Класс привилегий: G
Тип функции: G

SET

Используйте команду SET для управления различными функциями виртуальной системы. Эта команда имеет большое количество переменных, и подробности по каждой из них можно получить из справочного файла HELP CP SET.

Класс привилегий: A, B, E, F, G
Тип функции: O, R, A, C, G

SHUTDOWN

Эта команда, разумеется, систематически завершает все функции виртуальных машин и сохраняет состояние системы для последующего тёплого запуска.

Класс привилегий: A
Тип функции: O

SLEEP (или SL)

Для перевода виртуальной машины в спящий режим с сохранением отображения сообщений используйте команду SLEEP в формате `SLEEP nn (time-specification)`, где time-specification — SEC (секунды), MIN (минуты) или HR (часы), а nn — количество единиц времени для спящего режима.

Класс привилегий: G
Тип функции: G

SMSG (или SM)

Команда SMSG используется для отправки специального сообщения виртуальной машине, запрограммированной для его приёма и обработки. Формат: `SMSG userid msgtext`, где userid — получатель сообщения, а msgtext — текст сообщения.

Класс привилегий: G
Тип функции: G

SPACE

Используйте команду SPACE для принудительного перевода вывода на указанный принтер в режим одинарного интервала для текущего активного спул-файла независимо от команд управления кареткой в самом файле.

Класс привилегий: D
Тип функции: S

SPMODE

SPMODE позволяет системному оператору установить или сбросить среду режима однопроцессорной работы.

Класс привилегий: A
Тип функции: O

SPOOL (или SP)

Используйте команду SPOOL для изменения параметров управления спулингом, действующих для заданного виртуального спулирующего устройства или группы устройств. Команда SPOOL также может запускать или останавливать спулинг ввода/вывода виртуальной консоли. Вы можете направить файл в удалённое место, используя команду SPOOL совместно с командой TAG.

Класс привилегий: G
Тип функции: G

SPTAPE

Используйте эту команду для сброса спул-файлов на магнитную ленту или загрузки спул-файлов с ленты.

Класс привилегий: D
Тип функции: S

START

Команда START перезапускает спулирующее устройство после его останова или изменяет выходной класс, который оно может обслуживать.

Класс привилегий: D
Тип функции: S

STCP

Для изменения содержимого реального хранилища без изменения реального PSW или реальных регистров используйте команду STCP.

Класс привилегий: C
Тип функции: P

STORE (или ST)

Команда STORE используется для изменения содержимого указанных регистров и областей виртуальной машины. Помимо сохранения данных виртуальной машины в нижней части хранилища, могут быть изменены:

• Виртуальные области хранения
• Регистры общего назначения
• Регистры с плавающей точкой
• Управляющие регистры
• Слово состояния программы (PSW)

Класс привилегий: G
Тип функции: G

SYSTEM (или SYS)

SYSTEM используется для имитации действий кнопок RESET и RESTART на реальной консоли компьютера, а также для очистки хранилища. Переменные:

• **CLEAR** — обнуляет виртуальное хранилище и ключи виртуального хранилища.
• **RESET** — очищает все ожидающие прерывания и условия в виртуальной машине.
• **RESTART** — имитирует аппаратную функцию перезапуска системы: сохраняет текущее PSW по виртуальному адресу восемь и загружает в качестве нового PSW двойное слово с виртуального адреса ноль.

Класс привилегий: G
Тип функции: G

TAG (или TA)

TAG имеет множество различных переменных, которые можно помечать тегами (их слишком много для перечисления здесь ввиду разных настроек каждой), однако используется она для связывания описательной информации о файле со спул-файлом.

Класс привилегий: G
Тип функции: G

TERMINAL (или TERM)

Команда TERMINAL используется для управления следующими функциями виртуальной консоли:

• Символы логического построчного редактирования
• Маскирование пароля
• Набор символов APL
• Набор текстовых символов
• Сигнализация прерывания по вниманию
• Режим обработки прерываний по вниманию на виртуальной консоли
• Длина строки вывода на виртуальной консоли
• Задание типа терминального устройства: 3101 или TTY
• Положение курсора перед операцией считывания терминала
• Скорость прокрутки для терминала 3101

Класс привилегий: G
Тип функции: G

TRACE (или TR)

Используйте команду TRACE для трассировки указанных видов активности виртуальной машины и записи результатов на терминал, на виртуальный спулированный принтер или одновременно туда и туда. При выдаче нескольких команд TRACE операнды суммируются: операнды, указанные впервые, активируются, тогда как операнды с новыми модификаторами обновляются. Однако операнды RUN и NORUN могут быть указаны в разных функциях трассировки без конфликта.

Команду TRACE нельзя использовать, когда работает режим предпочтительной машинной помощи, независимо от того, включён ли переключатель управления функцией предпочтительной машинной помощи.

Класс привилегий: G
Тип функции: G

TRANSFER (или TRAN)

Эта команда используется для передачи ваших закрытых спул-файлов указанному пользователю или в очередь, либо для возврата закрытых спул-файлов, созданных вами.

Класс привилегий: D, G
Тип функции: S, G

UNLOCK

Используйте команду UNLOCK для разблокирования страничных фреймов, ранее заблокированных командой LOCK.

Класс привилегий: A
Тип функции: O

VARY

Команда VARY помечает устройство как доступное или недоступное для использования пользователем или управляющей программой.

Класс привилегий: B
Тип функции: R

VMDUMP (или VMD)

Команда VMDUMP выгружает виртуальное хранилище, созданное VM/SP HPO для пользователя виртуальной машины. VMDUMP выгружает следующее:

• Виртуальное слово состояния программы (PSW)
• Регистры общего назначения
• Регистры с плавающей точкой
• Управляющие регистры
• Ключи защиты хранилища
• Идентификатор типа виртуальной машины
• Значения таймеров

Класс привилегий: G
Тип функции: G

WARNING

Используйте команду WARNING для передачи высокоприоритетных сообщений указанному пользователю или всем пользователям.

Класс привилегий: A, B
Тип функции: O

Данная статья отнюдь не претендует на исчерпывающую полноту. Как я уже упоминал в различных частях этого файла, система VM/CMS имеет очень хорошую систему справочных файлов, и из режима CMS команда `HELP CP` в большинстве случаев позволит вам прочитать достаточно ясный текстовый файл с подробным описанием и спецификациями использования этих команд. Надеюсь, что, если вам придётся работать в системе VM/CMS, этот файл поможет вам в режиме CP.

Тем, кто хочет связаться со мной для обсуждения темы этого файла или других вопросов, пишите на мои сетевые адреса:


```
Internet:  C488869@UMCVMB.MISSOURI.EDU
  Bitnet:  C488869@UMCVMB.BITNET
```

Введение в MIDNET

Автор: Knight Lightning

16 июня 1989 года

Глава седьмая «Саги о будущем трансцендентном»

Более глубокий взгляд на NSFnet — Национальную сеть Фонда науки

Пролог

Если вы ещё не знакомы с NSFnet, рекомендую прочитать:

«Frontiers» (Phrack Inc., Volume Two, Issue 24, File 4 of 13), а также в обязательном порядке: «NSFnet: National Science Foundation Network» (Phrack Inc., Volume Three, Issue 26, File 4 of 11).

Содержание

Введение

MIDNET — это региональная компьютерная сеть, входящая в состав NSFnet, Национальной сети Фонда науки. В настоящее время одиннадцать университетов центральной части США соединены друг с другом и с NSFnet через MIDnet:

```
UA  - University of Arkansas at Fayetteville
ISU - Iowa State University at Ames
UI  - University of Iowa at Iowa City
KSU - Kansas State University at Manhattan
KU  - University of Kansas at Lawrence
UMC - University of Missouri at Columbia
WU  - Washington University at St. Louis, Missouri
UNL - University of Nebraska at Lincoln
OSU - Oklahoma State University at Stillwater
UT  - University of Tulsa (Oklahoma)
OU  - University of Oklahoma at Norman
```

Исследователи из любого из этих университетов, получившие финансируемые гранты, могут обращаться к шести суперкомпьютерным центрам, финансируемым NSF:

• John Von Neuman Supercomputer Center
• National Center for Atmospheric Research

• Cornell National Supercomputer Facility
• National Center for Supercomputing Applications
• Pittsburgh Supercomputing Center
• San Diego Supercomputing Center

Кроме того, исследователи и учёные могут общаться друг с другом через обширную всемирную компьютерную сеть, включающую NSFnet, ARPAnet, CSnet, BITnet и другие, о которых вы читали в «Care о будущем трансцендентном». Подробности смотрите в «Frontiers» (Phrack Inc., Volume Two, Issue 24, File 4 of 13).

MIDnet — лишь одна из нескольких региональных компьютерных сетей, составляющих систему NSFnet. Хотя все эти региональные сети работают одинаково, MIDnet — единственная, к которой у меня есть прямой доступ, поэтому данный файл написан с точки зрения пользователя MIDnet. Для тех, кто имеет доступ к другим региональным сетям NSFnet, единственным существенным отличием в этом файле будет список обслуживаемых университетов — в противовес сетям:

```
NYSERnet  — штат Нью-Йорк
SURAnet   — юго-восток США
SEQSUInet — Техас
BARRnet   — район Сан-Франциско
MERIT     — Мичиган

(Существуют и другие, которые в настоящее время строятся.)
```

Все эти региональные сети подключаются к магистрали NSFnet — сети, связывающей шесть суперкомпьютерных центров. Например, пользователь Канзасского государственного университета может подключиться к суперкомпьютеру через MIDnet и магистраль NSFnet. Этот же исследователь может отправить письмо коллегам из Университета Делавэра, используя MIDnet, NSFnet и SURAnet. Каждый университет имеет собственную локальную компьютерную сеть, которая соединяет компьютеры на территории кампуса и обеспечивает подключение к региональной сети.

Некоторые университеты уже подключены к более старым сетям, таким как CSnet, ARPAnet и BITnet. В принципе, любой кампус, подключённый к любой из этих сетей, может связаться с кем угодно в любой другой сети — для этого существуют шлюзы между сетями.

Шлюзы — это специализированные компьютеры, которые перенаправляют сетевой трафик, тем самым соединяя сети. На практике глобальные сети используют различные сетевые технологии, что делает невозможным обеспечение полной функциональности через шлюзы. Тем не менее электронная почта почти повсеместно поддерживается через все шлюзы — так что пользователь сайта BITnet может отправить письмо коллеге на ARPAnet (и куда угодно ещё). Вы уже должны быть с этим знакомы; если нет — обратитесь к:

«Limbo To Infinity» (Phrack Inc., Volume Two, Issue 24, File 3 of 13) и
«Internet Domains» (Phrack Inc., Volume Three, Issue 26, File 8 of 11).

Компьютерные сети опираются на аппаратное и программное обеспечение, позволяющее компьютерам общаться между собой. Язык, обеспечивающий сетевое взаимодействие, называется протоколом. Сегодня существует множество различных протоколов. MIDnet использует протоколы TCP/IP, известные также как набор протоколов DOD (Министерства обороны США).

Другие сети, использующие TCP/IP, — ARPAnet, CSnet и NSFnet. Фактически все региональные сети, подключённые к магистрали NSFnet, обязаны использовать TCP/IP. На уровне местного кампуса TCP/IP применяется часто, хотя распространены и другие протоколы — например, IBM SNA и DEC DECnet. Для связи с компьютером через MIDnet и NSFnet компьютер в кампусе должен использовать TCP/IP напрямую или через шлюз, преобразующий его протоколы в TCP/IP.

Интернет — это всемирная компьютерная сеть, представляющая собой совокупность большинства крупных глобальных сетей, включая ARPAnet, CSnet, NSFnet и региональные сети, такие как

MIDnet. В меньшей степени к Интернету относятся и другие сети, например BITnet, способные отправлять почту на хосты этих сетей. Эта огромная сеть сетей — Интернет, — о которой вы уже читали на страницах Phrack Inc., стремительно растёт и представляет собой весьма сложную структуру, обеспечивающую развитое взаимодействие между учёными, студентами, государственными служащими и другими людьми. Быть частью этого сообщества — одновременно захватывающе и непросто.

Данная глава «Саги о будущем трансцендентном» даёт общее описание протоколов и программного обеспечения, используемых в MIDnet и NSFnet. Также включено обсуждение ряда наиболее часто используемых сетевых инструментов — чтобы вы могли как можно скорее начать практически работать с сетью.

Набор протоколов DOD

Набор протоколов DOD включает множество различных протоколов. Каждый протокол — это спецификация того, каким образом должен осуществляться обмен данными между компьютерами. Производители компьютерного оборудования и программного обеспечения используют протокол для создания программ, а иногда и специализированного аппаратного обеспечения, реализующего предусмотренную протоколом сетевую функцию. Для разнообразного аппаратного обеспечения и операционных систем, присутствующих в сети, существуют различные реализации одного и того же протокола.

Три наиболее часто используемые сетевые функции:

```
Почта            -- отправка и получение сообщений
Передача файлов  -- отправка и получение файлов
Удалённый вход   -- вход в удалённый компьютер
```

Из них почта, пожалуй, используется чаще всего.

В мире TCP/IP существуют три различных протокола, реализующих эти функции:

```
SMTP   -- (Simple Mail Transfer Protocol) почта
FTP    -- (File Transfer Protocol) отправка и получение файлов
Telnet -- удалённый вход
```

Использование этих протоколов обсуждается в следующем разделе. На первый взгляд неочевидно, почему именно эти три функции являются наиболее распространёнными. В конце концов, почта и передача файлов кажутся одним и тем же. Однако почтовые сообщения не идентичны файлам: они обычно состоят только из символов ASCII и имеют последовательную структуру. Файлы же могут содержать двоичные данные и иметь сложные, непоследовательные структуры. Кроме того, почтовые сообщения, как правило, могут допускать некоторые ошибки передачи, тогда как файлы ошибок содержать не должны. Наконец, передача файлов обычно происходит в защищённой среде (то есть пользователи знают имена и пароли друг друга и имеют право на передачу файла), тогда как письмо можно отправить кому угодно, зная лишь его имя.

Если почта и передача файлов обеспечивают перемещение сырой информации с одного компьютера на другой, то Telnet позволяет удалённому пользователю обрабатывать эту информацию — входя в удалённый компьютер или подключаясь к другому терминалу. Telnet чаще всего используется для удалённого входа на удалённый компьютер, но на самом деле это протокол связи общего назначения. За прошедший год я нашёл его невероятно полезным. В каком-то смысле его можно использовать для получения весьма широкого доступа, поскольку можно напрямую подключиться к любому компьютеру, поддерживающему TCP/IP, — однако обратите внимание, что Telnet — это *НЕ* Telenet.

Существуют и другие функции, которые предоставляют некоторые сети:

• Трансляция имён в адреса для сетей, компьютеров и людей
• Текущее время
• Цитата дня или случайный афоризм
• Печать на удалённом принтере или использование любого другого удалённого периферийного устройства
• Постановка пакетных заданий для неинтерактивного выполнения
• Диалоги и конференции между несколькими пользователями
• Удалённый вызов процедур (то есть распределение выполнения программы между несколькими удалёнными компьютерами)
• Передача голосовой или видеоинформации

Некоторые из этих функций всё ещё находятся в экспериментальной стадии и требуют более быстрых компьютерных сетей, чем существующие. В будущем, без сомнения, будут изобретены новые функции, а существующие — усовершенствованы.

Набор протоколов DOD — это многоуровневая сетевая архитектура, что означает: сетевые функции выполняются различными программами, работающими независимо и слаженно. Существуют не только разные программы, но и разные протоколы. Протоколы SMTP, FTP и Telnet описаны выше. Определены протоколы для получения текущего времени, цитаты дня и трансляции имён. Эти протоколы называются прикладными, поскольку пользователи напрямую взаимодействуют с программами, их реализующими.

Протокол управления передачей, TCP, используется многими прикладными протоколами. Пользователи почти никогда не взаимодействуют с TCP напрямую. TCP устанавливает надёжное сквозное соединение между двумя процессами на удалённых компьютерах. Данные передаются по сети небольшими порциями, называемыми пакетами, — для повышения надёжности и производительности. TCP гарантирует, что пакеты приходят в правильном порядке и без ошибок. Если пакет всё же содержит ошибки, TCP запрашивает его повторную передачу.

В свою очередь, TCP обращается к IP, Интернет-протоколу, для перемещения данных из одной сети в другую. IP при этом не является низшим уровнем архитектуры — под ним обычно располагается «протокол канального уровня». Им может быть любой из ряда различных протоколов; двумя весьма распространёнными являются X.25 и Ethernet.

FTP, Telnet и SMTP называются «прикладными протоколами», поскольку они непосредственно используются прикладными программами, позволяющими пользователям работать с сетью. Сетевые приложения — это фактические программы, реализующие эти протоколы и обеспечивающие интерфейс между пользователем и компьютером. Реализация сетевого протокола — это программа или пакет программ, обеспечивающий нужную сетевую функцию, например передачу файлов. Поскольку компьютеры у разных производителей различаются (например, IBM, DEC, CDC), каждый компьютер должен иметь собственную реализацию этих протоколов. Однако протоколы стандартизированы, чтобы компьютеры могли взаимодействовать в сети (то есть понимать и обрабатывать данные друг друга). Например, пакет TCP, сформированный компьютером IBM, может быть прочитан и обработан компьютером DEC.

Во многих случаях программы сетевых приложений используют название протокола. Например, программа для передачи файлов может называться «FTP», а программа для удалённого входа — «Telnet». Иногда эти протоколы включаются в состав более крупных пакетов, что типично для SMTP. На многих компьютерах есть почтовые программы, позволяющие пользователям одного и того же компьютера обмениваться сообщениями. Функции SMTP нередко добавляются к этим почтовым программам, чтобы пользователи могли также отправлять и получать почту через сеть. В таких случаях отдельной программы SMTP, доступной пользователю, не существует — поскольку интерфейс к данной сетевой функции предоставляет сама почтовая программа.

Конкретные реализации сетевых протоколов, например FTP, адаптированы к аппаратному обеспечению компьютера и операционной системе, в которых они используются. Поэтому точный пользовательский интерфейс варьируется от реализации к реализации. Например, протокол FTP определяет набор команд FTP, которые каждая реализация обязана понимать и обрабатывать. Однако обычно они располагаются на низком уровне и зачастую невидимы для пользователя, которому предоставляется более высокоуровневый набор команд.

Эти высокоуровневые команды не стандартизированы, поэтому могут отличаться в разных реализациях FTP. В некоторых операционных системах не все эти команды имеют одинаковый смысл — например, «Сменить директорию» — или могут иметь разные значения. Поэтому конкретный пользовательский интерфейс, с которым работает пользователь, скорее всего, будет отличаться.

Данный файл описывает обобщённую реализацию стандартных прикладных протоколов TCP/IP. Для получения сведений, специфичных для конкретного узла, пользователи должны обращаться к местной документации.

Имена и адреса в сети

В наборе протоколов DOD каждой сети присваивается уникальный идентификационный номер. Он назначается центральным органом — Сетевым информационным центром под управлением SRI (SRI-NIC) — во избежание присвоения одного и того же номера сети более чем одной сети. Например, ARPAnet имеет номер сети 10, тогда как MIDnet — более длинный номер: 128.242.

Каждый хост в сети имеет уникальный идентификатор, чтобы другие хосты могли однозначно адресовать его. Номера хостов обычно назначаются организацией, управляющей сетью, а не единым центральным органом. Номера хостов не обязаны быть уникальными в масштабах всего Интернета, однако два хоста в одной сети должны иметь разные номера.

Комбинация номера сети и номера хоста называется IP-адресом хоста и представляет собой 32-битное двоичное число. Все IP-адреса в Интернете выражаются как 32-битные числа, хотя обычно записываются в десятичной нотации с разделителями-точками. Эта нотация разбивает 32-битное число на четыре восьмибитных части (октета), каждый из которых записывается в виде десятичного числа. Например, 00000001 — это двоичный октет, соответствующий десятичному числу 1, а 11000000 соответствует 192. Десятичная нотация с точками значительно облегчает чтение и запоминание IP-адресов.

Компьютеры в Интернете также идентифицируются именами хостов — строками символов, например «phrackvax». Однако IP-пакеты должны указывать 32-битный IP-адрес вместо имени хоста, поэтому необходим какой-то механизм трансляции имён хостов в IP-адреса.

Один из способов — иметь таблицу имён хостов и соответствующих им IP-адресов, называемую таблицей хостов. Практически в каждой реализации TCP/IP такая таблица хостов имеется, хотя недостатки этого метода вынуждают переходить на новую схему — систему доменных имён. В системах UNIX таблица хостов часто называется `/etc/hosts`. Обычно этот файл можно прочитать и узнать IP-адреса различных хостов. В других системах этот файл может называться по-другому и не быть доступен для публичного просмотра.

Пользователям компьютеров, как правило, предоставляются учётные записи, на которые относятся все расходы по использованию компьютера. Даже если машинное время в учреждении бесплатно, учётные записи используются для разграничения пользователей и применения защиты файлов. В данном файле для обозначения имени, по которому осуществляется доступ к учётной записи,

используется общий термин «имя пользователя».

В ранние дни ARPAnet — первой сети, использовавшей протоколы TCP/IP, — пользователи компьютеров идентифицировались по имени пользователя, за которым следовал коммерческий знак «at» (@), а затем — имя хоста, на котором существовала учётная запись. Сетям как таковым имена не давались, хотя IP-адрес указывал на номер сети.

Например, «knight@phrackvax» указывал на пользователя «knight» на хосте «phrackvax». При этом не указывалось, в какой сети находится «phrackvax», хотя эту информацию можно было получить, изучив таблицу хостов и IP-адрес для «phrackvax». (Впрочем, «phrackvax» — вымышленное имя хоста, использованное в данном изложении.)

Со временем каждый компьютер в сети должен был иметь в своей таблице хостов запись для каждого другого компьютера в сети. Когда несколько сетей объединились в Интернет, проблема поддержания этой центральной таблицы хостов вышла из-под контроля. Поэтому была введена схема доменных имён, разбившая таблицу хостов на части и сделавшая её меньше и удобнее в обслуживании.

В новой схеме доменных имён пользователи по-прежнему идентифицируются по именам пользователей, однако хосты теперь идентифицируются по имени хоста и всем доменам, частью которых они являются. Например, следующий адрес: «KNIGHT@UMCVMB.MISSOURI.EDU» указывает имя пользователя «KNIGHT» на хосте «UMCVMB». Хост «UMCVMB» является частью домена «MISSOURI», который в свою очередь входит в домен «EDU». В домене «EDU» существуют другие домены, но только один из них называется «MISSOURI». В домене «MISSOURI» существует только один хост с именем «UMCVMB».

Однако другие домены в «EDU» теоретически могли бы иметь хосты с именем «UMCVMB» (хотя в данном примере это, пожалуй, маловероятно). Таким образом, сочетание имени хоста и всех его доменов делает его уникальным. Метод трансляции таких имён в IP-адреса уже не так прост, как поиск имени хоста в таблице. Несколько протоколов и специализированное сетевое программное обеспечение — серверы имён и распознаватели — реализуют схему доменных имён.

Не все реализации TCP/IP поддерживают доменные имена — они появились сравнительно недавно. В таких случаях единственным способом трансляции имён хостов в IP-адреса остаётся локальная таблица хостов. Системный администратор такого компьютера будет вынужден вносить в таблицу хостов запись для каждого хоста, к которому пользователи могут захотеть подключиться. В ряде случаев пользователи могут сами обращаться к серверу имён, чтобы узнать IP-адрес данного имени хоста, а затем использовать этот IP-адрес непосредственно вместо имени хоста.

Ниже я выбрал несколько сетевых хостов, чтобы продемонстрировать, как хост-система может быть задана как по имени хоста, так и по числовому адресу хоста. Некоторые из выбранных мной узлов являются также узлами BITnet — возможно, даже некоторые из тех, о которых я не делаю пометки ввиду недостаточной осведомлённости обо всех хост-системах мира :-)

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Числовой адрес  Имя хоста                Местонахождение               BITnet
--------------  ---------                ---------------               ------
18.72.0.39      ATHENA.MIT.EDU           (Mass. Institute of Technology)     ?
26.0.0.73       SRI-NIC.ARPA             (DDN Network Information Center)    -
36.21.0.13      MACBETH.STANFORD.EDU     (Stanford University)               ?
36.21.0.60      PORTIA.STANFORD.EDU      (Stanford University)               ?
128.2.11.131    ANDREW.CMU.EDU           (Carnegie Mellon University)   ANDREW
128.3.254.13    LBL.GOV                  (Lawrence Berkeley Labrotories)   LBL
128.6.4.7       RUTGERS.RUTGERS.EDU      (Rutgers University)                ?
128.59.99.1     CUCARD.MED.COLUMBIA.EDU  (Columbia University)                ?
128.102.18.3    AMES.ARC.NASA.GOV        (Ames Research Center [NASA])       -
128.103.1.1     HARVARD.EDU              (Harvard University)          HARVARD
128.111.24.40   HUB.UCSB.EDU             (Univ. Of Calif-Santa Barbara)      ?
128.115.14.1    LLL-WINKEN.LLNL.GOV      (Lawrence Livermore Labratories)    -
128.143.2.7     UVAARPA.VIRGINIA.EDU     (University of Virginia)            ?
```

```
128.148.128.40 BROWNVM.BROWN.EDU          (Brown University)              BROWN
128.163.1.5    UKCC.UKY.EDU               (University of Kentucky)         UKCC
128.183.10.4   NSSDCA.GSFC.NASA.GOV       (Goddard Space Flight Center [NASA])-
128.186.4.18   RAI.CC.FSU.EDU             (Florida State University)        FSU
128.206.1.1    UMCVMB.MISSOURI.EDU        (Univ. of Missouri-Columbia)   UMCVMB
128.208.1.15   MAX.ACS.WASHINGTON.EDU     (University of Washington)        MAX
128.228.1.2    CUNYVM.CUNY.EDU            (City University of New York)  CUNYVM
129.10.1.6     NUHUB.ACS.NORTHEASTERN.EDU (Northeastern University)       NUHUB
131.151.1.4    UMRVMA.UMR.EDU             (University of Missouri-Rolla) UMRVMA
192.9.9.1      SUN.COM                    (Sun Microsystems, Inc.)            -
192.33.18.30   VM1.NODAK.EDU              (North Dakota State Univ.)    NDSUVM1
192.33.18.50   PLAINS.NODAK.EDU           (North Dakota State Univ.)    NDSUVAX
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Обратите внимание: не у каждой системы в BITnet есть IP-адрес. Равным образом, не каждая система с IP-адресом находится в BITnet. Кроме того, хотя в некоторых местах, например в Стэнфордском университете, могут быть узлы в BITnet и хосты в IP-сети, это не обязательно означает, что системы в BITnet и в IP (в данном случае домен EDU) — одни и те же системы.

Попытки несанкционированного доступа к системам в Интернете не допускаются и по закону являются федеральным преступлением. На некоторых хостах к этому относятся очень серьёзно — особенно государственные хосты, такие как Центр космических полётов имени Годдарда NASA, который не стесняется сообщить вам об этом прямо в главном приглашении при подключении к их системе.

Однако некоторые узлы в определённой мере открыты для общего доступа. Сетевым информационным центром DDN может пользоваться любой. Сервер и база данных там оказались бесценным источником информации при поиске людей, систем и других сведений, связанных с Интернетом.

Telnet

Удалённый вход подразумевает вход в удалённый компьютер с терминала, подключённого к локальному компьютеру. Telnet — стандартный протокол в наборе протоколов DOD для решения этой задачи. Программа «rlogin», поставляемая с системами Berkeley UNIX и некоторыми другими, также обеспечивает удалённый вход.

Для целей данного обсуждения «локальный компьютер» — это компьютер, к которому ваш терминал подключён непосредственно, а «удалённый компьютер» — это компьютер в сети, с которым вы общаетесь и к которому ваш терминал *не* подключён непосредственно.

Поскольку некоторые компьютеры используют иной способ подключения терминалов, более точное определение таково: «локальный компьютер» — это компьютер, который вы используете в данный момент, а «удалённый компьютер» — компьютер в сети, с которым вы общаетесь или будете общаться. Заметим, что в дальнейшем термины «хост» и «компьютер» используются как синонимы.

Чтобы использовать Telnet, просто введите команду:

```
TELNET
```

Приглашение Telnet выглядит так:

```
Telnet>
```

(Однако можно сразу указать, куда подключиться, и пропустить приглашения и другие задержки, введя команду: `TELNET [адрес]`.)

Справку можно получить, введя `?`. При этом выводится список всех допустимых подкоманд Telnet с однострочным пояснением.

```
Telnet> ?
```

Чтобы подключиться к другому компьютеру, используйте подкоманду `open` для установки соединения с этим компьютером. Например, чтобы подключиться к хосту «UMCVMB.MISSOURI.EDU»:

```
open umcvmb.missouri.edu
```

Telnet выполнит преобразование (то есть трансляцию) имени хоста «umcvmb.missouri.edu» в IP-адрес и отправит пакет этому хосту с запросом на вход. Если удалённый хост решит разрешить попытку входа, он запросит имя пользователя и пароль. Если хост не ответит, Telnet «истечёт по тайм-ауту» (то есть подождёт разумное количество времени — около 20 секунд) и завершится с сообщением наподобие «Host not responding».

Если у вашего компьютера нет записи для удалённого хоста в таблице хостов и он не может разрешить имя, можно явно указать IP-адрес в команде telnet. Например:

```
TELNET 26.0.0.73
```

(Примечание: это IP-адрес Сетевого информационного центра DDN [SRI-NIC.ARPA])

Если вы успешно вошли в систему, ваш терминал подключён к удалённому хосту. Фактически ваш терминал соединён с этим хостом напрямую, и вы должны иметь возможность делать на удалённом терминале всё то же самое, что и на любом локальном. Однако из этого правила есть несколько исключений.

Telnet предоставляет специальный управляющий символ — символ выхода в сеть, например CONTROL-T. Узнать, какой именно символ выхода используется, можно с помощью подкоманды `status`:

```
Telnet> status
```

Изменить символ выхода можно с помощью подкоманды `escape`:

```
Telnet> escape
```

При вводе символа выхода на экране появляется приглашение Telnet, и вы можете вводить подкоманды. Например, чтобы разорвать соединение, что обычно влечёт выход из удалённого хоста, введите подкоманду `quit`:

```
Telnet> quit
```

Соединение Telnet обычно разрывается при выходе из удалённого хоста, поэтому подкоманда `quit` обычно не используется для завершения сеанса.

При входе на удалённый компьютер через Telnet помните, что между вашим локальным компьютером и удалённым существует временная задержка. Это часто замечают пользователи при прокрутке длинного файла на экране терминала, когда они хотят прервать прокрутку, нажав CONTROL-C или что-то подобное. После ввода специального управляющего символа прокрутка продолжается. Специальному управляющему символу требуется некоторое время, чтобы достичь удалённого компьютера, который продолжает выводить информацию. Таким образом, отклик удалённого компьютера, вероятно, будет не таким быстрым, как отклик локального.

После удалённого входа компьютер, в который вы вошли, фактически становится вашим «локальным компьютером», хотя ваш исходный «локальный компьютер» по-прежнему считает вас вошедшим в систему. Вы можете войти в третий компьютер, который тогда станет вашим «локальным компьютером», и так далее. По мере выхода из каждого сеанса предыдущий сеанс снова становится активным.

FTP — программа, позволяющая пересылать файлы с одного компьютера на другой. «FTP» расшифровывается как «File Transfer Protocol» (Протокол передачи файлов).

При запуске FTP открывается канал связи с другим компьютером в сети. Например, чтобы запустить FTP и начать сеанс передачи файлов с компьютером в сети по имени «UMCVMB», следует ввести следующую подкоманду:

```
FTP UMCVMB.MISSOURI.EDU
```

Хост «UMCVMB» запросит имя учётной записи и пароль. Если вход выполнен успешно, FTP сообщит об этом; в противном случае будет выведено «login incorrect». Попробуйте ещё раз или прервите программу FTP (обычно это делается вводом специального управляющего символа, например CONTROL-C; символ «прерывания программы» варьируется от системы к системе).

Далее вы увидите приглашение FTP:

```
Ftp>
```

У FTP есть ряд подкоманд. Подкоманда `?` выведет их список с кратким описанием каждой.

Передачу файлов можно инициировать в любом направлении: с удалённого хоста или на удалённый хост. Подкоманда `get` инициирует передачу файла с удалённого хоста (то есть даёт команду удалённому компьютеру отправить файл на локальный компьютер, с которого была выдана команда `ftp`). Достаточно ввести `get`, и FTP запросит имя файла на удалённом хосте и (новое) имя файла на локальном хосте. Пример:

```
Ftp> get
Remote file name?
theirfile
local file name?
myfile
```

Можно сократить запись, указав оба имени файла в той же строке, что и подкоманда `get`. Если имя локального файла не указано, новому локальному файлу будет присвоено то же имя, что и у удалённого. Допустимые подкоманды FTP для получения файла:

```
get theirfile myfile
get doc.x25
```

Подкоманда `put` работает аналогичным образом и используется для отправки файла с локального компьютера на удалённый. Введите команду `put`, и FTP запросит имя локального файла, а затем имя удалённого файла. Если передача невозможна из-за отсутствия файла или по какой-либо другой причине, FTP выведет сообщение об ошибке.

Существует ряд других подкоманд FTP, позволяющих выполнять гораздо больше действий. Не все они являются стандартными, поэтому обратитесь к местной документации или введите знак вопроса в приглашении FTP. Некоторые функции, часто встроенные в FTP, включают возможность просматривать файлы перед их получением или отправкой, менять директории, удалять файлы на удалённом компьютере и выводить содержимое директории на удалённом хосте.

Интригующая возможность многих реализаций FTP — «передача третьей стороне». Например, если вы вошли на компьютер A и хотите заставить компьютер B отправить файл на компьютер C, можно использовать FTP для подключения к компьютеру B и команду `rmtsend`. Разумеется, необходимо знать имена пользователей и пароли на всех трёх компьютерах, поскольку FTP никогда не позволяет заглянуть в чужую директорию и файлы без знания имени пользователя и пароля.

Подкоманда `cd` меняет рабочую директорию на удалённом хосте. Подкоманда `lcd` меняет директорию на локальном хосте. Для систем UNIX смысл этих подкоманд очевиден. Другие

системы, особенно те, в которых нет файловой системы с древовидной структурой директорий, могут не реализовывать эти команды или реализовывать их иначе.

Подкоманды `dir` и `ls` делают одно и то же — выводят список файлов в рабочей директории удалённого хоста.

Подкоманда `list` показывает содержимое файла, не помещая его в файл на локальном компьютере. Это удобно, если нужно просто просмотреть файл. Вывод можно прервать до достижения конца файла с помощью CONTROL-C или другого специального символа — в зависимости от реализации FTP.

Команда `delete` позволяет удалять файлы на удалённом хосте. Можно также создавать и удалять директории на удалённом хосте с помощью `mkdir` и `rmdir`. Подкоманда `status` сообщит о текущем состоянии соединения, а также о текущих настройках всех параметров.

При передаче двоичных файлов или файлов с непечатаемыми символами включите двоичный режим с помощью подкоманды `binary`:

```
binary
```

Чтобы вернуться к недвоичной передаче, введите подкоманду `ascii`.

Передачу сразу нескольких файлов можно легко осуществить с помощью `mput` (множественная отправка) и `mget` (множественное получение). Например, чтобы получить каждый файл из определённой директории, сначала выполните команду `cd` для перехода в эту директорию, а затем команду `mget` со звёздочкой для указания всех файлов:

```
cd somedirectory
mget *
```

По завершении используйте подкоманду `close` для разрыва канала связи. Вы по-прежнему будете находиться в FTP, поэтому для выхода из FTP и возврата на командный уровень необходимо ввести подкоманду `bye`. Подкоманда `quit` закроет соединение и одновременно выйдет из FTP.

Почта

Электронная почта во многих отношениях является простейшим сетевым средством. Всё, что нужно сделать, — это создать сообщение (с помощью текстового редактора или на ходу) и отправить его. В отличие от FTP и Telnet, не нужно знать пароль имени пользователя на удалённом компьютере. Это обусловлено тем, что вы не можете изменять или просматривать файлы удалённого пользователя и не можете использовать его учётную запись для запуска программ. Всё, что можно сделать, — это отправить сообщение.

Вероятно, на вашем локальном компьютере есть программа для обмена сообщениями между пользователями этого компьютера. Такая программа называется почтовым агентом (mailer). Она может быть, а может и не быть способом отправки и получения почты от других компьютеров в сети, хотя интегрированные почтовые агенты встречаются всё чаще. В качестве примера в данном обсуждении будут использованы почтовые агенты UNIX.

Обратите внимание: протокол, используемый для отправки и получения почты по сети TCP/IP, называется SMTP, «Simple Mail Transfer Protocol» (Простой протокол передачи почты). Как правило, вы не будете использовать никакой программы под названием SMTP — вместо неё вы будете использовать вашу локальную почтовую программу.

Почтовые агенты UNIX обычно вызываются программой «mail». Для получения новой почты достаточно ввести `mail`.

Существует несколько разновидностей почтовых агентов UNIX. Подробности смотрите в местной документации. Например, команда `man mail` выводит страницы руководства для почтовой программы на вашем компьютере.

Для отправки почты обычно необходимо указать адрес получателя в команде mail. Например: `mail knight@umcvmb.missouri.edu` отправит следующее сообщение пользователю «knight» на хосте «umcvmb».

Обычно можно вводить сообщение построчно, нажимая RETURN после каждой строки и вводя CONTROL-D для завершения сообщения. Иногда существуют средства для включения уже существующих файлов. Например, Berkeley UNIX позволяет вводить команды наподобие следующей для включения файла в текущее почтовое сообщение:

```
r myfile
```

В данном примере содержимое файла «myfile» вставляется в сообщение в этом месте.

Большинство систем UNIX позволяют отправлять файл по почте с помощью перенаправления ввода. Например:

```
mail knight@umcvmb.missouri.edu < myfile
```

В данном примере содержимое файла «myfile» отправляется в качестве сообщения пользователю «knight» на «umcvmb».

Обратите внимание, что во многих системах UNIX единственным различием между почтой, предназначенной другому пользователю на том же компьютере, и почтой другому пользователю на удалённом компьютере является просто указанный адрес: для локальных получателей имя хоста не указывается. В остальном почта функционирует абсолютно одинаково. Это характерно для интегрированных почтовых пакетов. Система сама определяет, отправлять ли почту локально или через сеть, исходя из адреса, — и пользователь избавлен от необходимости разбираться в прочих деталях.

«Стремление к знаниям не имеет конца...»

Список NUA для сетей Datex-P и X.25

Автор: Oberdaemon

9 апреля 1989 года

Условные обозначения

```
cccc naa aaa aaa... oooo...      ddd....
```

Примечание: В список включены также очевидно опечатанные NUA, встречавшиеся в широко распространённых списках. Есть и номера, которые не образуют корректный NUA, а являются общим префиксом (например, `0202 2` — Helpak).

Формат записи

Каждый NUA в этом списке состоит из следующих полей:

Поле	Описание
cccc	Префикс страны (например, 0262 — Германия). Может быть опущен, если вызывающая и вызываемая стороны имеют одинаковый префикс.
naa	Первые три цифры адреса. n нередко указывает на конкретную сеть в данной стране.
aaa aaa...	Остальные цифры адреса.
oooo...	Дополнительные цифры/буквы, которые следует добавлять после NUA. Правильный синтаксис зависит от вашего PAD. В данном списке используется любой синтаксис — как правило, тот, что применял автор источника. Поле oooo... обычно пусто.
ddd...	Краткое описание сервиса.

Поле	Описание
cccc	Префикс страны (например, 0262 — Германия). Может быть опущен, если вызывающая и вызываемая стороны имеют одинаковый префикс.

naa	Первые три цифры адреса. n нередко указывает на конкретную сеть в данной стране.
aaa aaa...	Остальные цифры адреса.
oooo...	Дополнительные цифры/буквы, которые следует добавлять после NUA. Правильный синтаксис зависит от вашего PAD. В данном списке используется любой синтаксис — как правило, тот, что применял автор источника. Поле oooo... обычно пусто.
ddd...	Краткое описание сервиса.

Если два NUA различаются только количеством завершающих нулей, но ведут к одному и тому же сервису, более длинный можно смело отбросить.

!! Обратите внимание: большинство PAD не принимают пробелы внутри NUA !!

Таблица NUA

Ниже приведён полный список NUA для сетей Datex-P и X.25, охватывающий узлы в Европе, Северной Америке, Азии, Австралии и других регионах. Каждая запись содержит статус, NUA-адрес, имя узла (если известно) и описание.

```
  0200                  GR          Греция
  0202
  0202 2                            Helpak (enkelriktad trafik)
X 0202 452 241 24104
  0204                  NL          Нидерланды
  0204 0                            Datanet (1?)
  0204 1                            Datanet (1?)
A 0204 129 001 3                    ? (Netz ?)
A 0204 129 001 4                    X.25
A 0204 129 003 1                    NONOBY
A 0204 129 003 4                    Searchline
D 0204 129 004 33       SARA        National Institute for High Energy Physics
                                    (NIKHEF) SARA network
D 0204 129 004 34       NIKHEF      National Institute for High Energy Physics
                                    (NIKHEF) SARA network
D 0204 129 005 6        MCVAX       MCVAX, HOLLAND
A 0204 129 005 675      HARING      MCVAX Line 2
   0204 129 400 2                    DUPHAR WEESP,HOLLAND
A 0204 134 014 80500                Utrecht ?
  0204 303 0                        EPOIS EPO Den Haag
  0204 304 0                        DSAMISOOM SAMSON
  0204 4                            Dabas
  0206                  B           Бельгия
  0206 2                            DCS
A 0206 210 300 003                  Eigebib
A 0206 222 100 6        BBDA        Brussels DEC A
A 0206 222 101 2        ?           Ministry of economic affairs
A 0206 222 102 6                    celex
A 0206 224 001 903      PRLB2       Belgium Unix Backbone
  0206 3                            Euronet
A 0206 228 821 0                    DGxiiiF
  0208                  F           Франция
  0208 0                TRANSPAC    French Transpac
A 0208 006 040 010                  Telesystemes 1
```

```
A 0208 006 040 201                Telesystemes 2
A 0208 026 020 843                ?
A 0208 034 020 036      CNUSC     CNUSC (France)
A 0208 034 020 258      CNUSC     CNUSC Montpelier
A 0208 038 020 100                CICG Grenoble
A 0208 038 020 676                ILL VEGA VAX 8700 VMS 4.7
I 0208 044 001 645                ?
A 0208 057 040 540                QSD (Chat system)
I 0208 069 021 258
A 0208 075 000 087      IRCAM     IRCAM-ERIK VAX 11/780 4.2 BSD
I 0208 075 000 355                ?
I 0208 075 001 281*D    CCPN      Computing Centre Nuclear Physics
I 0208 075 002 314                GRF
A 0208 075 020 655      LITP      LITP Unix 4.3 BSD (France)
A 0208 075 041 280                Pasteur MV8000
A 0208 078 020 118      INRIA     INRIA, Rocquencourt (France) Multics
B 0208 078 020 16901    INRIA     Institute National de Recherche en
                                  Informatique
  0208 078 081 67304    INRIAUU   INRIA - UUCICO
I 0208 091 000 270*DCISICISI3     IBM - TSO
I 0208 091 000 309*DCISICISI1     IBM - TSO
I 0208 091 000 519*DCISICISI2     IBM - TSO
I 0208 091 010 320      CJRCE
I 0208 091 040 047      SACLAY    Saclay - France
I 0208 091 040 532                Pascal
A 0208 091 190 258                LURE, VAX 11/780 VMS 4.6, Synchrotron
                                  source (SES)
  0208 1                          NTI
A 0208 101              TEXTFRA   Text Generator, FRANCE
  0214                  E         Испания
  0214 1                SPAIN     Spanish data network (NID/CTNE)
  0214 5                          Iberpac
O 0214 521 202 5022
A 0214 521 302 1020               ETSITM (EANNET) VAX 11/750 VMS 4.5
  0222                  I         Италия
  0222 2                          Itapac
A 0222 262 002 1        ESAIRS1   ESA-QUEST, IRS 1
I 0222 262 002 2        ESAIRS2   ESA-IRS 2
O 0222 262 003 2                  IASI VAX
A 0222 262 004 3                  VAXLNF (INFNET) VAX 8650
O 0222 263 200 4                  NUA-Information ?
A 0222 265 014 0                  Techni-Link
I 0222 306 3                      Progetto-Sirio
I 0222 306 700                    European Space Agency
I 0222 306 9*D          CNUCE     CNUCE
I 0222 307 0                      CILEA
I 0222 307 1                      CED Datenbanksysteme Rom
I 0222 307 2*D          RTC20     JRC
I 0222 307 7*D QUESTD5  ESA       ESA
D 0222 307 8*D QUESTD5  ESA2      ESA
  0228                  CH        Швейцария
D 0228 310 1*DN         DATASTAR  Data-Star, Switzerland
  0228 4                          Telepac
A 0228 462 110 0101               Cigy IBMA
A 0228 462 110 0102               Cigy DEC1091
A 0228 462 110 09                 EDP Basel
A 0228 462 110 23                 ?
A 0228 462 110 34                 ?
A 0228 462 110 36                 ?
A 0228 462 110 52                 DANZA'S 11/785 VMS 4.4
A 0228 462 110 61                 PKK node RBPK00
A 0228 462 110 66                 PROGNOS Basel (CIERR 1402)
A 0228 462 110 70                 ?
A 0228 462 110 84                 (CIERR 1402)
Y 0228 462 170 02                 INFOTEX PTT
I 0228 464 109 06                 GD PTT Schweiz (ring with CTRL G)
A 0228 464 110 10       DM        DATAMAIL (RSAG)
A 0228 464 110 110      DSTAR2    Datastar (2nd. Line)
A 0228 464 110 112                RSAG
Z 0228 464 110 113                RSAG
A 0228 464 110 115      DATASTAR  Data-Star, Switzerland (Pharmadatenbank ?)
```

```
A 0228 468 113 150                Management Joint Trust
D 0228 468 114 05       CERN      CERN (=CERNXX?)
A 0228 468 114 0505               CS Group LAVC on node UXCOMS
A 0228 468 114 0510     CER       CERN, Geneva
A 0228 468 114 0510     CERNVAX   CERN X25 Multigate
B 0228 468 114 0510*DLO CERNLO    CERN 300 bps     OUTDIAL (where ???)
B 0228 468 114 0510*DME CERNME    CERN 1200 bps    OUTDIAL (where ???)
B 0228 468 114 0510*DHI           CERN ?
A 0228 468 114 0514               4.2 BSD UNIX (Mint)
A 0228 468 114 0515               Cern LS Group LAVC VXGIFT
A 0228 468 114 0520               Cern
A 0228 468 114 0532               Cern
A 0228 468 114 0533               L3 test beam VAX-750 VXC3
A 0228 468 114 0534               UXINFN
A 0228 468 114 0538               CS Group LAVC on node UXCOMS
A 0228 468 114 054                Cern
A 0228 468 114 0545               Cern
A 0228 468 114 0551               VXCERN VMS 4.6
A 0228 468 114 0553               VXCERN VMS 4.6
A 0228 468 114 0556               VXCERN VMS 4.6
A 0228 468 114 0560               CERN VXNA31
A 0228 468 114 0561               CERN VXNA31
A 0228 468 114 0562               L3 VAX 11/750 VXC3MU
A 0228 468 114 0572               ISOLDES VAX 11/750
A 0228 468 114 0574               ? (Operator)
A 0228 468 114 0581               ?
A 0228 468 114 0583               %Merit:X.25 (Merit Computer Network, see
                                  appendix)
A 0228 468 114 0584               Develcon
A 0228 468 114 0587               ? (Operator)
A 0228 468 114 0588               ? (Operator)
A 0228 468 114 0589               ? (Operator)
A 0228 468 114 0592               Princeton University High Energy Physics
                                  Group Vax 11/750
A 0228 468 114 0593               University of Michigan Physics Vax 11/750
A 0228 468 114 0596               N.U. Physics Vax 11/750
A 0228 468 114 0597               Harvard University High Energy Physics Lab.
                                  Vax 8650
A 0228 468 114 0598               MIT-LNS*PIERRE
A 0228 468 114 0599               DoD, Distributed Databases Coordination
                                   Center (JMILLER,X0TF3AP)
D 0228 468 114 18                 BIOGEN (=GODEL?)
A 0228 468 114 23                 EDCHUB::
A 0228 469 110 02                 EPFL (something)
A 0228 469 110 0202               EPFL HELP
D 0228 469 110 0203               EPFL DE.VAX
D 0228 469 110 0204               EPFL GC.VAX
A 0228 469 110 0205               EPFL DP.VAX
A 0228 469 110 0206               EPFL ME.VAX
A 0228 469 110 0207               EPFL GR.VAX
A 0228 469 110 0208               EPFL MA.VAX
A 0228 469 110 0209               EPFL DI.VAX
D 0228 469 110 0210               EPFL IMAC.PDP
D 0228 469 110 0211               EPFL CGL.VAX
D 0228 469 110 0212               EPFL DE.MVAX
A 0228 469 110 0213               EPFL CC.VAX
A 0228 469 110 03                 EPFL Cyber 855
Ar0228 469 110 0301               EPFL Cyber
A 0228 475 110 02                 HSG St.Gallen
Ar0228 479 104 00                 Cern
A 0228 479 110 23                 I.P.Sharp (CA)
X 0228 479 110 86                 KOMETH (ETH ZH)
A 0228 479 110 650                KOMETH (ETH ZH)
I 0228 479 111
A 0228 479 111 06                 GRS
I 0228 479 111 086
I 0228 479 111 11
I 0228 479 111 18                 ZEV-Mailbox Zuerich
A 0228 479 111 750                ComNet (R-Nua)
A 0228 479 311 49                 KOMETH Output (ETH ZH)
A 0228 499 111 02001              KOMETH (Entry Uni)
```

```
  0228 9                          Radio-Suisse
  0232                  A         Австрия
  0232 2                          Datex-P
O 0232 242 210 91
? 0232 242 211 42*DMAI            Sysnet Wien (Gast,Gast)
A 0232 252 310 000                Uni Wien
  0232 9                          Radio Austri
A 0232 911 602 323                Inpadoc
  0234                  GB        Великобритания
  0234 1                IPSS      IPSS UK network
A 0234 110 020 02018              BT DIALCOM GROUP (PRESTEL ?)
  0234 2                          PSS
  0234 198 061 60                 Queen Marry C.
B 0234 207 920 002                SWVA
  0234 211 920 100515             Hostess Doc.
  0234 212                        Dialnet
O 0234 212 080 105
I 0234 212 080 110      EPSONUK   Epson (UK)
A 0234 212 300 120      DIALNET   IGS Leased line to DIALOG in US
A 0234 212 300 12011    DIALNET   LRS-DIALOG 2   Dialog via London
Ar0234 212 300 12013    DIALMRC   LRS-Dialmail   (Reverse Charging)
A 0234 212 300 120*D@   DIALNET   IGS Leased line to DIALOG in US
A 0234 212 300 2920               GeoNet GEO2
B 0234 212 301 161                OPTEL
  0234 212 301 186                GEOSYSTEMS
  0234 212 301 187                CAP GROUP LTD.
  0234 212 301 18722    CAP       CAP Industry Ltd.
  0234 212 301 281                ONE TO ONE COMMS
O 0234 212 302 02192    PSSCLK    PSS Clock
B 0234 212 399 12013    DIALMAL   Dialmail via London
A 0234 212 900 115      STL       STL : ACER (BSD UNIX 4.2)
  0234 213 000 11
  0234 213 000 151      COMPUTAS  Computas Ltd
  0234 213 000 1511               COMPUTAS LTD.
D 0234 213 900 10150   ALVEY     Alvey Mail and FTP.
  0234 214 200 162      GLAXO     Galaxo Industries
  0234 214 400 12                 CONTROL DATA LTD.
  0234 215 000 11600    C3
  0234 215 710 104                Consultans Ltd
  0234 216 700 127      PFIZER    Pfizer, SANDWICH
  0234 216 700 12701    PFIZER1   Pfizer, SANDWICH
  0234 216 700 12702    PFIZER2   Pfizer, SANDWICH
  0234 216 700 12703    PFIZER3   Pfizer, SANDWICH
  0234 216 700 12704    PFIZER4   Pfizer, SANDWICH
  0234 216 700 12706    PFIZER6   Pfizer, SANDWICH
  0234 218 801 00300              British Telecom Hotline
  0234 219                        PSS-Network
  0234 219 200 001                Network Monitoring Centre (NFS)
  0234 219 200 002                Network Monitoring Centre (NFS)
  0234 219 200 100                University of London Computing Centre
  0234 219 200 10069    JANETGW   PSS/JANET Gateway (ULCC)
B 0234 219 200 101                Finsbury Data Service
  0234 219 200 1082               BING COMPUTER SERVICES (EUROPE) LTD.
A 0234 219 200 118      ADPUK     ADP NETWORK SERVICES LTD. (=AUTONET?)
  0234 219 200 118                atomic energy research establishment
  0234 219 200 13370    QTLON     Quantime
A 0234 219 200 146      CEGB      CEGB, Park Street, London
B 0234 219 200 14869    ULCC      Univ. London Computer Centre (=JANET2?)
B 0234 219 200 14918    UCLMVAX   UCL Microvax ARPA Gateway
B 0234 219 200 14970
  0234 219 200 154                UNILEVER COMPUTER SERVICES LTD.
A 0234 219 200 171      LEXIS     LEXIS
A 0234 219 200 190      INFOLINE  PERGAMON INFOLINE LTD. (NFS)
A 0234 219 200 203      IPSH      SHARP, I. P. ASSOCIATES LTD.
A 0234 219 200 220                BRITISH LIBRARY ON-LINE SYSTEM
A 0234 219 200 222      BLAISE    British Library Information System
  0234 219 200 297                RLFE & NOLAN COMPUTER SERVICES PLC
B 0234 219 200 300      UCL       University College London - Computer
  0234 219 200 300      UCLFTP    UCL (FTP)
A 0234 219 200 300      UCLMAIL   UCL (JNT Mail)
  0234 219 200 304                University Computing Company (GB) Ltd.
```

```
B 0234 219 200 333      EUCLID     University College London  Computer Centre
  0234 219 200 394      CISI       CISI (=SIANET?;=Computer Services, London?)
  0234 219 200 871                 Instrument Rentals (UK) Ltd.
B 0234 219 201 002      POOLE
  0234 219 201 004      BGOLD81    Telecom BT-GOLD System 81
  0234 219 201 00472    BGOLD72    Telecom BT-GOLD System 72
  0234 219 201 00474    BGOLD74    Telecom BT-GOLD System 74
  0234 219 201 00479    BTGOLD     Telecom BT-GOLD System 79
  0234 219 201 00481    BTGOLDA    Telecom BT-GOLD System 81
  0234 219 201 00482    BTGOLD82   Telecom BT-GOLD System 82
  0234 219 201 00484    BGOLD84    Telecom Gold System 84
  0234 219 201 005      PSSMAIL    PSS TELE-MAIL service
B 0234 219 201 00513    DIANENQ    Euronet DIANE Enquiry Service
                                   (=Echo,Rutherford?)
B 0234 219 201 00513    EUROINFO   Euronet Diane Information Service
                                   (=Echo,Rutherford?)
A 0234 219 201 00515    BTDOC      BT Online Documentation Service
A 0234 219 201 00515    HOSTESS    Hostess system (BT)
  0234 219 201 00530    BAYNARD    BT Protocol Study Centre (NFS)
  0234 219 201 00615    PSSDOC     PSS documentation service/X25 technical
                                   info on line
  0234 219 201 00620    BTBILL     BT Online Billing
  0234 219 201 0100513
  0234 219 201 01013    HOSTESS    Hostess system (BT) (=PSS Switchstream 1 ?)
T 0234 219 201 01030    TSTB       British Telecom
  0234 219 201 025      PRESTEL    BT Prestel Service
  0234 219 201 02517
  0234 219 201 07800
  0234 219 201 15600    ESA1       ESA-IRS via London
  0234 219 201 18       ADPUK      ADP Network Services Ltd
  0234 219 210 050                 BT Mailbox facility (NFS)
  0234 219 511 31       GEC        GEC Computers Borehamwood
  0234 219 511 311      GECB       GEC Computers Ltd. Borehamwood
  0234 219 513 11       GECB       GEC Computers Ltd. Borehamwood
  0234 219 709 111                 Modular Computer Services Ltd. (MODCOMP)
? 0234 219 709 111      NPL1       National Physical Laboratory
  0234 219 709 210      NPL2       National Physical Laboratory, Protocol Std
                                   Group
B 0234 219 806 160      QMC        Queen Mary College London
X 0234 220 200 1070               island-Adventure-Game
X 0234 220 200 10700              island-Adventure-Game
  0234 220 641 141      ESSX       Essex, University of, Computing Service
                                   (2653,2653,Mist)
A 0234 220 641 1411               MUD (Adventure Game), <guest>, <mist> or
                                   <2653,2653>
B 0234 221 222 122      MIDB       MIDNET Gateway at Birmingham (=MIDBHM)
  0234 221 222 223      BIRP       Prime R & D at Birmingham
  0234 221 222 225                 Freight Comp. Services
  0234 222 236 163      CARDF      Cardiff, University College
  0234 222 236 16300    CARDIFF    Univ. Coll. Cardiff Multics
  0234 222 236 236      UWIST      University of Wales
  0234 222 300 16102    ACORN      Acorn Computers
  0234 222 339 399      CAMBRID    Cambridge University (Phoenix)
  0234 222 530 303      SWURCC     South-West Universities
  0234 222 530 30388    SWURCC     South-West Universities Network
  0234 222 530 30398    SWCFTP     SWURCC (FTP)
A 0234 222 715 151      KENT       University of Kent
X 0234 222 715 11                 ? (---,Guest,Friend (call PIP))
  0234 223 440          TI         Texas Instruments Ltd
  0234 223 440 144      BED5       Prime R & D at Bedford (NFS)
  0234 223 440 345      TI         Texas Instruments Ltd
  0234 223 500 10998    HLH        High Level Hardware Ltd.
B 0234 223 519 111      AERE       Atomic Energy Research Establishment at
                                   Harwell
T 0234 223 519 11198    ADA        ADA UK Database
  0234 223 519 119169               JANET
  0234 223 519 191      DLVAFTP    Daresbury SRS VAX (FTP)
A 0234 223 519 191      JANET      Gateway to JANET at Rutherford
  0234 223 519 191      OUCSFTP    OUCS VAX (FTP) - Experimental
  0234 223 519 191      REVSFTP    ROE Starlink VAX (FTP)
  0234 223 519 191      RLDAFTP    Rutherford DCS 11/70 (FTP)
```

```
  0234 223 519 191      RLGBFTP    RL GEC (FTP)
  0234 223 519 191      RLIBFTP    RL IBM 370 CMS (FTP)
  0234 223 519 191      RLPCFTP    L Prime C (FTP)
  0234 223 519 191      SERC       Gateway to SERCNET at Rutherford
  0234 223 519 191      SERCENQ    SERCNET Acc & P/word Fac.
  0234 223 519 191      SYPEFTP    Surrey Prime 550 (FTP)
  0234 223 519 191      UEAFTP     East Anglia via SERC (FTP)
  0234 223 519 191      ZUVSFTP    UCL Starlink VAX (FTP)
A 0234 223 519 19169    SERCNET    R/ford XXX SERCnet g/way
                                   (=DARESBURY,=JANET?)
? 0234 223 519 19169,.10404000     Lancaster Uni
B 0234 223 519 19169,.36           Oxford2
? 0234 223 519 19169,49000001
B 0234 223 519 19169,.50200014     Oxford
B 0234 223 519 19169,.CPVC         Omega VAX
A 0234 223 519 19169,.CPVD         Merlin VAX
B 0234 225 621 126      DECSS      DEC Software Support VAX (=BEANO?)
  0234 227 200 110                 GEAC 8000 ITI
  0234 227 200 112      HPLB       HPLB (Hewlett Packard Labs, Bristol)
  0234 227 230 230      BRST       University of Bristol
  0234 227 230 23000    BRISTOL    University of Bristol
  0234 227 230 231                 DLLON Comp. & Manag. Services Ltd.
  0234 227 230 301                 GAC Computers Ltd.
  0234 227 230 333      AVON       Avon Universities Computer Centre
  0234 227 230 33300    AUCC       Avon Universities Computer Centre
  0234 227 230 33398    AUCCFTP    AUCC (FTP)
B 0234 227 900 102      BLAISE     British Library Information System
  0234 227 900 10400    ESTELLE    STC Estelle
  0234 227 900 14302    ITT        ITT Harlow (=ALCATEL?)
  0234 231 300 101                 PRIME Office, Edinburgh
  0234 231 300 102                 Forestry Commission FTP
  0234 231 300 105      LATTLOG    Lattice Logic LTD
  0234 231 300 107
B 0234 231 354 354      ERCC       Edinburgh Regional Computer Centre
  0234 231 354 35419    BUSHFTP    RCO 2988 (FTP)
B 0234 231 354 35422    ERCC       ERCC - 2980, 2972 (EMAS) (=RCONET?)
  0234 232 500 124      EXIS       EXIS
I 0234 233 458 158      STAND      St. Andrews University VAX
B 0234 233 458 15898    STANFTP    St. Andrews Univ. (FTP)
  0234 234 417 117                 ICL at Bracknell
B 0234 239 232 323      EXETER1    Exeter University
  0234 239 232 32304    EXTR       University of Exeter
  0234 241 200 107
  0234 241 260 106      SCRSX      University of Strathcylde PDP-11/44 (RSX)
A 0234 241 260 10604              ? (,5020015,Birch/Bryan)
  0234 241 260 260      GLSG       University of Glasgow (NFS)
B 0234 241 260 26004              Glasgow
  0234 246 200 10243              ICL West Gorton 'B' Service
  0234 246 200 10248              ICL West Gorton 'X' Service
  0234 246 200 10277              ICL West Gorton Perq
  0234 246 240 240      ICLL       ICL at Letchworth (=Kidsgrove?) (NFS)
  0234 247 300 103                 MTIER Management Systems Ltd.
  0234 247 300 10300               Bridge, Switch
  0234 247 300 10340               Bridge, (VAX/VMS)
  0234 247 300 10345               Bridge, (MUX(VT100))
  0234 247 300 10346               Bridge
  0234 247 302 022      MHGA       LDC at Martlesham
  0234 248 300 106                 DWENT-SDC Search Service
  0234 248 321 321                 DWENT-SDC Search Service
B 0234 251 248 248      LIVE       University of Liverpool
  0234 252 724 241      BSL        BL Systems Ltd.
  0234 253 265 165      LEEDS      University of Leeds (NFS)
  0234 253 300 124      CAMTEC     Camtec, Leicester
  0234 253 300 12406    CAMTEC     Camtec, Leicester (hard copy printer)
  0234 258 200 106      ARC        Agricultural Research Council (GEC - Switch)
  0234 258 200 106      EMALFTP    East Malling (FTP)
  0234 258 200 106      RESFTP     RES (Rothampstead) - FTP
  0234 258 200 10604    AGRIFTP    AGRINET (CPSE) FTP
  0234 258 200 10604    AGRINET    AGRINET Gateway
  0234 258 200 10604    EASTMAL    East Malling
  0234 258 240 242      GECD       GEC Computers Ltd at Dunstable
```

```
  0234 258 240 24200    MRCA       GEC - Marconi Research Centre
B 0234 260 227 227      MIDN       MIDNET Gateway at Nottingham
B 0234 261 456 8383                Microlink
B 0234 261 600 119                 Manchester
  0234 261 600 133                 IBM - SALE (also FTP)
B 0234 261 600 152      UMDAFL     University of Manchester Dataflow VAX
  0234 261 643 143      UMRCC      University of Manchester Regional Computer
                                   Centre
  0234 261 643 14398    UMRFTP     UMRCC (FTP)
  0234 261 643 210      SALF       Salford University
  0234 261 643 21090    SALFORD    Salford -> GANNET
  0234 261 643 21090   NRS        NRS
B 0234 261 643 343      FERRANTI   Feranti Computer Systems
  0234 262 500 484                 Software Sciences Ltd.
B 0234 262 800 151                 CDM/EH (=Maidenhead?)
B 0234 263 259 159      NUMAC      University of Newcastle
  0234 264 200 136                 Primenet
B 0234 270 500 115                 MAXXIM
B 0234 270 500 142                 Farenham
T 0234 270 500 15                  Uni Brighton (GUEST,WELCOME)
  0234 270 712 217      HATF       Hatfield Polytechnic
  0234 273 417 171      DEC-RDG    Digital Equipment Ltd Reading
  0234 273 417 217      MODC       Modcomp
  0234 273 417 317      DECR       DEC at Reading
  0234 274 200 103                 SHEFFIELD, University of, Dept.of
                                   Electronic & Elec...
  0234 274 200 103*DCODUCODUS      Codus
  0234 274 253 385                 DVY Computing Ltd.
  0234 275 300 102                 GIS Ltd.
  0234 275 312 212      BOC        British Oxygen (=The World Reporter??)
  0234 275 312 212      DATASOLVE  as above
  0234 275 312 212      EUROLEX    British Oxygen Company
  0234 275 317 173                 Lynx Computers Ltd.
  0234 275 317 177                 TELEFILE Computer Services Ltd.
  0234 275 317 177      GSI        GSI (NFS)
  0234 278 228 282                 ICL Letchworth
  0234 278 228 288                 ICL Letchworth
  0234 284 400 108                 Culham, (VAX)
  0234 284 400 123      ALVEY      Alvey Electronic Mail
B 0234 289 500 109                 UXB
  0234 290 468 168      YORK       York University PSS Gateway
B 0234 290 468 168      YORKFTP    York University (FTP)
  0234 290 468 168                 Gateway To DEC-10 At York
  0234 290 468 16804    YORKTS     York TS29 Port
  0234 290 524 242      RSRE       Radio, Space Research Establishment
  0234 290 524 24203    RSREDL     RSRE
  0234 290 524 24204    RSRESNK    RSRE
  0234 290 524 24250   RSREA      Radio, Space Research Establishment for
                                   ALVEY mail
  0234 290 840 111      POLIS      SCION
  0234 290 840 111      SCICON     SCICON, South England
  0234 292 549 149      DL         SERC at Daresbury Laboratory
  0234 293 212 212                 DATASOLVE LTD.
  0234 293 212 212      BOC        British Oxygen Company (NFS)
D 0234 293 765          ARTTEL     British Library, Boston Spa
  0234 293 765 265                 British Library Lending Divi.
  0234 299 212 221      NOLTON     Nolton Communications Ltd. (NFS)
  0234 3                           Euronet
  0234 307 813          EUROINFO   Euronet Diane Information Service
  0234 8                TELEX      UK Telex network
  0234 892 992 0        DECTELX
I 0235 200 143 00165
  0238                  DK         Дания
  0238 2                           Datapak
A 0238 241 592 400                 Valby I/S Datacentralen
A 0238 241 745 600      RECKU      Univac in Copenhagen University
  0238 241 745 60000               Recku Univac (Enter @@ENQ)
  0238 241 745 60002    UDIKU
A 0238 242 126 400                 Lyngby DTB; I/S Datacentralen
I 0238 389 3                       Euronet Aarhus
  0240                  S          Швеция
```

```
I 0240 181 559 76       LIUIDA S    Linkvping LiUIDA Teletex
  0240 2                            Datapak
A 0240 200 002 05                   Uppsala STUNS VAX/UNIX KULING
I 0240 200 044 4        ENEA        ENEA
A 0240 200 100 110                  Stockholm QZ/DEC-10
A 0240 200 100 120                  Stockholm QZ/CD Cyber 730
O 0240 200 100 203                  Uppsala, UU, Teknikum, NORD 100/500
A 0240 200 100 205                  Uppsala, UU, Stuns, VAX 750
A 0240 200 100 206                  Uppsala, UDAC/DECnet RTR18A
O 0240 200 100 207                  Uppsala, UDAC, Cyber 835
A 0240 200 100 228                  Uppsala, UDAC/UPNET - Terminalnaet
A 0240 200 100 232                  Uppsala, UDAC, IBM/GUTS (BASF 7/68 ?)
O 0240 200 100 28                   Uppsala Upnet
? 0240 200 100 30                   Umeaa VAX-750 Skogsh. Umeaa Univ
A 0240 200 100 303                  Umeaa, UMDAC/BIOVAX
A 0240 200 100 304                  Umeaa, Skogshoegskolan, VAX 750
A 0240 200 100 305                  Umeaa, UMDAC/DECnet RTR09A, (Vax 11/750)
A 0240 200 100 30520                Umeaa, UMDAC/BASUN
A 0240 200 100 30540                Umeaa, UMDAC/UTB1 (Vax 11/780)
A 0240 200 100 30550                Umeaa, UMDAC/UTB2 (Vax 11/750)
A 0240 200 100 30570                Umeaa, UMDAC/OSTVAX (Vax 11/780,
                                    Hoegsk i Oe-sund)
A 0240 200 100 307                  Umeaa, UMDAC/Cyber 850
D 0240 200 100 312                  Luleaa, Tekn hoegsk, NORD 100
D 0240 200 100 313                  Luleaa, Tekn hoegsk, NORD 100
A 0240 200 100 328                  Umeaa, UMDAC/NUNET - Terminalnaet
D 0240 200 100 33                   Umeaa VAX-11/780
A 0240 200 100 403                  Linkoeping, ULi/LIUIDA, uVAX-I
D 0240 200 100 404                  Linkoeping, ULi/PDP 11/23 BULL
A 0240 200 100 405                  Linkoeping, LIDAC, VAX 11/780 VIKTOR
A 0240 200 100 407                  Linkoeping, LIDAC/DECnet RTR13A, uVAX-II
D 0240 200 100 432                  Linkoeping, LIDAC/TEXAS - Terminalnaet
A 0240 200 100 7                    Primenet
A 0240 200 101 903                  Stockholm, SU, Psykologi, Prime 750
A 0240 200 101 904                  Stockholm, QZ IBM (Amdahl)
A 0240 200 101 905                  Stockholm, QZ, NFRVAX
A 0240 200 101 907                  Stockholm, QZ/DECnet RTR08A
A 0240 200 101 914                  Stockholm, SU, Fysik, Vax 780
D 0240 200 101 926                  Stockholm, KTH/KTHNET - Terminalnaet
A 0240 200 101 928                  Stockholm, QZ/QZNET - Terminalnaet
O 0240 200 102 06                   Uppsala UDAC uVAX-II RTR18A
O 0240 200 102 07                   Uppsala CD Cyber 835
A 0240 200 102 7                    Stockholm DEC-10/Janus
A 0240 200 102 71                   Stockholm DEC-10/Janus
A 0240 200 201 603                  Goeteborg, CTH, Infobeh, VAX 750, Unix
D 0240 200 201 604                  Goeteborg, GU, Pedagogiska inst, Prime 550
A 0240 200 201 605                  Goeteborg, GU, Statistiska inst, Prime 550
D 0240 200 201 606                  Goeteborg, CTH, Tillaempad Elektronik, VAX
                                    750
A 0240 200 201 607                  Goeteborg, Tillaempad Elektronik/DECnet
                                    RTR31A (RTR18A ?)
A 0240 200 201 628                  Goeteborg, GD/GUCNET - Terminalnaet
D 0240 200 201 632                  Goeteborg Upnod
A 0240 200 205 4                    SCB
A 0240 200 278 0                    Oerebro, Hoegskolan, Prime
A 0240 200 292 6                    Karlstad, Hoegskolan, VAX 11/780
D 0240 200 310 204                  Lund, Fysikum, NORD 500, Lucas
O 0240 200 310 206                  Lund, Maxlab, NORD 100
A 0240 200 310 207                  Lund, LDC/DECnet RTR46A, uVAX-II
A 0240 200 310 20720                Lund, LDC/GEMINI, Vax 8350
A 0240 200 310 228                  Lund, LDC/LUNET - Terminalnaet
  0240 201 001 30                   Stockholm QZ/Amdahl
  0240 201 002 03                   Uppsala Teknikum Nord 100/500
  0240 5                SWEDEN      Swedish data network (Telepak)
I 0240 500 025 3        QZXB        QZ by yet another route
I 0240 500 025 7                    Stockholm, DEC, VAX
I 0240 501 50                       Scannet, Goteborg
I 0240 501 51                       Scannet, Helsingfors
I 0240 501 52                       Stockholm KTH/TTDS
I 0240 501 531 0        QZCOM       QZ-COM - Stockholm University DEC-10
I 0240 501 532 0        QZCB        QZ Cyber
```

```
I 0240 501 533 0        QZIB        QZ Amdahl
I 0240 501 54           UPPS        Uppsala network, Sweden
I 0240 501 550 3                    Gottenburg, Sweden
I 0240 501 582 8        LUND        Lund University
I 0240 501 60                       Helsinki CP9500 HYLK B7800
I 0240 502 00                       Scannet, Stockholm
I 0240 502 01                       Denmark, Copenhagen Scannet
I 0240 502 02                       Tandem Computers
I 0240 502 032 8        QZXA        QZ Sweden via reverse PAD (=UPNET?)
I 0240 502 032 832                  Oden, Sweden
I 0240 502 033 2        QZDA        QZ DEC-10 Sweden
I 0240 502 04                       Prime Computers
I 0240 502 05                       Vaesteraas PAD ASEA Multics
I 0240 502 52                       KEMIDATA
I 0240 502 53           QZXB        QZ by yet another route
  0240 515 330                      Amdahl
  0242                  N           Норвегия
  0242 2                NORWAY      Norwegian data network (Datapak/Norpak)
  0242 192 010 1013                 PSS DOC
X 0242 211 000 00107    OSLO        DEC-1099 DEC-net/PSI at Oslo University
D 0242 211 000 001*D02              Oslo univ BRU-nett UNINETT
D 0242 211 000 001*D03  OSLO        DEC-10 at Oslo University
D 0242 211 000 00100                Oslo univ DEC-1099 UNINETT
D 0242 211 000 002                  Oslo Scannet NSI Nord-100
D 0242 211 000 01018    DATAPIN     DATAPAK Info - Norway
B 0242 211 000 074                  Oslo VAX
T 0242 223 000 00151    RBK         Cyber 170 at IFE (Energy Research Centre)
T 0242 223 000 001*D00  RBK         Cyber 170 at IFE, Kjeller RBK UNINETT
D 0242 223 000 002                  Kjeller FFI UNINETT
D 0242 245 000 00101    BERGEN      Univac at Bergen University (UNINETT)
D 0242 245 000 001*D00  BERGEN      Univac at Bergen University
A 0242 245 013 4                    BBB Mailbox (Bergen By Byte)
  0242 253 000 001*D11              Trondheim UNINETT RUNIT UNIVAC
T 0242 253 000 00101    RNI         Univac at Trondheim University
X 0242 253 000 00103                Trondheim RUNIT UNINETT VAX-780
T 0242 253 000 00104                Trondheim NLHT UNINETT VAX-750
  0242 265 000 001*D00              Tromso UNINETT U of Tromso, Cyber 171
  0242 253 000 001*D11  RUNIT       Univac at Trondheim University
  0242 265 000 001*D81              Tromso UNINETT U of Tromso, NORD-10
  0242 265 000 001*D82              Tromso UNINETT U of Tromso, NORD-100
  0242 265 000 001*D83              Tromso UNINETT U of Tromso, NORD-500
  0242 265 000 00101    TROMSOE     Cyber 170 at Tromsoe University (UNINETT)
  0242 265 000 001*D81  TROMSO      ELAN at Tromsoe University
X 0242 265 000 106                  PORTACOM (PORTACOM)
  0244                  SF          Финляндия
  0244 2                            Datapak (Finpak)
A 0244 202 006                      Economics HP 3000
A 0244 202 007                      University of Helsinki, B7800 (=CANDE ?)
A 0244 202 008                      VTKK (Staten DC) IBM 360
A 0244 202 012                      U o Helsinki Mopo Mikko3
A 0244 203 008          HELVA       High Energy Physics Vax 11/750
A 0244 203 017                      U of Technology DEC-20
D 0244 231 006                      Technical University of Tampere VAX
A 0244 253 001                      Tech U of Lappeenranta VAX/VMS
A 0244 261 001                      U of Vaasa VAX/VMS
A 0244 273 002                      University of Joensuu VAX
D 0248 321 321                      DWENT-SDC Search Service
  0262                  D           Германия
  0262 3                            Euronet
X 0262 307 4                        INFAS
  0262 4                GERMANY     German data network (Datex-P)
```

[Таблица из ~400 записей для Германии (0262) — NUA Datex-P: Аахен, Берлин, Бохум, Бонн, Бремен, Гамбург, Ганновер, Дармштадт, Дортмунд, Дюссельдорф, Франкфурт, Фрайбург, Штутгарт, Карлсруэ, Кёльн, Мюнхен и другие узлы — опущена]

```
  0310                  USA         США — Tymnet
```

[Таблица из ~150 записей для США/Tymnet (0310) — опущена]

```
  0311 0                TELENET     США — Telenet
```

[Таблица из ~200 записей для США/Telenet (0311) и других американских сетей (0312, 0313) — опущена]

```
  0334                          Мексика
  0334 0                        Telepac
  0340                  FA      Французские Антилы (Мартиника)
  0340 0                        Dompac/NTI
  0342                  BDS     Барбадос
  0342 235 191 9169
  0350                          Бермуды
  0350 3                        PSDS
  0425                  IL      Израиль
  0425 1                        Isranet
B 0425 130 000 215              Israelbox
  0426                  BRN     Бахрейн
  0426 3                        BTC
  0431                  DXB     ОАЭ — Дубай
  0440                  J       Япония
  0440 1                        DDX-P
B 0440 129 431 04               KEK VAX
B 0440 129 431 21               Tsukuba Uni
  0440 8                VENUSP  Venus-P (Japanese data network)
I 0440 820 023                  KDD ?
B 0440 820 060 01       KDD     KDD Test Host, TOKYO
  0442
B 0442 110 403 25               OKI
B 0442 433 403 07               CMES
  0450                          Южная Корея
  0450 1                        Dacom/DNS
  0454                  HK      Гонконг
  0454 2                        Intelpak
  0454 5                        Datapak
A 0454 550 010 4        HKDATA  Hong Kong DATAPAK Info
A 0454 550 043 1                DATAFAX
  0487                          Тайвань
  0487 2                        Pacnet
  0487 7                        Udas
  0505                  AUS     Австралия
  0505 2                        Austpac
  0505 228 621 000              Anglo/Australian Observatory
  0505 228 621 001              CSIRO Radio-Physics
  0505 228 621 001              FTP for Epping
  0505 233 422 000      MELBUNI Melbourne Univ. Australia
A 0505 273 720 000      UQ      Univ. of Queensland Australia
A 0505 273 720 000      UQXA    University of Queensland ANF-10 gateway
D 0505 273 722 0000             Uni Queensland
  0505 282 620 000              FTP For Austek
A 0505 282 620 000              VAX in Sidney, Australia
  0505 3                        Midas
  0505 321 000 1                Network test
  0505 321 000 3                MIDAS FOX Test
  0510                          Индонезия
  0510 1                        PSDS (1986)
  0525                  SGP     Сингапур
  0525 2                        Telepac
A 0525 211 668 8        TELEPAC Telepac Info
  0530                  NZ      Новая Зеландия
  0530 1                        P.S.S. (Pacnet)
  0530 171 000 004      WAIKATO Univ of Waikato New Zealand
B 0530 197 000 016              ASMAIL
  0547                          Фр. Полинезия
  0547 0                        Tompac
  0612                          Кот-д'Ивуар
  0612 2                        Sytranpac
  0647                          Реюньон
  0647 0                        Dompac/NIT
  0655                  ZA      ЮАР
  0655 0                        Saponet
D 0655 011 101 207              UNI-NET
  0714                          Панама
```

```
   0714 1                          Intelpac
   0722                            Аргентина
   0722 2                          Arpac
 I 0722 221 110 0171
   0724                  BR        Бразилия
   0724 0                          Interdata
   0724 1                          Renpac
 D 0724 782 450 8                  Nuclear Research Institute
   0730                            Чили
   0730 0                          Entel
   0732                            Колумбия
   0732 0
   0742                            Французская Гвиана
   0742 0                          Dompac/NTI
   0900                            США ?
   0900 0                          Dialnet
```

Приложение: локальные адреса на KOMETH (0228 479 110 86)

```
    11  KOMETH-Informations
   120  Modems 1200 bps (predefined numbers, some with a PW)
   124  Modems 2400 bps (     "        "   ,  "   "    a PW)
   130  Modems 300 bps  (     "        "   ,  "   "    a PW)
   1D0  RZ-VAX (EZRZ1)
   300  ETZ-VAX (CUMULI)
   520  ETHICS, Library database
   D11  PSI-Informations
  C000  Time
  C025  X25 Gateway (RZU, with password)
  C011  NUZ-Informations
  C100  RZU, VM/SP, full-screen
```

На RZ-VAX работают две информационные системы:

• **MAC-BBS** — доска объявлений с информацией по тематике Mac. Доступ только для авторизованных пользователей (необходимо ввести имя, адрес и указать, являетесь ли вы студентом ETH, после чего ожидать несколько дней). Имя пользователя: `MAC`.
• **VisInfo** — информационный сервер VIS (Verein der InformatikStudenten). Содержит тематические разделы с почтой из нескольких сетей и локальных источников. Есть чат (закрыт в часы пик). Свободный доступ. Имя пользователя: `VISINFO`.

Приложение: локальные адреса в CERN (0228 468 114 0510)

```
    17  Lyon (own network)
    23  PAD
    31  VXOMEG
    41  Wisconsin/Madison
    42  CERNLINE 193
    45  DECserver
    51  ALEPH
    56  MERLIN VAX
    61  (Prompt )
    72  Wylbur / VM
   100  Wylbur / VM
   101  VM/370 CERNVM
   102  VM/370 CERNVMB
   103  VM/370 CERNVM
   110  VXLDB1 VAX 8650 VMS 4.6
   111  Information
```

```
112  VXSB
115  VXLDB1
120  Service CAD_CAM (VAX 8650+VAX785)/SYSTEME=VMS 4.6
121  CAD_CAM
122  VXCERN
123  VXCERN
124  BSD
125  CERNVM
127  PAD
130  L3 test beam VXC3
137  ALEPH-TPC
140  VXEPEL
141  DECserver 200 ("user friendly")
142  CERNADD
146  VXEPEL
147  Uni Genf TEC VAXTEC
151  CCVAX / DECserver 200
152  Uni Genf WA70
154  ALEPH 750 Fastbus VAX
161  MCR
162  MCR
166  VXWA80
167  cernvax
170  VXINFN
175  ALEPH
176  MCR with HELP
X29  X25 Gateway
```

Приложение: узлы сети Merit (0228 468 114 0583)

Основные хост-компьютеры сети Merit:

Name	System/machine	Organization	Location
MSUnet-IBM	VM/CMS IBM 3090-180	Michigan State Univ	East Lansing
OU	Multics Honeywell	Oakland Univ	Rochester
UB	MTS IBM 3090-400	Univ of Michigan	Ann Arbor
UM	MTS IBM 3090-400	Univ of Michigan	Ann Arbor
WM	DECsystem-10	Western Michigan Univ	Kalamazoo
WU	MTS Amdahl 470V/8	Wayne State Univ	Detroit

По вопросам использования сети Merit звоните по телефону (313) 764-9423 и просите соединить с консультантом.

Прочие хост-компьютеры и сервисы, доступные в сети Merit:

Autonet	CMU-Cyber	CMU-IBM	Datapac
DIALOUT-AA	DIAL1200-AA	DIAL2400-AA	DIAL300-AA
EMU-VAX	IGW	ITI	MAGNET
MSU-CLSI	MSU-CLVAX1	MSU-EGRNET	MSU-IBM
MSU	MTU	MTUS5	OU-SecsNet
RPI	RUAC	Survey	Telenet
UM-Annex	UM-CIC	UM-CLINFO	UM-dippy
UM-DSC	UM-EnginHarris	UM-MMVAX	UM-Public-Service
UM-QuickSlides	UM-RAVAX	UM-zippy	UMD-LIB
UMLIB	UMLIB-300	WAYNEST1	WAYNEST2
WMU-CAE	WMU-Kanga	WMU-Pooh	WMU-Puff
WMU-Tigger	WMU-Winnie	WSU-CSVAX	WSU-ET
WSUNET	ZOOnet-KCollege	ZOOnet-KVCC	ZOOnet-Nazareth

Некоторые компьютеры и сервисы, доступные через Telenet, Autonet и Datapac:

ABA/NET	ACP	ADPNS-261	ADPNS-3
ADPNS-446	ADPNS-9	Alberta	ARTFL
Automail-23	Automail-297	Boeing	British-Columbia
BRS	Cal-Berkeley	Calgary	Caltech-HEP

Carnegie-DEC-20	Carnegie-MICOM	Carnegie-11/45	CompuServe
Comshare	Cornell	Dalhousie	DatapacInfo
Dialcom	Dialog	Dow-Jones	Guelph
Guelph-Cosy	Illinois	Illinois-Cyber	LEXIS
Manitoba	Maryland-Unix	McGill	MGH
Minnesota-Cyber	Minnesota-VAX	MIT-Multics	MIT-VM
Montreal	Natl-Lib-Med	NCAR-Telenet	New-Brunswick
Newsnet	NJIT-EIES	NLM	NLM-MCS
Notre-Dame	NRC	NYTimes	OAG
Queens	Rice	SDC	SFU

COSMOS — Компьютерная система для обслуживания мейнфреймов. Часть вторая

Автор: King Arthur

В этой статье я предлагаю решения проблем компьютерной безопасности, описанных в моём предыдущем файле. Ниже перечислены простые, но нередко игнорируемые меры, которые при должном соблюдении способны существенно повысить безопасность компьютерных систем вашей компании. Эти принципы применимы не только к COSMOS, но и ко всем компьютерам во всех организациях.

A) Безопасность коммутируемых линий

При защите любой компьютерной системы, независимо от её типа, важно помнить следующее: единственный способ получить к ней удалённый доступ — это наличие коммутируемой линии, ведущей к этой системе. Если у вашей системы есть коммутируемое подключение, убедитесь, что вы приняли все возможные меры для его защиты. «Единственный совет, который я дам: будьте осторожны с коммутируемыми линиями», — говорит Эд Пиннес из Bellcore.

Дейв Импарато, менеджер по управлению базами данных в New York Telephone, говорит: «У нас установлены устройства, расположенные перед компьютерами, через которые необходимо пройти аутентификацию. Чтобы добраться до COSMOS, нужно преодолеть три или четыре уровня защиты — и это ещё до того, как вы вообще попадёте в систему».

Правила защиты коммутируемых линий:

1. Используйте как можно меньше коммутируемых линий. Выделенные линии или прямые соединения зачастую являются достойной им заменой.

2. Если телефонные линии к вашему компьютеру всё же необходимы, по возможности применяйте внешнее аппаратное обеспечение. Например, коммутатор виртуальных каналов Datakit (VCS) требует от пользователя указать «пароль доступа» и адрес системы назначения. После этого VCS подключает вас к запрошенной системе, которая в свою очередь запрашивает логин и пароль. Использование подобного оборудования преследует двойную цель:

A) Проникнуть в компьютер становится сложнее из-за дополнительных паролей;

B) Сотрудникам достаточно набрать один номер для доступа к нескольким системам.

Другой хороший тип оборудования — модем с функцией обратного вызова (callback modem). Такой модем запрашивает у пользователя логин и пароль. Если они верны, модем автоматически перезванивает на заранее заданный номер, после чего выполняется вход в систему. Преимущество callback в том, что подключиться можно только со строго определённого телефонного номера. К сожалению, для систем с большим числом пользователей такой подход не всегда эффективен.

Наконец, наиболее действенный способ защиты — использовать систему, которая никак не идентифицирует себя. Звонящий должен ввести секретный пароль, который не отображается на экране. Если пароль введён неверно, система просто завершает соединение, не сообщая звонящему, что произошло.

3. Если вы обнаружили, что «хакеры» звонят на определённый номер, рекомендуется его сменить. Телефонные номера не должны быть указаны в справочниках. По словам одного хакера, он однажды узнал номер компьютера AT&T, позвонив в справочную службу и попросив номер AT&T по

адресу 976 Main Street.

4. Если коммутируемые линии не используются в ночное время или по выходным, их следует отключать. Хакеры, как правило, занимаются своими «делами» именно в эти часы. Система COSMOS позволяет ограничивать доступ в зависимости от времени суток.

B) Парольная безопасность

Проводя аналогию между компьютером и картотечным шкафом, пароль можно сравнить с замком на этом шкафу. Наличие учётных записей без паролей фактически означает, что шкаф стоит нараспашку. Пользователи системы зачастую выбирают пароли, которые легко запомнить. Это неразумно, особенно для базы данных с большим числом пользователей. Первыми хакеры пробуют самые очевидные варианты. Например, если известно, что MF01 — имя учётной записи для кросс-монтажного зала, хакер наверняка попробует MF01, FRAME, MDF или MAINFRAME в качестве пароля. Если хакеру известно, что начальника кросс-монтажного зала зовут Питер Пинкертон, пароли PETE или PINKERTON будут крайне неудачным выбором.

Правила выбора паролей:

1. Пароли должны назначаться системными администраторами или уполномоченными лицами. Пользователи нередко выбирают пароли, не обеспечивающие никакой защиты. Пароли не должны быть в открытом доступе в компьютерном зале — их следует рассылать по внутренней почте соответствующим подразделениям.

2. Пароли следует менять часто, но в случайные промежутки времени — оптимально каждые четыре-семь недель. Руководителей подразделений необходимо уведомлять о смене паролей по почте за неделю. Это гарантирует, что все сотрудники будут своевременно осведомлены об изменениях. Нежелательно создавать массовую неразбериху, при которой все пытаются понять, почему не могут войти в свои компьютеры.

3. Пароли системных администраторов следует менять вдвое чаще, поскольку эти учётные записи открывают доступ ко всем ресурсам системы. По возможности учётные записи системных администраторов должны быть ограничены от входа через коммутируемые линии.

4. Пароль НИКОГДА не должен совпадать с именем учётной записи. Убедитесь, что ВСЕ стандартные пароли по умолчанию изменены.

5. Лучший вариант — использовать случайные последовательности букв и цифр, например: 3CB06W1, Q9IF0L4 или F4W21D0. Все пароли не обязательно должны быть одинаковой длины или формата. Импарато говорит: «Мы написали программу на PC, которая генерирует различные пароли безопасности для разных систем и гарантирует отсутствие дублирования».

6. Важно менять пароли всякий раз, когда сотрудник покидает компанию или переходит в другой отдел. Импарато говорит: «Когда менеджеры уходят из нашей организации, мы обязательно меняем те пароли, которые необходимы для работы системы».

7. Операционная система Unix имеет встроенную функцию «устаревания паролей» (password aging), которая требует обязательной смены паролей по истечении определённого времени. Если вы используете Unix-системы, обязательно активируйте эту функцию.

8. Если вы подозреваете, что произошёл инцидент безопасности, меняйте ВСЕ пароли, а не только те, которые непосредственно связаны с этим инцидентом.

C) Физическая безопасность объекта

Хакеры и авторы ряда статей, опубликованных в журнале 2600 Magazine, подробно описывали практику обыска мусорных контейнеров, которую сами хакеры называют «трэшинг» (trashing). Важно следить за тем, что вы выбрасываете. Во многих компаниях в мусор выбрасываются руководства по эксплуатации, содержащие конфиденциальную информацию. COSMOS сам по себе не является системой с дружественным интерфейсом. Иными словами, без предварительного знакомства с системой работать с ней крайне сложно. Беверли Крюз из Bellcore говорит: «COSMOS используется в таком количестве мест по всей стране, что я не удивлюсь, если в мусоре найдут документацию... особенно после разукрупнения AT&T. Один интересный момент: в статье о COSMOS, написанной хакерами, содержалось много устаревшей информации, что говорит о том, что источник этих сведений... был давним».

Правила физической безопасности объекта:

1. Хотя это может казаться очевидным, сотрудники должны предъявлять надлежащее удостоверение личности при входе в терминальные залы или компьютерные помещения. Вряд ли хакер когда-либо попытается физически проникнуть в офис, однако хакеры — не единственная угроза.

2. Призывайте сотрудников запоминать процедуры входа в систему наизусть. Плохая практика — записывать пароли на клочках бумаги и клеить их к терминалам. Рано или поздно такая бумажка может попасть не в те руки.

3. Мусор должен быть максимально защищён. При использовании частного вывоза держите мусор на погрузочных доках, в подвалах или в огороженных зонах. Если мусор вывозится городскими коммунальными службами, рекомендуется измельчать конфиденциальные материалы в шредере.

4. Прежде чем выбрасывать старые руководства или книги, проверьте, не могут ли ими воспользоваться другие подразделения. Чем больше сотрудников знакомы с системой, тем ниже вероятность проблем с безопасностью.

5. Печатающие терминалы должны проверяться на предмет того, не отображаются ли на них пароли. Если пароли выводятся на печать в открытом виде, проверьте правильность настройки режима дуплекса. Некоторые операционные системы позволяют настраивать коммутируемые линии для использования с принтерами.

D) Безопасность и работа с персоналом

Когда хакер выдаёт себя за сотрудника, велика вероятность, что инцидент останется незамеченным, — если только попытка не провалилась явно. Даже если хакер говорит невпопад, сотрудники зачастую спишут звонок на неосведомлённого или некомпетентного человека. Неприятно чувствовать себя обязанным относиться с подозрением к каждому звонку с незнакомым голосом, но это необходимо.

Правила безопасности при работе с персоналом:

1. При межотдельственных звонках всегда представляйтесь: 1) своим именем; 2) должностью; 3) отделом и местом нахождения.

2. С подозрением относитесь к звонящим, чей голос похож на детский, или к тем, кто задаёт нестандартные вопросы. Если кто-то вызывает подозрение, узнайте имя его руководителя и номер для обратного звонка. Не обсуждайте ничего конфиденциального до тех пор, пока не удостоверитесь в личности звонящего. Никогда не сообщайте пароли по телефону.

3. При возникновении проблем с безопасностью системы разошлите всем пользователям уведомления с предписанием не обсуждать систему по телефону, особенно с незнакомыми людьми.

4. Напоминайте всем пользователям коммутируемых линий о правилах безопасности перед завершением сеанса связи.

5. Если в рабочих помещениях разместить плакаты по вопросам безопасности, сотрудники станут внимательнее в работе и в телефонных разговорах.

6. Если руководители будут распространять эту и другие статьи по компьютерной безопасности среди начальников отделов, уровень защищённости со стороны персонала возрастёт.

E) Общие меры безопасности

Компания Bellcore недавно направила пакет документов всем системным администраторам систем COSMOS. В пакете подробно описаны процедуры безопасности, применимые к COSMOS и Unix-системам. Если вы получили этот пакет, рекомендуется перечитать его ещё раз, чтобы убедиться в защищённости ваших систем. Крюз говорит: «В прошлом году... ко мне обратился сотрудник одной из операционных компаний с проблемой безопасности COSMOS. Всё, что мы сделали, — предоставили им документацию, которая напомнила им о существующих функциях безопасности... В операционной системе COSNIX есть встроенные средства защиты... Мы не дали им ничего нового. Эти функции уже были там; мы лишь порекомендовали задействовать их все».

Если вы не уверены, что в полной мере используете доступные функции безопасности, обратитесь к поставщикам ваших компьютерных систем и запросите документацию по вопросам безопасности. Выясните, какие функции защиты вы, возможно, не используете. Существуют также сторонние программные компании, предлагающие пакеты безопасности для различных операционных систем и компьютеров.

Компьютерная безопасность — крайне деликатная тема. Многие предпочитают делать вид, что компьютерной преступности не существует. Поскольку проблема реальна, лучшее, что можно сделать, — изучать её и искать оптимальные решения. Чем больше людей будут писать и сообщать о компьютерной безопасности, тем легче остальным будет защитить себя. Я хотел бы, чтобы Bellcore опубликовала руководящие принципы безопасности, доступные всей телекоммуникационной отрасли. Помните: цепь прочна ровно настолько, насколько прочно её самое слабое звено.

Исследование сети DECNET

Автор: Deep Thought, Западная Германия

1 июня 1989 года

Отказ от ответственности: Автор не несёт никакой ответственности за использование или злоупотребление информацией, содержащейся в данной статье, а также за любой ущерб, причинённый применением описанных методов. DECNET, VAX и VMS являются возможно зарегистрированными товарными знаками компании Digital Equipment Corporation.

Рано или поздно каждый мало-мальски сообразительный программист задаётся вопросом: а трудно ли заниматься хакингом? Оказавшись в университетской сети, почему бы просто не попробовать? Поскольку ты являешься официальным студентом и в какой-то мере имеешь право пользоваться вычислительными ресурсами, тестирование современных средств коммуникации не должно повлечь никаких проблем.

Итак, начинаешь исследовать узлы, к которым у тебя есть официальный доступ, в поисках интересных программ и процедур. И находишь: Netdcl — всего лишь одна из многих программ, которая, судя по всему, позволяет выполнять команды на удалённых узлах без учётной записи на них. Действительно интересная вещь, поскольку разрешено почти всё то, что может делать обычный пользователь.

Уважаемый читатель, быть может, начнёт думать: разве не кричали всегда, что VMS является САМОЙ БЕЗОПАСНОЙ компьютерной системой, НЕПРОНИЦАЕМОЙ для хакеров? Ладно, спокойно: эта возможность может быть отключена, и потому, если у кого-то на его VAX хранятся суперсекретные данные, он, разумеется, заблокирует любое использование или злоупотребление этой функцией.

Акт второй. Где-то приходилось слышать о таинственных вещах под названием системные вызовы. Поскольку давно хотелось разобраться, как обрабатывать нажатия клавиш на VAX (задача, вовсе не тривиальная!), начинаешь более внимательно читать документацию, чтобы выяснить, как это сделать на Pascal.

Случайно листая страницы, обнаруживаешь функции, возвращающие информацию об идентификаторах пользователей. Это весьма кстати, поскольку знакомый, занимающийся университетской политикой, хочет разослать листовку по электронной почте всем зарегистрированным пользователям. На самом деле получить список всех пользователей совершенно несложно. Пример программы, пусть и написанной на Ассемблере, даже содержится в документации. Наслаждайтесь списком из 1000 идентификаторов пользователей с полной информацией о правах сетевого доступа. Программа на Pascal приведена в Приложении B (далее в этом файле).

Пароли, к сожалению, в этом списке не хранятся. Даже Системный оператор не имеет к ним доступа, так что это не такая уж большая потеря. Угадайте, какие пароли стоят у многих учётных записей? Верно, просто попробуйте имя пользователя. Поразительно, насколько беспечными бывают пользователи. Конечно, это проблема групповых учётных записей, к которым имеют доступ несколько пользователей и которые все должны знать пароль. Тем не менее дыра существует.

Настоящий хакер, однажды войдя в такую учётную запись, наверняка найдёт способы получить системные привилегии. Это требует глубоких знаний ядра VMS и является уже другой историей, которой я здесь касаться не буду.

Что такое DECNET?

DECNET — это средство, с помощью которого компьютеры компании Digital Equipment Corporation (DEC) могут быть соединены друг с другом. Каждый компьютер в этой сети имеет адрес, который обычно задаётся в виде x.y, где x — номер области (целое число), а y — номер узла в этой области, принимающий значения от 1 до 1023. Для обращения к узлам DECNET указывается единственное число, которое можно вычислить из x и y по следующей формуле:

```
nodenumber = x * 1024 + y
```

Узлы, особенно локальные (имеющие тот же номер области, что и ваш текущий узел), нередко имеют присвоенные им имена, чтобы их было легче запоминать.

Интересные команды DECNET

Чтобы получить (первый) список доступных узлов DECNET, попробуйте команду:

```
$ SHOW NET
```

Знак `$` (как и в последующих примерах) является стандартным приглашением VMS и вводить его не нужно. Эта команда выдаст список (будем надеяться) достижимых узлов. Каждая строка вывода содержит сетевой адрес в форме x.y и, как правило, имя, под которым известен данный узел.

Ваш текущий узел упоминается в первой строке: "VAX/VMS network status for local node X.Y Name". В большинстве случаев далее вы увидите список локальных узлов и строку "The next hop to the nearest area router is node XX.YY". Этот узел содержит больше информации о DECNET, чем тот, на котором вы сейчас находитесь. Если у вас есть учётная запись на указанном узле, войдите туда и попробуйте снова. Если нет — что ж, поиграйте с перечисленными локальными узлами и изучите команду NCP, описанную далее.

Итак, что можно делать с теми узлами, которые были упомянуты в выводе? Первая команда:

```
$ SET HOST <node>
```

Где ` — это либо имя узла, либо его номер (см. выше). Таким образом, если SDIVAX значился в списке SHOW NET как 42.13, можно попробовать как SET HOST SDIVAX, так и SET HOST 43021 (42*1024+13 = 43021). Скорее всего, вы увидите неприятный запрос Username:`. Дальше — сами.

Вторая возможность DECNET — электронная почта. В VMS программа MAIL умеет отправлять письма другим пользователям. Если вы и ваш друг оба имеют учётные записи в одной сети DECNET, можно послать ему письмо, зная имя или номер его узла, указав `SDIVAX::FREDDY` или `43021::FREDDY`.

Есть ещё PHONE. Это утилита для общения с другим (или несколькими) пользователями в сети DECNET. Если вы хотите позвонить Фредди, просто наберите `PHONE SDIVAX::FREDDY`. Если он вошёл в систему, его терминал подаст звонок, и если он ответит на звонок (командой `PHONE ANSWER`), вы сможете с ним поговорить. В PHONE есть ещё одна приятная возможность: можно запросить список активных пользователей на удалённом узле командой `%DIR SDIVAX`. Подробнее см. встроенную справку PHONE.

Следующая поистине мощная возможность DECNET — удалённый доступ к файлам. Корректные имена файлов в VMS состоят из компонентов: узел, диск, каталог и имя файла. Пример корректного имени файла: `SDIVAX::DISK$2:[NASA.SECRET]SDI.DOC`, причём некоторые компоненты могут

быть опущены и вместо них используются значения по умолчанию.

Имена файлов, включающие спецификацию узла, можно использовать почти во всех командах VMS — например, DIR, TYPE и COPY. Доступ к указанному файлу предоставляется, если защита файла разрешает доступ для всех (world), или если владельцем файла является пользователь DECNET. Этот псевдоидентификатор существует на каждом VAX и имеет пароль DECNET. Доступ к этой учётной записи ограничен сетевой обработкой, так что просто войти под именем Username=DECNET, password=DECNET нельзя. По умолчанию на каждом узле существует специальный каталог, принадлежащий пользователю DECNET. К этому каталогу можно обратиться, указав лишь имя узла без какой-либо информации о диске или каталоге:

```
$ DIR SDIVAX::
```

Если пользователи злоупотребляли этой возможностью, каталог может быть защищён или иным образом отключён.

Последняя описываемая здесь возможность — средство удалённой обработки команд. Если попытаться открыть файл со спецификацией:

```
$ SDIVAX::"task=foo.com"
```

Вместо открытия DCL-процедуры файл foo.com будет выполнен. Чтобы удобно пользоваться этой возможностью, были написаны программы для интерактивного взаимодействия с удалённым хостом. Командная процедура NETDCL.COM выполняет эту задачу и приводится в Приложении A (далее в этом файле). Изучите эту DCL-процедуру, чтобы узнать больше о возможностях DECNET.

Ключ к универсальному знанию

Среди программ на VAX есть одна жемчужина — NCP. Она охотно предоставит информацию обо всей сети DECNET. Запустить эту программу можно командой `MCR NCP` или выполнив `SET DEF SYS$SYSTEM` и затем `RUN NCP`. Воспользуйтесь встроенной справкой NCP (Network Control Program — программа управления сетью), чтобы узнать больше.

```
NCP> SHOW KNOWN NODES
```

Эта команда выдаёт список всех узлов, известных вашему текущему узлу, включая имена, которые можно использовать как спецификации узлов. Но это ещё не всё: можно подключиться к базе данных другого узла и получить список узлов, известных на удалённом узле:

```
NCP> SET EXEC SDIVAX
```

А затем снова выполнить команду `SHOW KNOWN NODES`. Эта возможность должна обеспечить вас почти бесконечным списком имён и номеров узлов.

Заключение

В DECNET доступно немало приятных возможностей. Возможно, я знаю не все из них, но надеюсь, что данная статья показала вам мощные инструменты, доступные в VMS для того, чтобы сделать работу в сети удобнее.

ПРЕДУПРЕЖДЕНИЕ: У автора был неприятный опыт общения с некоторыми администраторами узлов, которым не нравилось, что к их машинам обращаются через DECNET. Да, это оборотная сторона медали: каждая активность в DECNET записывается в протокольный файл, который ежемесячно распечатывается и удаляется. Поэтому следует соблюдать осторожность при

использовании DECNET.

Приложение А

Процедура NETDCL.COM (иногда называемая TELL.COM, NET.COM)

```
$ IF f$mode() .EQS. "NETWORK" THEN GOTO network
$ IF p1 .EQS. "" THEN READ/PROMPT="_Node: " sys$command p1
$ nodespec = p1 - "::"
$ nodename = f$extract(0,f$locate("""",nodespec),nodespec)
$! include the following line for "hard cases"
$! nodespec = nodespec+"""decnet decnet"""
$ ON WARNING THEN CONTINUE
$ CLOSE/ERR=open_server dcl_server
$open_server:
$ OPEN/READ/WRITE dcl_server 'nodespec'::"TASK=NETDCL"/ERROR=open_failure
$ ON WARNING THEN GOTO exit
$flush_output:
$ READ dcl_server record
$ IF record .EQS. "SEND_ME_A_COMMAND" -
  THEN GOTO send_command
$ WRITE sys$output record
$ GOTO flush_output
$send_command:
$ IF p2 .NES. "" THEN GOTO single_command
$ READ sys$command record /PROMPT="''nodename'> " /END=exit
$ record  := 'record
$ IF record .EQS. "EXIT" THEN GOTO exit
$ WRITE dcl_server record
$ GOTO flush_output
$single_command:
$ command := 'p2' 'p3' 'p4' 'p5' 'p6' 'p7' 'p8'
$ WRITE dcl_server command
$single_flush:
$ READ dcl_server record
$ IF record .EQS. "SEND_ME_A_COMMAND"-
$ THEN GOTO exit
$ WRITE sys$output record
$ GOTO single_flush
$open_failure:
$ ON WARNING THEN EXIT
$ COPY/LOG Netdcl.Com 'nodespec'::
$ WAIT 0:0:1
$ OPEN/READ/WRITE dcl_server 'nodespec'::"TASK=NETDCL"
$ ON WARNING THEN GOTO exit
$ GOTO flush_output
$exit:
$ CLOSE dcl_server
$ EXIT
$network:
$ OPEN/READ/WRITE dcl_link sys$net
$ SET NOON
$ dcl_verify = 'f$verify(0)'
$ DEFINE sys$output dcl_link:
$server_loop:
$ WRITE dcl_link "SEND_ME_A_COMMAND"
$ READ dcl_link dcl_string /END_OF_FILE=server_exit /ERROR=server_exit
$ 'dcl_string'
$  GOTO server_loop
$server_exit:
$ IF dcl_verify THEN set verify
$ CLOSE dcl_link
$ DEASSIGN sys$output
$ EXIT
```

Приложение В

ALLUSER.PAS — Вывод всех зарегистрированных пользователей

```
{
* alluser.pas - get names of all users
* by Deep, 1989
* This program is freely redistributable as long no modifications are made
* DISCLAIMER: I take no responsibility for any use or abuse of this
*             program.  It is given for informational purpose only.
*
* program history:
* 04-May-89   started
* 02-Jun-89   clean up of code
}
[inherit ('sys$library:starlet.pen')]
program alluser(input,output);

  type $word      = [word] 0..65535;
       $byte      = [byte] 0..255;
       $quadword  = record
                      lo,hi : unsigned;
                    end;
       $uquad  = record
                      lo,hi : unsigned;
                    end;
var
  id: unsigned;
  status, status2: integer;
  length: $WORD;
  attrib,context,context2,context3: unsigned;
  ident, ident2: unsigned;
  name: varying [512] of char;
  holder: $uquad;

begin

writeln('Alluser - use at your own risk!');
status := SS$_NORMAL;
{ id = -1 selects next identifier }
id := -1;
context := 0;
while (status <> SS$_NOSUCHID) do
   begin
   { find next identifier }
   status := $idtoasc(id,name.length,name.body,ident,attrib,context);
   if (status <> SS$_NOSUCHID) then begin
      write(pad(name,' ',16));
      if (ident div (65536*32768) > 0) then
         { it's a rights-list, so print the hex-value of the identifier }
         begin
         writeln(oct(ident,12));
         context2 := 0;
         context3 := 0;
         { find all holders of this right }
         repeat
            holder := zero;
            status2 := $find_holder(ident,holder,attrib,context2);
            if (holder.lo <> 0) then begin
                ident2 := ident;
                { get UIC and username }
                status := $idtoasc(holder.lo,name.length,name.body,ident2
                    ,attrib,context3);
                write('               ',pad(name,' ',16));
                writeln('[',oct(holder.lo div 65536,3),','
                    ,oct(holder.lo mod 65536,3),']');
              end;
         until (holder.lo = 0);
```

```
            end
         else
            { it's a UIC, so translate to [grp,user] }
            begin
            writeln('[',oct(ident div 65536,3),',',oct(ident mod 65536,3),']');
            end;
         end;
      end;
   end.
```

Эта статья была написана Deep Thought из Западной Германии. Если вам понравилась статья — предоставьте мне доступ, если я однажды загляну на ваш BBS!

Становление хакера

Автор: Framstag (Западная Германия)

2 июня 1989 года

Пролог для тех, кто не знаком с VMS

DECnet — это сеть для машин компании DEC, в большинстве случаев речь идёт о VAX-системах. DECnet позволяет выполнять следующее:
• электронная почта
• передача файлов
• удалённый вход в систему
• удалённое выполнение команд
• удалённая постановка заданий в очередь
• PHONE

PHONE — это интерактивное общение между пользователями, аналог команды TALK в UNIX или «расширенного» CHAT в VM/CMS.

BELWUE, университетская сеть федеральной земли Баден-Вюртемберг в Западной Германии, включает в себя (помимо прочих) сеть DECnet, насчитывающую около 400 VAX-машин. На каждой VAX есть стандартная учётная запись DECNET с паролем DECNET, которая недоступна для удалённого входа. Эта учётная запись предназначена для различных утилит DECnet и выполняет роль своеобразной гостевой записи. Учётная запись DECNET обладает крайне ограниченными привилегиями: нельзя редактировать файлы или осуществлять ещё один удалённый вход.

Меню HELP предоставляется системой и аналогично команде MAN в UNIX.

Дополнительную информацию о DECnet можно найти в статье «Looking Around In DECnet» за авторством Deep Thought в этом же номере Phrack Inc.

• -

Здесь, в Ульмском университете, у нас *невероятно* некомпетентный персонал вычислительного центра, к тому же страдающий острой нехваткой системной документации (если не считать 80 кг руководств VAX/VMS). Любой активный пользователь, интересующийся чем-то выше уровня «run», «FORTRAN» или «logout», вынужден искать информацию самостоятельно. К моему счастью, у меня есть другие учётные записи в BELWUE-DECnet, где пользователям предоставляется больше информации. Я обычный студент в Ульме, и все мои учётные записи совершенно легальны и соответствуют законодательству Германии. Я не называю себя «хакером» — скорее считаю себя «пользователем» (...это скорее вопрос терминологии).

В меню HELP на одном из хостов в Тюбингене я обнаружил файл netdcl.com и соответствующее описание, которое отправляет команды в учётную запись DECNET других VAX-машин и выполняет их там (удалённое выполнение команд). Объяснение в меню HELP было составлено так, что разберётся даже полный чайник — следовательно, справился и я :-)

С помощью команды `$ mcr ncp show known nodes` можно получить список всех активных в сети VAX-машин — как известно, это стандартная возможность — и я опросил все эти VAX-системы, разыскивая полезную информацию как жаждущий знаний пользователь. С помощью «help», «dir» и других подобных команд я просматривал содержимое тех учётных записей DECNET, всегда

обращая внимание на темы, связанные с сетью BELWUE. Жаль, что на 2/3 всех VAX-машин учётная запись DECNET заблокирована для NETDCL.COM. Системные администраторы там, по всей видимости, опасаются несанкционированного доступа, хотя я не могу представить себе, как он был бы возможен, ведь войти в эту учётную запись нельзя — никаких шансов для троянских программ и тому подобного.

Некоторые системные администраторы связались со мной после того, как я посетил их VAX, чтобы пообщаться о сети и спросить, могут ли они чем-нибудь помочь. Один сисоп из Штутгарта даже прислал мне версию NETDCL.COM для операционной системы ULTRIX.

А затем, спустя месяц, на меня обрушился У Ж А С в виде следующего письма:

```
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
From:   TUEBINGEN::SYSTEM       31-MAY-1989 15:31:11.38
To:     FRAMSTAG
CC:
Subj:   don't make any crap, or you'll be kicked out!

From:   ITTGPX::SYSTEM       29-MAY-1989 16:46
To:     TUEBINGEN::SYSTEM
Subj:   System-breaking-in 01-May-1989

To the system manager of the Computer TUEBINGEN,

On May 1st 1989 we had a System-breaking-in in our DECNET-account, which
started from your machine.  By help of our accounting we ascertained your user
FRAMSTAG to have emulated an interactive log-on on our backbone-node and on
every machine of our VAX-cluster with the "trojan horse" NETDCL.COM.  Give us
this user's name and address and dear up the occurrence completely.  We point
out that the user is punishable.  In case of repetition we would be forced to
take corresponding measures.  We will check whether our system got injured.  If
not, this time we will disregard any measure.  Inform us via DECnet about your
investigation results -- we are attainable by the nodenumber 1084::system

Dipl.-Ing. Michael Hager
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
```

Мой системный администратор пригрозил удалить мою учётную запись, если я немедленно не объясню произошедшее. *Сглотнул*!

Я осознавал свою невиновность, но как донести это до других? Я объяснил системному администратору всё шаг за шагом. Спустя некоторое время он понял меня, однако угроза уголовного преследования по-прежнему нависала надо мной... Поэтому я немедленно бросился к клавиатуре, чтобы составить объяснительный файл и отправить его тому разгневанному системному администратору в Штутгарте (узел 1084 — это институт там). Но выхода не было: у него закончилась квота на диск, и моё объяснительное письмо улетело в никуда:

```
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
$ mail explanation
  To:   1084::system
%MAIL-E, error sending to user SYSTEM at 1084
%MAIL-E-OPENOUT, error opening SYS$SYSROOT:[SYSMGR]MAIL$00040092594FD194.MAI;
as output
-RMS-E-CRE, ACP file create failed
-SYSTEM-F-EXDISKQUOTA, disk quota exceeded
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
```

Попытка связаться через PHONE также потерпела неудачу: в своей безграничной хакерской паранойе он отключил PHONE... А никакого списка с РЕАЛЬНЫМИ адресами виртуальных DECnet-адресов нигде нет (в целях защиты от хакеров). Так я и стоял с клеймом «ОПАСНЫЙ ХАКЕР!», не имея никакой возможности оправдаться. Я излил душу своему знакомому, который является сисопом в вычислительном центре Фрайбурга. Он стал опрашивать других сисопов и администраторов по всей сети BELWUE, пока через несколько дней кто-то не дал ему телефонный номер — и этот номер оказался верным!

Я позвонил этому Хагеру и рассказал ему, что я делал с его учётной записью DECnet, а также чего я НЕ делал. Я хотел узнать, какое именно преступление я совершил. Он незамедлительно отозвал все свои обвинения, однако так и не извинился за свои клеветнические инсинуации. Я попросил его уведомить моего системного администратора в Тюбингене о том, что я не совершил ничего противозаконного, и остановить его от удаления моей учётной записи. Именно это уже случилось с одним из моих однокурсников (и в том случае Хагер тоже был виновен). Он пообещал мне официально отозвать свои обвинения.

Спустя более чем неделю этого так и не произошло (мне по-прежнему разрешают пользоваться моей учётной записью). В качестве «компенсации» я получил новое письмо от Хагера на другую свою учётную запись:

```
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
From:   1084::HAGER         1-JUN-1989 12:51
To:     50180::STUD_11
Subj:   System-breaking-in

On June 1st 1989 you have committed a system-breaking-in on at least one of our
VAXes.  We were able to register this occurrence.  We would be forced to take
further measure if you did not dear up the occurrence completely until June
6th.

Of course the expenses involved would be imposed on you.  Hence enlightenment
must be in your own interest.

We are attainable via DECnet-mail with the address 1084::HAGER or via following
address:

Institut fuer Technische Thermodynamik und Thermische Verfahrenstechnik
Dipl.-Ing. M. Hager    Tel.: 0711/685-6109
Dipl.-Ing. M. Mrzyglod Tel.: 0711/685-3398
Pfaffenwaldring 9/10-1
7000 Stuttgart-80

 M. Hager
 M. Mrzyglod
--- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
```

Это была реакция на мою попытку: `$ PHONE 1084::SYSTEM`. На это письмо я не ответил. МНЕ ВСЁ ЭТО УЖЕ НАДОЕЛО!

Framstag
(FRAMSTAG@DTUPEV5A.BITNET)

С особой благодарностью Schrulli B. за помощь в переводе.

Отправка поддельной почты в Unix

Автор: Dark OverLord

26 мая 1989 г.

Ниже приведён shell-скрипт, с помощью которого можно отправлять поддельные письма с любой Unix-системы. Пользуйтесь на здоровье и не попадайтесь.

— Dark Overlord

```
#!/bin/sh
# fakemail — shell-скрипт для отправки поддельной почты.
# Настройка пути
PATH=/usr/ucb:/bin:$HOME/Bin
# Разбор командной строки
case $# in
0)echo "USAGE: user@host [ from@somewhere ] [ mailer_host ]" >& 2
exit 1
;;
1)mailto=$1
from="person@campus"
mailerhost=localhost
;;
2)mailto=$1
from=$2
mailerhost=localhost
;;
3)mailto=$1
from=$2
mailerhost=$3
;;
*)echo "USAGE: user@host [ from@somewhere ] [ mailer_host" >& 2
exit 1
;;
esac
# Создание заголовка для sendmail
cat <<E!O!F!> /tmp/cli$$
helo $mailerhost
mail from:$from<$from>
rcpt to: $mailto <$mailto>
data
From: $from
To: $mailto
Subject:
Status: RO


E!O!F!
# Редактирование письма
vi /tmp/cli$$
# Добавление завершающей части для mailer
cat <<E!O!F!>> /tmp/cli$$
.
quit
E!O!F!
# Подключение к демону sendmail удалённого хоста
telnet $mailerhost smtp < /tmp/cli$$
# Уборка за собой
/bin/rm -f /tmp/cli$$
```

Служба почтовой инспекции

(C) UNITED STATES POSTAL SERVICE (U.S. MAIL)

Автор: Vendetta

10 мая 1989 г.

Защита почты США

Ответственность за защиту почты США и почтовой системы в целом несёт Служба почтовой инспекции. Являясь правоохранительным и ревизионным подразделением Почтовой службы США, Инспекционная служба представляет собой высокоспециализированную профессиональную организацию, осуществляющую следственные, правоохранительные и ревизионные функции, необходимые для стабильной и надёжной работы почтовой системы.

Будучи старейшим федеральным правоохранительным органом страны, Инспекционная служба обладает юрисдикцией во всех уголовных делах, затрагивающих целостность и безопасность почты, а также сохранность всех почтовых ценностей, имущества и персонала.

С момента возникновения почтовой системы в этой стране криминальные и административные проблемы Почтовой службы были неразрывно связаны между собой. Выявляя и расследуя преступления против почты и почтовых доходов, создавая безопасные и эффективные почтовые системы, охраняя всё почтовое имущество, гарантируя, что почтовая система не используется в преступных целях в ущерб общественным интересам, Инспекционная служба играет неотъемлемую роль в поддержании эффективной работы Почтовой службы.

Деятельность ведомства вносит жизненно важный вклад в защиту экономики страны. Охранные и правоохранительные функции Инспекционной службы обеспечивают американскому бизнесу уверенность в безопасном обмене денежными средствами и ценными бумагами через почту США, а клиентам почты — гарантию неприкосновенности корреспонденции при её передаче в любые точки мира. Ревизии обеспечивают стабильность финансовых операций, помогают контролировать расходы и повышать эффективность Почтовой службы.

Почтовые инспекторы

Почтовые инспекторы — это оперативно-следственные агенты Почтовой службы США. Сегодня почти две трети своего рабочего времени они тратят на расследование и раскрытие почтовых преступлений. Наделённые законодательными полномочиями на производство арестов, они задерживают нарушителей закона и тесно сотрудничают с прокурорами США при рассмотрении дел в суде. В круг их обязанностей также входят профилактика преступлений, ревизия почтовых операций, расследование несчастных случаев и широкий спектр других служебных и ревизионных вопросов.

Работа почтового инспектора требует полной самоотдачи и готовности к ненормированному рабочему дню. Расследования почтовых преступлений нередко предполагают межштатную или международную координацию; ответственность за восстановление почтового сообщения после таких катастроф, как наводнения, пожары и авиакатастрофы, отнимает много времени и может

быть сопряжена с опасностью.

В Соединённых Штатах и Пуэрто-Рико насчитывается около 1 900 почтовых инспекторов. Все стажёры проходят одиннадцатинедельный базовый курс подготовки, охватывающий обращение с огнестрельным оружием, тактику самозащиты, правовые вопросы, обыск и изъятие, техники задержания, судебные процедуры, почтовые операции, ревизионные функции и детальное изучение федеральных законов, попадающих под юрисдикцию Инспекционной службы. Занятия проводятся в учебном центре Инспекционной службы в Потомаке, штат Мэриленд.

Курсы повышения квалификации позволяют инспекторам быть в курсе текущих судебных решений, законов и правовых процедур. Постоянно проводятся дополнительные специализированные курсы, обеспечивающие Службу высококвалифицированными кадрами.

Все кандидаты на должность почтового инспектора обязаны успешно пройти следующие этапы: вступительный экзамен; всестороннюю проверку биографических данных, включающую медицинское освидетельствование; прохождение Центра оценки кандидатов; и все этапы базового курса подготовки.

Деятельность Инспекционной службы

Уголовные расследования и профилактика почтовых преступлений составляют наибольшую долю в деятельности Инспекционной службы.

Почтовые инспекторы расследуют нарушения всех почтовых законов и сопутствующие уголовные правонарушения. К преступлениям, входящим в сферу почтовых расследований, относятся: почтовое мошенничество, незаконная пересылка контролируемых веществ через почту США, рассылка детской порнографии, хищение почтовых отправлений или почтовых ценностей, нападения на сотрудников почты, отправка бомб по почте или направление их против почтового имущества, а также рассылка ядовитых веществ, незарегистрированного оружия и вредных или запрещённых предметов.

Пять криминалистических лабораторий, расположенных по всей стране, помогают инспекторам анализировать доказательные материалы, необходимые для установления личности и отслеживания подозреваемых в преступлениях, а также для дачи экспертных показаний на судебных процессах.

Целью профилактики почтовых преступлений является предвидение, выявление и анализ областей наибольшего криминального риска, потенциально затрагивающих сотрудников, денежные средства, имущество и клиентов почты. Затем почтовые инспекторы принимают меры для устранения или снижения этого риска и поддержания целостности Почтовой службы.

> *«Служба почтовой инспекции отвечает за внутренний аудит Почтовой службы.»*

Почтовые инспекторы обеспечивают руководство независимыми ревизиями и расследованиями всей почтовой деятельности в рамках системы внутреннего контроля Почтовой службы.

Проверки объектов и систем защищают активы Службы, совершенствуют систему финансового управления, помогают разрешать жалобы клиентов, расследуют вопросы, представляющие интерес для Конгресса, и выявляют конкретные меры по улучшению обслуживания клиентов и снижению операционных затрат.

Финансовые ревизии обеспечивают независимую проверку адекватности и эффективности систем контроля, подтверждают наличие активов и надлежащее соблюдение мер их защиты. Операционные ревизии проводятся для оказания помощи руководству почты в организации

эффективной и надёжной работы Почтовой службы.

Служба безопасности

Офицеры почтовой полиции обеспечивают защиту почтовых отправлений, почтовых ценностей, сотрудников, объектов и транспортных средств Почтовой службы. Являясь частью правоохранительной команды, они помогают почтовым инспекторам соблюдать определённые почтовые законы и нормативные акты на территории почтовых объектов и обеспечивают мобильное реагирование в экстренных ситуациях, связанных с Почтовой службой.

Оснащённые портативными рациями и оповещаемые посредством системы видеонаблюдения замкнутого контура, они обеспечивают охрану периметра крупных почтовых объектов и других зданий, эксплуатируемых Почтовой службой. Их присутствие на почтовых объектах по всей стране служит сдерживающим фактором для почтовых преступлений и способствует поднятию морального духа сотрудников.

Офицеры почтовой полиции также привлекаются для сопровождения ценных почтовых отправлений в пути между почтовыми подразделениями и в аэропортах.

Опыт в военном или гражданском правоохранении, промышленной безопасности или аналогичных сферах деятельности является преимуществом при поступлении на должности в Службу безопасности. Все принятые на работу проходят четырёхнедельный курс подготовки в учебном центре Инспекционной службы.

Взаимодействие с другими ведомствами

Инспекционная служба оказывает полное содействие всем местным и федеральным следственным и прокурорским органам в правоохранительной деятельности в целях обеспечения более надёжной защиты населения. Почтовые инспекторы участвуют в работе национальных оперативных групп Министерства юстиции, направленных на пресечение широко распространённых преступных действий организованного характера. Почтовые инспекторы также тесно сотрудничают с внешними аудиторами, оказывая поддержку при сертификации финансовой отчётности Почтовой службы.

Процент обвинительных приговоров

Инспекционная служба стабильно поддерживает высокий процент обвинительных приговоров — около 98% от числа дел, переданных в суд, — что не превзойдено ни одним другим федеральным правоохранительным органом.

Юрисдикция, почтовые законы и охрана

Инспекционная служба осуществляет следственную юрисдикцию приблизительно в отношении 85 почтовых законодательных актов. Их можно разделить на две категории: уголовные действия

против почты, почтовых объектов или почтового персонала; и уголовное злоупотребление почтовой системой.

ПОЧТОВОЕ МОШЕННИЧЕСТВО

Вся преступная деятельность с использованием почты США с целью обмана подпадает под юрисдикцию Службы почтовой инспекции. Закон о почтовом мошенничестве является старейшим законом о защите прав потребителей в Соединённых Штатах и представляет собой одно из наиболее эффективных прокурорских инструментов в борьбе с беловоротничковой и организованной преступностью. Ежегодно вследствие почтового мошенничества теряются миллионы долларов, причём жертвами становятся не только малоимущие и пожилые граждане, но и предприниматели, и рядовые потребители. К распространённым схемам относятся: страховые, банковские и фиктивные расчётные мошенничества; земельные аферы и мошенничество с авансовыми платежами; франчайзинговые схемы; мошенничество с надомной работой и поддельными дипломами; благотворительные схемы; продвижение фальшивых средств лечения, косметических приборов, чудодейственных диет и сексуальных стимуляторов; цепные письма, лотереи и предложения о покупке рекламной продукции.

Хотя почтовые инспекторы не имеют законодательных полномочий выступать посредниками при урегулировании неудовлетворительных финансовых или имущественных сделок, осуществлённых через почту, их расследования нередко приводят к прекращению мошеннических или сомнительных операций. Административные приказы о прекращении доставки почты могут выдаваться для предотвращения продолжающегося ущерба для населения в период сбора достаточных доказательств для уголовного преследования в судах, а также в случаях, когда можно доказать наличие ложных заявлений, но не обязательно мошеннического умысла. Инспекционная служба играет ведущую роль в защите прав потребителей благодаря реализации образовательных программ, направленных на предотвращение схем почтового мошенничества, и усилиям по разрешению жалоб, связанных с недопониманием между потребителями и продавцами или ненадлежащей деловой практикой.

ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ

Расследования почтовыми инспекторами дел, связанных с организованной преступностью, чаще всего касаются хищений и сбыта крупных объёмов марочных запасов и ценных бумаг организованными преступными группами, взламывающими почтовые отделения; страховых и инвестиционных мошенничеств; а также спланированных банкротств и схем, направленных на разграбление активов компаний. Закон о контроле над организованной преступностью 1970 года прямо включает нарушение Закона о почтовом мошенничестве в число «рэкетирских действий». Почтовые инспекторы прикомандированы к оперативным группам Министерства юстиции по борьбе с организованной преступностью, действующим в различных точках страны.

ХИЩЕНИЕ/ВЗЛОМ/ОГРАБЛЕНИЕ ПОЧТЫ

Расследование хищений почтовых отправлений составляет значительную часть обязанностей Инспекционной службы и чаще всего связано с похищением чеков, продовольственных купонов или иных оборотных ценных бумаг. Приоритетное внимание уделяется крупным преступным группировкам, изощрённым операциям по сбыту похищенного, масштабным хищениям и реализации профилактических программ.

Взломы почтовых отделений варьируются от вандализма до действий высокоорганизованных преступных группировок, занимающихся взломами и перепродажей похищенного в рамках организованной преступной деятельности.

Вооружённые ограбления создают угрозу жизни сотрудников почты и населения и потому являются приоритетными для расследования. Объектами таких преступлений, как правило, становятся почтовые объекты, транспортные средства, перевозящие почту, и отдельные сотрудники — прежде всего почтальоны.

НАРКОТИКИ

Незаконный оборот наркотиков, наркотических средств и других контролируемых веществ через почту расследуется совместно с другими федеральными и региональными правоохранительными органами.

ПОРНОГРАФИЯ

Инспекционная служба расследует нарушения Закона о почтовой непристойности, принятого в 1865 году, который запрещает пересылку непристойных материалов через почту США. Это включает расследование преступлений, связанных с детской порнографией, предполагающей сексуальное насилие или эксплуатацию детей, на основании законов, принятых в 1977 и 1984 годах.

ВЗРЫВНЫЕ УСТРОЙСТВА

Расследование инцидентов, связанных с угрозами применения взрывных устройств и зажигательных предметов, пересылаемых по почте или направленных против почтового имущества или деятельности, входит в юрисдикцию Инспекционной службы.

ВЫМОГАТЕЛЬСТВО

На Инспекционную службу возложена следственная ответственность в случаях, когда почта используется для вымогательства денег или имущества путём угрозы нанесения ущерба репутации лица или обвинения его в совершении преступления.

ИНЫЕ ЗАПРЕЩЁННЫЕ ПОЧТОВЫЕ ОТПРАВЛЕНИЯ

Рассылка ядов или других вредных веществ, запрещённых законом, расследуется почтовыми инспекторами.

Помощь со стороны населения

В большинстве случаев Инспекционная служба вынуждена опираться на бдительность и внимательность получателей почтовых отправлений, которые должны сообщать о возможной преступной или вредоносной деятельности с использованием почты. О любых подозрительных нарушениях почтовых законов или злоупотреблениях почтой следует сообщать местному постмастеру для передачи информации почтовому инспектору. Оперативные действия со стороны клиентов почты и почтовых инспекторов играют ключевую роль в профилактике и раскрытии преступлений.

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN               Issue XXVII/Part 1            PWN
PWN                                             PWN
PWN                  June 20, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Добро пожаловать в выпуск XXVII Phrack World News!

В этом номере — материалы о хакерской афёре SouthernNet, инциденте с нарушением условий испытательного срока во Флориде, электронных досках объявлений в Аргентине, факс-атаках, компьютерной безопасности и других хакерских историях, а также новые статьи и свежая информация о Кевине Дэвиде Митнике (он же Condor), Роберте Тэппане Моррисе, Карле Кохе (Hagbard Celine, один из «хитрых хакеров» Клиффорда Столла), о TRW и Администрации социального обеспечения, о «супербазе данных» Национального центра криминальной информации (NCIC) и о многом другом интересном.

В связи с нашим временным отлучением от Bitnet этот выпуск станет последним регулярным номером Phrack World News до следующей осени. В следующем выпуске ожидайте подробный отчёт о деталях и весёлых событиях SummerCon '89. До него остаётся всего два дня с момента написания этих строк (для некоторых из нас всё начинается в четверг вечером), и это обещает стать лучшим SummerCon за всё время!

Особая благодарность Delta Master, Hatchet Molly и The Mad Hacker, которые помогли с этим номером PWN, предоставив свои материалы. Hatchet Molly будет выполнять роль агента по сбору материалов для Phrack Inc. в течение лета. Обязательно пересылайте ему любые новостные статьи, которые кажутся вам актуальными для PWN, — он передаст их мне (рано или поздно). С ним можно связаться в широких сетях по адресам:

```
(Hatchet Molly)

TK0GRM2@NIU.BITNET
TK0GRM2%NIU.BITNET@CUNYVM.CUNY.EDU
```

Ещё одна вещь, которую стоит упомянуть, — особый привет одному из наших читателей из правительства... Питеру Эдмонду Йи из Исследовательского центра NASA «Эймс». Он недавно заметил, что «имеет доступ к Phrack!» Интересно, думал ли он, что Phrack Inc. — это совершенно секретное издание, которое сложно достать? Но раз уж ему так нужен Phrack, мы с Taran King решили: «А почему бы не облегчить ему жизнь и просто не отправить на его сетевой адрес?» Так и сделали :-)))

:Knight Lightning

«Настоящее будущее у тебя за спиной... И это только начало!»

—

Судья отклонил сделку о признании вины Митника как слишком мягкую — 25 апреля 1989

Выдержки из материала Ким Мёрфи (Los Angeles Times)

> *«Мистер Митник, вы занимаетесь этим слишком долго, и никто вас по-настоящему не наказал. Это последний раз, когда вы это сделаете.»*

Как сообщается, федеральный окружной судья Мариана Пфэлзер неожиданно отклонила сделку о признании вины Кевина Митника — хакера, которого когда-то называли «столь же опасным с клавиатурой, как грабитель банка с пистолетом». Пфэлзер заявила, что Митник заслуживает более длительного тюремного срока.

Как сообщалось в недавних выпусках Phrack World News, «Митник признал себя виновным по одному пункту в компьютерном мошенничестве и одному пункту во владении несанкционированными кодами дальней телефонной связи... Митнику грозит один год лишения свободы. По соглашению о признании вины с правительством он также обязан находиться под наблюдением офицеров испытательного срока в течение трёх лет после освобождения из тюрьмы».

24 апреля 1989 года судья Пфэлзер заявила: «Мистер Митник, вы занимаетесь этим слишком долго, и никто вас по-настоящему не наказал. Это последний раз, когда вы это сделаете». Она сообщила, что конфиденциальный доклад с рекомендациями по вынесению приговора предложил ей превысить даже максимальный 18-месячный срок лишения свободы, предусмотренный новыми обязательными федеральными руководящими принципами по назначению наказания. Решение судьи аннулировало признание Митника виновным.

И прокуроры, и адвокаты защиты были удивлены. Адвокат Митника сказал, что не знает, согласится ли его клиент на признание вины с более длительным сроком заключения. Это может затруднить предъявление обвинений предполагаемым сообщникам Митника. Если дело Митника дойдёт до суда, для его осуждения потребуются показания как минимум одного из его сообщников, а те не стали бы давать показания без получения иммунитета от уголовного преследования.

Хакер-компьютерщик работает над новой сделкой о признании вины — 6 мая 1989

Выдержки из Los Angeles Herald Examiner

По словам адвокатов, вчера они ведут переговоры о второй сделке о признании вины для хакера Кевина Митника, чьё первое предложение признать вину было отклонено судьёй как предусматривающее слишком малый срок лишения свободы.

Митник, 25 лет, из Панорама-Сити (Калифорния), в марте предложил отбыть один год в тюрьме и признать себя виновным в компьютерном мошенничестве и владении несанкционированными кодами дальней телефонной связи.

Обновление по делу Митника — 10 мая 1989

Выдержки из Los Angeles Times

Когда мы в последний раз слышали о Кевине Митнике — хакере, которого когда-то называли «столь же опасным с клавиатурой, как грабитель банка с пистолетом», — судья Мариана Пфэлзер отклонила сделку о признании вины как слишком мягкую, заявив, что Митник заслуживает большего, чем оговорённый один год заключения [см. статьи выше].

Согласно более свежей информации, Митник заключил новое соглашение без оговорённого срока лишения свободы. Он признал себя виновным в краже программы обеспечения безопасности DEC и незаконном владении 16 кодами дальней телефонной связи, принадлежащими MCI Telecommunications Corp. По обоим пунктам предусмотрено максимальное наказание — 15 лет лишения свободы и штраф в размере 500 000 долларов. Правительство согласилось снять телефонные ограничения, введённые в отношении Митника с момента его заключения под стражу в декабре 1988 года.

По просьбе DEC Митник поможет компании выявить и устранить уязвимости в её программном обеспечении безопасности, чтобы защититься от других хакеров. Он также будет сотрудничать в расследовании правительством дела Леонарда ДиЧикко, хакера-сообщника. (ДиЧикко — это тот самый «друг», который сдал Митника властям.)

Кеннет Сиани высказывается о Кевине Митнике — 23 мая 1989

Кевин Митник — хакер, «настолько опасный, что ему даже нельзя пользоваться телефоном». «Он может разрушить вашу жизнь с помощью клавиатуры». «Вооружён клавиатурой и считается опасным».

Вот что говорят об этом человеке. Весь этот медиашум был бы терпим, если бы он просто продавал газеты. Но он сделал куда больше, чем продал несколько номеров. Он повлиял на тех, кто в конечном счёте решит его судьбу. Я лично не знаком с этим человеком, но разговаривал с теми, кто его знает. В том числе с одним из людей, расследовавших дело Митника. Из всего, что я о нём слышал, я считаю его мерзавцем! Но даже мерзавца не следует загонять в тюрьму, если другие, виновные в равной или большей степени, избежали наказания.

Лично я считаю, что это просто преступник — как тот парень, который грабит магазин, ничуть не лучше, но и не хуже. К сожалению, его воспринимают как «СУПЕР-ХАКЕРА» какого-то сорта. Глава отдела по компьютерным преступлениям полицейского департамента Лос-Анджелеса процитирован так: «Митник находится на несколько уровней выше того, что вы бы охарактеризовали как компьютерный хакер».

Без всякого неуважения, но подобное заявление от руководителя подразделения по компьютерным преступлениям свидетельствует о его незнании возможностей хакеров и телефонных фрикеров. Да, он делал такие вещи, как получение доступа и, возможно, изменение уголовных записей полицейского департамента, кредитных записей в TRW Corp. и Pacific Telephone, отключение телефонов людей, которые ему не нравились, и тому подобное. Но большинство людей, не связанных с хакерским/фрикерским миром, не понимают: ВСЁ ЭТО ОЧЕНЬ ЛЕГКО ДЕЛАЕТСЯ И ДЕЛАЕТСЯ ПОСТОЯННО. В сообществе хакеров и фрикеров подобные манипуляции с компьютерными и телефонными системами проще простого. Я не вижу ничего особенного в его способностях. Единственное, что отличает Кевина Митника, — это то, что он не «начинающий» хакер, как большинство тринадцатилетних ребят, которых ловят за взлом и фрикинг. Прошло немало лет с тех пор, как был арестован «продвинутый» хакер. Со времён банды Inner Circle у правоохранительных органов не было опыта работы с хакером такого уровня. Как правило, продвинутых хакеров ловят не за их деятельность — почти всегда их сдают другие. Поэтому понятно, почему его способности воспринимаются как экстраординарные, хотя на самом деле это

не так.

Из-за всей медиашумихи вокруг этого дела я опасаюсь, что:

1. С ним не обойдутся справедливо. Его будут судить как несравненно большую угрозу обществу, чем других, совершивших аналогичные преступления.

2. Он станет своего рода народным героем. Джесси Джеймс с клавиатурой. Это лишь подтолкнёт других идти по его стопам.

Я не защищаю ни его, ни то, что он делал, ни в каком смысле. Всё, что я говорю: давайте будем справедливы. Судите человека по фактам, а не по заголовкам.

Примечание: изложенные здесь взгляды являются моими личными.

Кеннет Сиани, старший специалист по безопасности, отдел информационных систем, NYMA Inc.

Если вы ищете другие статьи о Кевине Дэвиде Митнике, известном под псевдонимом Condor, обратитесь к:

• «Pacific Bell Means Business» (10/06/88) PWN XXI, Часть 1
• «Dangerous Hacker Is Captured» (Без даты) PWN XXII, Часть 1
• «Ex-Computer Whiz Kid Held On New Fraud Counts» (12/16/88) PWN XXII, Часть 1
• «Dangerous Keyboard Artist» (12/20/88) PWN XXII, Часть 1
• «Armed With A Keyboard And Considered Dangerous» (12/28/88) PWN XXIII, Часть 1
• «Dark Side Hacker Seen As Electronic Terrorist» (01/08/89) PWN XXIII, Часть 1
• «Mitnick Plea Bargains» (03/16/89) PWN XXV, Часть 1

___

Сеть компьютерного взлома в Детройте — 25 мая 1989

Взято из San Jose Mercury News (Knight-Ridder News Service)

ДЕТРОЙТ — Агенты Секретной службы в среду, 24 мая, разгромили то, что они охарактеризовали как дорогостоящую, сложную сеть компьютерных взломов, и были удивлены, обнаружив, что она в основном состоит из подростков.

По данным агентов, исполнявших ордера на обыск по всей стране, были взломаны компьютерные системы более 20 компаний, включая Министерство финансов штата Мичиган, кабельный телеканал Home Box Office и [RCA].

Федеральные чиновники заявили, что взломы этой сети нанесли ущерб в виде мошенничества на сумму от 200 000 до 1,5 миллиона долларов в виде присвоенных товаров, телефонного и компьютерного времени.

Агенты ожидали арестовать взрослых людей, когда нагрянули к восьми предполагаемым руководителям сети в нескольких штатах. Вместо этого они обнаружили только одного взрослого — в Чикаго. Остальные оказались подростками от 14 лет: двое в Колумбусе (Огайо), двое в Бостоне (Массачусетс), двое в Стерлинг-Хайтс (Мичиган) [The Outsider и The Untouchable] и один в Атланте (Джорджия). Агенты рассчитывали произвести ещё один арест в Лос-Анджелесе.

Официальные лица сообщили, что по меньшей мере ещё 55 человек по всей стране пользовались информацией сети.

В Стерлинг-Хайтс агенты Секретной службы вытащили из школы двух мальчиков-восьмиклассников, обоим по 14 лет, и допросили их в присутствии родителей, которые,

судя по всему, не знали о деятельности своих детей. Джеймс Хьюс, специальный агент, возглавляющий офис Секретной службы США в Детройте, сообщил, что подростки признали причастность к схеме.

Он пояснил, что восьмиклассники, будучи несовершеннолетними, не могут быть привлечены к ответственности по федеральным законам и будут переданы местным органам по делам несовершеннолетних.

По мнению властей, вдохновительницей является Линн Дусетт, 35 лет, из Чикаго. Она была арестована в среду, 24 мая, и сотрудничает со следствием, сообщил Хьюс.

Дусетт, осуждённая в Канаде за телекоммуникационное мошенничество, содержит себя и двоих детей за счёт компьютерных взломов, включая использование краденых или поддельных кредитных карт для получения наличных авансов или денежных переводов, — согласно аффидавиту, поданному в Федеральный окружной суд США.

В случае осуждения ей грозит до 10 лет лишения свободы и штраф в размере 250 000 долларов.

Особая благодарность Jedi за дополнительную информацию

—

HR 1504 — Закон о предотвращении злоупотребления пейджерами — 22 мая 1989

«Пейджеры не совершают преступлений — это делают конгрессмены.»

Дураки в конгрессе снова взялись за своё. Три года тюрьмы за продажу пейджера несовершеннолетнему? Если вы не верили Эбби Хоффману, когда он говорил, что истерия вокруг наркотиков — лишь предлог для усиления контроля над гражданами, подумайте ещё раз.

В USA Today вышла «дискуссия» по этому вопросу. Согласно статье, представитель Квеиси Мфуме (демократ от Мэриленда) говорит следующее:

> *«Наркобизнес использует новейшие технологии для продвижения своей смертоносной торговли. Одним из таких достижений является пейджер, который теперь появляется в классах и на школьных дворах. Я внёс Закон о предотвращении злоупотребления пейджерами, чтобы ограничить использование пейджеров молодёжью, торгующей наркотиками. Он обяжет Федеральную комиссию по связи предписать правила, ограничивающие владение пейджерами и их использование лицами моложе 21 года. Сотрудники правоохранительных органов говорят, что дилеры и поставщики отправляют в школу молодёжи закодированные сообщения через пейджер. Коды расшифровываются в сообщения вроде «встреть меня после уроков на нашем обычном месте, чтобы забрать наркотики». Наркоторговцы сейчас даже используют номера 800, доступные в региональных пейджинговых службах. Поставщик мог бы фактически проводить сделку в Балтиморе, находясь в Майами, например.*
> *Мой законопроект, H.R. 1504, обяжет любого продавца или арендодателя пейджинговых устройств проверять удостоверение личности и возраст каждого клиента; побудит родителей и предприятия взять на себя большую ответственность за деятельность своих детей или сотрудников; сделает незаконным для лица умышленную аренду, продажу или использование пейджинговых устройств в нарушение правил, предписанных FCC (предусмотрены суровые штрафы и до трёх лет лишения свободы для взрослых, незаконно предоставляющих пейджеры молодёжи); и обяжет родителей или предприятия, разрешающие использование пейджеров, указывать это намерение в аффидавите при покупке.»*

Он также добавляет, что признаёт наличие законных применений пейджеров, но мы больше не можем стоять в стороне и смотреть, как наркотики льются в наши кварталы. Противоположную позицию занимает Линн Скарлетт из Санта-Моники (Калифорния). Она спрашивает, какое отношение пейджеры имеют к наркоторговле, и утверждает, что регулирование их использования не нанесёт ей никакого урона. Она также говорит, что мало свидетельств того, что контроль над оружием лишает бандитов пистолетов, и для того, чтобы не дать пейджеры злоумышленникам, потребуется хорошая доза волшебства. Она заканчивает словами:

> *«Логика Закона о предотвращении злоупотребления пейджерами открывает дверь для законов, обязывающих нас подписывать обещания, что мы, клянёмся, не будем использовать эти вещи в незаконных целях при покупке. Де Токвиль, выдающийся наблюдатель нашей нации, предупреждал, что наша свобода будет исчезать через принятие тихих, кажущихся невинными и благонамеренными законов — таких законов, как H.R. 1504.»*

___

Ассоциация исследования компьютерных угроз (Великобритания) — 31 марта 1989

Для тех, кто интересуется: в Соединённом Королевстве была создана зонтичная организация для координации информации и исследований во всех аспектах компьютерной безопасности. В первую очередь одной из главных задач организации станет борьба с угрозой компьютерных вирусов — она будет выступать в роли информационного центра по вирусам и программному обеспечению для контроля над ними.

Ниже приводится копия первоначального письма, разосланного потенциальным членам:

The Computer Threat Research Association

Ассоциация исследования компьютерных угроз, CoTra — некоммерческая организация, созданная для исследования, анализа, публичного освещения и поиска решений угроз целостности и надёжности компьютерных систем.

Причиной создания CoTra послужил рост числа компьютерных вирусов. Эта проблема окутана страхом, неопределённостью и сомнениями. Для рядового пользователя компьютерный вирус и его последствия — это тревога неизвестного масштаба. Для немногих несчастливчиков, чьи системы стали жертвами, это критический вопрос.

Главным преимуществом членства в CoTra станет доступ к советам и информации. Консультации будут предоставляться через публикации, электронную конференцию (в системе Compulink CIX создана закрытая конференция для членов CoTra), а также через другие каналы, например рассылки напрямую членам при обнаружении нового вируса.

Членство в CoTra будет доступно на студенческой, полной или корпоративной основе. Всё программное обеспечение, находящееся в распоряжении CoTra и повышающее надёжность систем, — например, ПО для обнаружения и удаления вирусов — будет доступно всем членам. Планируется установить скидки у поставщиков инструментов и услуг по обеспечению надёжности. Библиотека исходных кодов вирусов, исполняемых файлов и других опасных исследовательских материалов будет предоставлена членам, которые смогут обосновать соответствующую необходимость.

CoTra опубликует реестр консультантов, обладающих конкретными навыками в области надёжности систем, а также обзоры программного обеспечения, повышающего надёжность.

Ваша поддержка CoTra обеспечит вам самую раннюю и точную информацию о потенциальных угрозах вашим компьютерным системам.

CoTra, The Computer Threat Research Association,
c/o 144 Sheerstock, Haddenham, Bucks. HP17 8EX

—

Странный отдел часов Таможенной службы — 1 мая 1989

Написано Ванессой Джо Гримм (Government Computer News, стр. 6)

Прокуратура США по Вашингтону рассматривает обвинение в том, что чиновник Таможенной службы нарушил Закон о компьютерной безопасности [предположительно PL 100-235], изменив внутренние часы компьютера.

Инспектор General Министерства финансов Майкл Р. Хилл передал обвинение прокурору после расследования расходов в конце года, произведённых чиновниками Таможни в конце финансового 1988 года. Обвинение касается чиновника, который, возможно, дал разрешение на изменение даты, хранимой компьютерами, которые агентство использует для документов о государственных закупках, — по словам Мориса С. Муди, директора по аудиту Службы финансового управления при инспекторе General.

Муди недавно сообщил подкомитету Комитета Палаты представителей по путям и средствам по надзору, что компьютеры являются частью Автоматизированной коммерческой системы агентства. Он отказался сообщить Government Computer News дополнительные подробности.

По имеющимся данным, компьютерные часы были переведены назад в первые три дня октября 1988 года, чтобы 41,8 миллиона долларов в виде обязательств по закупкам были датированы сентябрём в счёт ассигнований финансового 1988 года, — сообщил Муди.

Доклад инспектора General, опубликованный в конце февраля, пришёл к выводу о том, что Таможня не нарушала законы о государственных закупках. Тем не менее расследование инспектора продолжается.

«Неужели никого не беспокоят закупки на 41,8 миллиона долларов в последний день финансового года?» — спросил представитель Ричард Т. Шульце (республиканец от Пенсильвании). Закупки действительно насторожили инспектора General, сообщил Муди, и именно это беспокойство привело к привлечению прокурора США. «Эта проблема носит системный характер в федеральном правительстве, — сказал он. — Расходы в конце года — обычное явление».

Уильям Ф. Райли, контролёр Таможни, сообщил, что знал об откате часов, однако он и заместитель уполномоченного Майкл Х. Лейн отказались называть того, кто дал соответствующее разрешение... Члены подкомитета продолжали давить на Райли и Лейна. «Этот человек всё ещё работает в Таможне?» — спросил председатель подкомитета Дж. Дж. Пикл (демократ от Техаса). «Он работает на полную ставку и на той же должности, что и тогда», — ответил Лейн.

Представитель Берил Ф. Энтони-младший (демократ от Арканзаса) спросил, как Райли узнал об откате часов. «Он (чиновник, давший разрешение) сообщил мне, что это будет сделано», — ответил Райли.

Представитель Пикл предположил, что подобное решение мог принять только высокопоставленный чиновник, однако советник порекомендовал Лейну не отвечать. Тот лишь сообщил, что ни он, ни уполномоченный Фон Рааб этого решения не принимали.

Остальная часть статьи посвящена действиям Линды Гиббс, которая узнала об инциденте и сообщила о нём инспектору General после того, как не смогла остановить происходящее. Гиббс также утверждала, что целью этих действий было использование свободных средств конца года для покрытия перерасхода по контракту с Northrop Corp. Она также заявила, что была переведена на другую должность и не получала никаких новых обязанностей.

Phrack World News — Мировые новости Phrack

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN               Issue XXVII/Part 2            PWN
PWN                                             PWN
PWN                  June 20, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Роберт Т. Моррис отчислен из Корнелла — 25 мая 1989 г.

Источник: New York Times

Корнеллский университет отчислил аспиранта, которого университетские чиновники называют автором «интернет-червя».

В письме от 16 мая, адресованном Роберту Тэппану Моррису (23 года), декан аспирантуры Корнеллского университета сообщил, что университетская комиссия признала его виновным в нарушении университетского Кодекса академической честности.

Студент отчислен до начала осеннего семестра 1990 года, после чего сможет подать заявление о повторном поступлении.

Уголовных обвинений Моррису предъявлено не было. В этом году федеральное большое жюри направило свои рекомендации в Министерство юстиции, которое пока не предприняло никаких действий.

•----------

Министерство юстиции осторожничает в компьютерном деле — 28 мая 1989 г.

Автор: Мэтью Спина (Syracuse Herald-American)

«Боится ли Вашингтон проиграть знаковый процесс?»

Ряд компьютерных экспертов высказывает предположение, что Министерство юстиции, боясь провалить то, что могло бы стать знаковым компьютерным делом, до сих пор не знает, как поступить с корнеллским студентом, чей компьютерный червь в ноябре 1988 года расползся по всей стране.

Ещё одна головная боль Вашингтона: судебный процесс по этому делу может поставить в неловкое положение Министерство обороны, если его специалистам придётся публично рассказывать о том, каким образом их компьютеры оказались в числе тысяч машин, выведенных из строя червём.

На протяжении нескольких месяцев вопрос о том, какие обвинения предъявить 23-летнему Роберту Т. Моррису-младшему, находился на рассмотрении у Марка Ричарда — заместителя помощника

генерального прокурора. Несколько недель назад Ричард вынес решение, которое сейчас проходит проверку у помощника генерального прокурора — по словам специалиста в области компьютеров, поддерживающего контакты с Министерством юстиции.

«Я думал, что к этому времени из Вашингтона уже что-нибудь услышим», — сказал Эндрю Бакстер, помощник прокурора США, который в ноябре и декабре представлял дело большому жюри в Сиракузах.

Доклад большого жюри был направлен в Министерство юстиции, которое отказывается публично комментировать это дело, поскольку Моррис так и не был привлечён к суду.

«Думаю, в ближайшие две недели решение будет принято», — заявил один из чиновников.

«Если они решат начать дорогостоящий процесс, им нужно быть уверенными в победе — иначе это подорвёт будущие попытки привлечь к ответственности по данному закону», — сказал Юджин Спаффорд, адъюнкт-профессор Университета Пердью, чей анализ червя помог федеральным следователям. — «Если они решат не возбуждать дело, а единственным последствием для него окажется отчисление из Корнелла, я буду возмущён».

До сих пор только Корнелл принял в отношении Морриса дисциплинарные меры, отчислив его на 1989–90 учебный год. Однако аспирант покинул кафедру компьютерных наук ещё в начале ноября — на следующий день после того, как червь вырвался с компьютера в Апсон-холле.

Моррис, аспирант факультета компьютерных наук, считается автором вредоносной программы — червя, — распространившейся с компьютера Корнеллского университета. Программа была создана для того, чтобы воспроизводиться и заражать любые компьютеры, подключённые к сети Internet, которую совместно используют университеты, научные центры и военные учреждения.

Однако эксперты утверждают: из-за ошибки программа стала бесконтрольно размножаться, рассылая тысячи своих копий на тысячи компьютеров.

Если Моррису будет предъявлено обвинение в тяжком преступлении, прокурорам придётся доказать, что он намеревался уничтожить или похитить информацию.

Доказать это будет непросто, поскольку программа не уничтожила и не удалила информацию ни с одного компьютера.

Для осуждения Морриса по большинству менее тяжких статей прокурорам пришлось бы доказать его умысел на причинение вреда компьютерам.

Прокуроры также могли бы воспользоваться статьёй о мисдиминоре, требующей доказать лишь факт несанкционированного доступа Морриса к компьютеру федерального правительства. Червь действительно проник на компьютеры Баллистической исследовательской лаборатории армии США и Исследовательского центра НАСА в Лэнгли, среди прочих.

Ряд компьютерных экспертов задаётся вопросом: не откажутся ли чиновники Министерства обороны публично свидетельствовать о том, каким образом были взломаны их компьютеры — даже те, что хранили несекретную информацию. В феврале на компьютерной конференции в Сан-Диего специалисты по компьютерной безопасности Министерства обороны подробно рассказали о некоторых улучшениях, внесённых в систему безопасности сети после ноября, однако затем отказались раздать присутствующим на семинаре копии своего доклада.

ФБР — структура, обеспечивающая соблюдение Закона о компьютерном мошенничестве и злоупотреблениях 1986 года, — и часть представителей компьютерной индустрии настаивают на жёстком преследовании, чтобы продемонстрировать бескомпромиссную борьбу с хакерством. Другие представители отрасли, в том числе некоторые друзья Морриса из Гарвардского университета и Корнелла, призывают проявить снисхождение, поскольку он лишь стремился показать уязвимости в защите компьютеров.

• -

Другие статьи о Роберте Тэппане Моррисе-младшем и интернет-черве:

• «Computer Network Disrupted By 'Virus'» (11/03/88) PWN XXII/Part 2
• «Virus Attack» (11/06/88) PWN XXII/Part 2
• «The Computer Jam: How It Came About» (11/08/88) PWN XXII/Part 2
• «US Is Moving To Restrict {...} Virus» (11/11/88) PWN XXII/Part 2 *
• «FBI Studies Possible Charges In Virus» (11/12/88) PWN XXII/Part 2
• «Big Guns Take Aim At Virus» (11/21/88) PWN XXII/Part 3
• «Congressman Plan Hearings On Virus» (11/27/88) PWN XXII/Part 3
• «Pentagon Severs Military {...} Virus» (11/30/88) PWN XXII/Part 3 *
• «Networks Of Computers At Risk From Invaders» (12/03/88) PWN XXII/Part 4 *
• «Computer Virus Eradication Act of 1988» (12/05/88) PWN XXII/Part 4 *
• «Breaking Into Computers {...}, Pure and Simple» (12/04/88) PWN XXIV/Part 1 *
• «Cornell Panel Concludes Morris {...} Virus» (04/06/89) PWN XXVI/Part 1

* — Статья не была непосредственно посвящена Роберту Моррису, однако упоминала его в контексте инцидента с интернет-червём.

Психологическая игра SouthernNet против хакеров — апрель 1989 г.

ВНИМАНИЕ! Ваш звонок перехвачен!

Ошибка: Абоненты не могут изменять настройки.

```
Welcome to:  S o u t h e r n N e t   I n c.
```

Вы обратились в Отдел по борьбе с мошенничеством SouthernNet. Код авторизации, который вы пытаетесь использовать, недействителен. Взлом и незаконное использование кодов являются нарушением законодательства штата и федеральных законов.

В настоящее время мы проводим расследование фактов злоупотребления кодами в вашем регионе совместно с правоохранительными органами. Лица, уличённые во взломе или злоупотреблении кодами, будут привлечены к уголовной ответственности в полной мере, предусмотренной законом.

До скорой встречи,

Hacker Tracker

• -

Подождите, дополнительная информация:

Hacker Tracker сейчас недоступен; однако вы можете избежать возможного ареста и/или уголовного преследования, лично позвонив Hacker Tracker'у.

Вы можете связаться с г-ном Tracker'ом с 9:00 до 17:00 по восточному стандартному времени, с понедельника по пятницу, просто набрав тот номер доступа, который вы только что использовали, и код 101010 или 011010, если используемый вами номер доступа требует семизначного кода. Просто оставайтесь на линии 10 секунд, и ваш звонок автоматически будет переключён на г-на Tracker'а — бесплатно для вас.

Это *НЕ* уловка, и компания SouthernNet Inc. намерена урегулировать этот вопрос без привлечения правоохранительных органов при условии вашего стопроцентного содействия нашему отделу по борьбе с мошенничеством.

Контакт с г-ном Tracker'ом определённо будет в ваших интересах и покажет ваше решение оказать содействие и избежать преследования с нашей стороны!!!

Я буду ждать вашего звонка.

Hacker Tracker

Секунду... Активирую автопейджер для Hacker Tracker'a...

```
        50 seconds till disconnect
        40 seconds till disconnect
        30 seconds till disconnect
        20 seconds till disconnect
        10 seconds till disconnect
         5 seconds till disconnect

  NO CARRIER
```

[Неужели кто-то в это поверил и действительно позвонил «Hacker Tracker'y»? — KL]

Что происходит: расходы на компьютерную безопасность растут — 4 июня 1989 г.

Источник: Gannett Westchester Newspapers

[Комментарии в скобках от Delta-Master]

Высокотехнологичные компании тратят на компьютерную безопасность на 64% больше [чем прежде], согласно недавнему опросу, проведённому Национальным центром данных о компьютерных преступлениях в Лос-Анджелесе. В опросе участвовали 3 500 правоохранительных органов и специалистов по компьютерной безопасности, тема — компьютерная преступность. Уровень привлечения к ответственности также вырос — 6,4% в 1988 году против лишь 2,4% в 1987 году.

Вопреки расхожему образу, хакеры — не всегда молодые парни. Исследование показало, что 32% задержанных за компьютерные преступления составляют женщины, тогда как лишь 14% — лица моложе 21 года. По данным исследования, 45% хакеров — в возрасте от 25 до 30 лет.

•----------

Комментарий Delta-Master

Не знаю, как вы, но меня начинает раздражать путаница в общественном восприятии хакеров, особенно когда в ней допускаются откровенные ошибки. Серьёзно: я лично знаю лишь нескольких хакеров старше 21 года. Не менее раздражает и то, что газеты ставят знак равенства между грубыми компьютерными преступниками и хакерами-интеллектуалами (то есть вами). Разве нет? Запомните ключевую фразу: «32% ИЗ ТЕХ, КТО БЫЛ ЗАДЕРЖАН». Ну что ж, такова цена газетных ошибок.

Комиссия по коммунальному обслуживанию запрещает компании-операторы — 24 апреля 1989 г.

Автор: Джерри Страуд (St. Louis Post-Dispatch)

На прошлой неделе Комиссия по коммунальному обслуживанию штата Миссури проголосовала 4 против 1 за запрет провайдеров так называемых альтернативных операторских услуг в Миссури, поскольку деятельность этих компаний «не отвечает общественным интересам».

Компании, предоставляющие альтернативные операторские услуги, заключают договоры с гостиницами, мотелями, колледжами, больницами, аэропортами, ресторанами и другими заведениями, обеспечивая помощь операторов клиентам, пользующимся таксофонами или внутренними телефонами. Потребительские организации по всей стране жалуются на ценовой произвол этих компаний.

Марк Уитли, юрист Офиса публичного совета, похвалил решение комиссии.

По его словам, Офис публичного совета получил многочисленные жалобы на завышенные тарифы и надбавки со стороны компаний, предоставляющих альтернативные операторские услуги. Некоторые из них также принимали кредитные карты других компаний без разрешения эмитентов.

«Мы считаем это крайне важным решением комиссии», — сказал Уитли. Однако он ожидает, что затронутые им компании обжалуют его.

Адвокаты компаний — поставщиков альтернативных операторских услуг — оказались недоступны для комментариев.

В своём решении комиссия указала, что многие потребители не осведомлены о тарифах компаний альтернативных операторских услуг вплоть до получения «счёта за услуги связи по ценам выше привычных». Потребительские организации утверждают, что тарифы нередко в два-три раза превышают расценки более известных операторов дальней связи.

Даже если компания, предоставляющая операторские услуги, называет себя при соединении, потребители зачастую не понимают значения этой идентификации, говорится в решении комиссии.

«Если конечный пользователь не осведомлён о тонкостях работы с альтернативным поставщиком операторских услуг, он лишён подлинного права выбора», — отметила комиссия.

Решение распространяется только на внутриштатные звонки, обслуживаемые компаниями альтернативных операторских услуг, однако фактически может воспрепятствовать и их деятельности в сфере межштатных переговоров.

Комиссия специально отклонила тарифные заявки International Telecharge Inc. и American Operator Services Inc. Кроме того, комиссия обязала три другие компании — Teleconnect Inc., Dial US и Dial USA — подать новые тарифы в соответствии с принятым решением.

Решение допускает работу компаний, предоставляющих операторские услуги в рамках основной деятельности — например, операторов дальней связи и местных телефонных компаний. Однако на них также наложены ограничения.

Согласно решению, компании, предоставляющие операторские услуги, обязаны:

• Называть себя как звонящему, так и стороне, которой выставляется счёт (в случае звонка за счёт вызываемого абонента или третьего лица).
• По требованию сообщать тарифы звонящему или плательщику бесплатно.
• Применять процедуры проверки calling card, приемлемые для компаний-эмитентов.
• Вывешивать на видном месте наименование компании, подробный порядок подачи жалоб и инструкцию о том, как выйти на оператора местной телефонной компании и других операторов дальней связи.
• Переключать экстренные вызовы на местную телефонную компанию или American Telephone & Telegraph Co. до тех пор, пока альтернативный поставщик услуг не докажет, что в состоянии самостоятельно обрабатывать экстренные вызовы.

Факс-атака — 13 мая 1989 г.

Источник: The Ann Arbor News

«Попытка губернатора запретить нежелательную рекламу обернулась против него самого!»

ХАРТФОРД, Коннектикут — Большая факс-атака 1989 года — массированная лоббистская кампания против законопроекта о запрете нежелательной факсимильной рекламы — похоже, дала обратный эффект: факс-аппарат губернатора на несколько часов оказался заблокирован нежелательными сообщениями.

Начиная с четверга, 11 мая, и в течение всей пятницы, 12 мая, факс-аппарат губернатора Уильяма А. О'Нилла беспрерывно пищал, выдавая нежелательные сообщения от разъярённых компаний, рекламирующих товары по факсу.

Эти компании выступают против законопроекта, ожидающего подписи О'Нилла, который запретит рекламировать продукцию по факсу без предварительного согласия получателя. Нарушителям грозит штраф в 200 долларов.

Начиная с четверга утром десятки коннектикутских компаний направили в офис О'Нилла типовое письмо с протестом против запрета факсовой рекламы. Поток факс-сообщений был столь непрекращающимся (40 штук поступило до 10 утра), что в четверг (11 мая) офис губернатора отключил факс-аппарат.

Пресс-секретарь О'Нилла Джон Л. Сандберг сообщил, что губернатор ещё не принял решения о подписании законопроекта. Но помощники губернатора отметили: настойчивая лоббистская кампания наглядно продемонстрировала, насколько раздражающими бывают нежелательные сообщения. Неудобства усугублялись тем, что офис губернатора не мог воспользоваться факсом для получения информации о весеннем паводке в штате.

NYNEX представляет шлюз Info-Look — 28 апреля 1989 г.

Представляем новый сервис для доступа к информации и многому другому — прямо с вашего персонального компьютера!

С мая 1989 года шлюзовой сервис INFO-LOOK (tm) компании New York Telephone может стать вашим каналом доступа к разнообразным информационным ресурсам, продуктам и услугам.

Шлюз INFO-LOOK упрощает онлайн-подключение с персонального компьютера к широкому кругу информационных провайдеров. Позвонив на номер шлюза через модем, вы сможете просматривать меню информационных сервисов.

Доступные типы информационных сервисов включают: развлечения, бизнес, здоровье, кулинария, новости, погода, спорт, путешествия, государственное управление, образование и справочная информация. Сервисы, часть из которых интерактивна, предоставляются независимыми компаниями.

Шлюз INFO-LOOK прост в использовании — даже для тех, кто только начинает работать с компьютером.

Что необходимо для использования шлюза INFO-LOOK

1. Практически любой тип персонального компьютера.

2. Модем (300, 1200 или 2400 бод) и программное обеспечение для связи. Они позволяют компьютеру общаться с другими компьютерами через телефонную сеть.

3. Calling card New York Telephone. Если вам нужна карта New York Telephone Calling Card (она **бесплатна**), позвоните своему представителю по обслуживанию — его номер указан на первой странице вашего счёта New York Telephone.

Стоимость использования шлюза INFO-LOOK

Плата за подключение к шлюзу и ежемесячная абонентская плата **отсутствуют**. В большинстве случаев жителям Нью-Йорка предъявляются следующие счета:

• Стоимость местного звонка для подключения к шлюзу INFO-LOOK.
• Пока вы просматриваете каталог сервисов шлюза или переключаетесь между сервисами — 0,05 доллара в минуту.
• После подключения к конкретному сервису стоимость определяется поставщиком. Некоторые сервисы имеют поминутную тарификацию, некоторые — бесплатны. Тарифы на каждый сервис указаны в меню шлюза.

Большинство платежей будут включены в ваш ежемесячный счёт New York Telephone. Некоторые поставщики могут выставлять счета за пользование своими сервисами отдельно и напрямую.

Для получения дополнительной информации:

Чтобы получить бесплатный информационный буклет об INFO-LOOK Gateway, позвоните по бесплатному номеру 1-800-338-2720, добавочный 20, ежедневно с 9 до 23 часов.

Примечание: New York Telephone не предоставляет и не контролирует сервисы, доступные через шлюз INFO-LOOK Gateway. Они предоставляются независимыми компаниями, которые несут ответственность за содержание, характер и качество своих услуг.

Прогнозы сейчас составляют 5 миллиардов долларов, ещё 5–10 миллиардов ожидается к 1991 году.

[INFO-LOOK уже работает в Bell South и Bell Atlantic.]

Pacific Bell планирует доступ к компьютерным ресурсам — 9 июня 1989 г.

Источник: Santa Cruz Sentinel (Раздел B)

САН-ФРАНЦИСКО (AP) — В четверг компания Pacific Bell заявила о намерении составить конкуренцию телевидению, предоставив людям удобный доступ к компьютерным библиотекам, доскам объявлений и электронной почте.

California On-line от PacBell — доступная любому обладателю персонального компьютера, телефона и calling card — станет одним из первых в стране сервисов на основе графического интерфейса, упрощающего работу настолько, что потребуется лишь минимальное знакомство с компьютерами.

«Это позволит нашим клиентам дополнить привычный досуг... и, в частности, в ходе испытаний мы наблюдали, как многие пользователи перестали смотреть телевизор», — сказал Роджер П. Конрад, директор службы Videotex Gateway Services.

«Мы считаем, что это более продуктивный способ проводить время, и думаем, что многие пользователи с нами согласятся», — добавил он. Пользователи будут платить

«инфопредпринимателям» по времени использования различных сервисов, счета выставляются в ежемесячных телефонных квитанциях. В отличие от некоторых онлайн-информационных служб, предварительная подписка не требуется.

По словам Конрада, виды доступных сервисов ограничены лишь фантазией разработчиков. PacBell будет зарабатывать на продаже компаниям доступа к телекоммуникационным линиям.

Доски объявлений Аргентины — 5 июня 1989 г.

Код страны = 54 (Аргентина)
Код города = 1 (Буэнос-Айрес)

Список может быть частично устаревшим в связи с течением времени. Последнее обновление — 23 декабря 1986 года.

Name	Hours Of Operation	======= Number=
Beta	23:00 - 6:30	802-0288
C-Mania	21:00 - 7:00	362-8843
CBM	16:00 - 12:00	90-4988
Century 21	24 hours	632-7070
Cerebruss	24 hours	47-2717
Cerebruss Information	?	48-8300
		48-9886
Databank	?	44-9760
Drean Conection	?	953-2523
Los Pinos	13:00 - 19:00	21-0375
Magenta	?	392-0124
Magenta	?	392-0016
Maxes	23:00 - 7:00	542-2695
Mendieta	22:00 - 8:00	654-6999
Pirates Cove	24:00 - 6:00	783-5023
Sanctuary	24:00 - 3:00	641-4608
Soft-work	22:30 - 9:00	88-2065
TCConection	19:00 - 12:00	22-4197
The Connection	24 Hours	82-5780
The Hacker	23:00 - 7:00	748-2005
Tiger	?	784-2226
XCASA	?	611-8136
BBS-IOM	24 Hours	804-3602

Примечание: параметры для всех систем в списке — чётный бит чётности, 7 бит данных, 1 стоп-бит.

Предоставлено: Noli

Один из «хитрых хакеров» Клиффорда Столла мёртв (самоубийство?)

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                               PWN
PWN        P h r a c k   W o r l d   N e w s      PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~      PWN
PWN               Issue XXVII/Part 3              PWN
PWN                                               PWN
PWN                  June 20, 1989                PWN
PWN                                               PWN
PWN          Created, Written, and Edited         PWN
PWN               by Knight Lightning             PWN
PWN                                               PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

---

5 июня 1989 года

По данным западногерманских изданий, «хитрый хакер» Карл Кох из Ганновера (ФРГ) скончался в пятницу, 3 июня, предположительно в результате самоубийства. Его тело было найдено сожжённым (с применением бензина) в лесу близ Целле — западногерманского городка рядом с Ганновером, где он совершал свои взломы, что было зафиксировано немецкой почтовой службой.

Кох был одним из двух хакеров, которые признались государственным прокурорам в своей роли в деле о взломе в пользу КГБ, тем самым придав делу огласку. Как сообщают немецкие газеты, он, по всей видимости, страдал психическим расстройством: он считал, что за ним постоянно следят инопланетные существа — «иллюминаты», — которые пытаются его убить. По всей видимости, он глубоко идентифицировал себя с персонажем «Капитан Хагбард» (его псевдоним в хакерской среде), позаимствованным из американской книги; этот персонаж (как и сам Кох) страдал от преследования иллюминатов. Сотрудники полиции, очевидно, склоняются к версии самоубийства (хотя, по имеющимся сведениям, существуют «некоторые обстоятельства», которые могут подкреплять иные версии; точной информации об этих обстоятельствах не сообщается).

По мнению немецких полицейских экспертов, роль Карла Коха в деле КГБ и его повседневная жизнь в полной мере объяснимы при прочтении упомянутой малоизвестной книги.

Информация предоставлена Клаусом Брунштайном (Гамбургский университет)

> *[Иллюминаты... КГБ... как угодно... -KL]*

Illuminatus!

14 июня 1989 года

Книгой, о которой идёт речь, считается «Illuminatus!» Гарольда Ши и Роберта Антона Уилсона. Это пародия на теории заговора, в которой утверждается, что большинство, а то и все человеческие институты являются лишь ширмой для небольшой группы «просветлённых», которые сами по себе служат прикрытием для Временных карликов из Сети Зета Сетки (Reticuli Zeta), или, возможно, для Атлантических Адептов, остатков «Золотой Зари» Кроули, или, что ещё вероятнее, для Ллойгор из «Мифов Ктулху» Г. Ф. Лавкрафта. Главный персонаж книги носит имя Хагбард Селин.

«Illuminatus!» — занятное чтение, если вы любите психоделику и паранойю. Книга, по всей видимости, оказала большое влияние на последующие произведения, в первую очередь на «Путеводитель по галактике для путешествующих автостопом» Адамса. Нетрудно представить, как неуравновешенный человек, воспринимая её буквально, может целиком в ней раствориться. Фактически «Illuminatus!» производит впечатление книги, намеренно написанной ради подобного эффекта программирования — сами авторы называли это «Операцией «Промывание мозгов»» (Operation Mindfuck).

Для подавляющего большинства психически здоровых взрослых людей это, вероятно, не представляет реальной опасности, однако в данном случае всё могло оказаться иначе — к величайшему сожалению. Или же, не желая никого обижать, Кох в ходе различных взломов действительно узнал слишком много об иллюминатах. В конце концов, считается, что именно они — тайная сила, стоящая за КГБ :-)

Для получения дополнительной информации о Клиффорде Столле и «хитрых хакерах» из Западной Германии см.:

«Who Is Clifford Stoll?» (без даты) — Phrack World News, выпуск XXII/Часть 1
«A Message From Clifford Stoll» (10.01.89) — Phrack World News, выпуск XXIII/Часть 2

А также следующие статьи из Phrack World News, выпуск XXV/Часть 2:

• «German Hackers Break Into Los Alamos and NASA» (2.03.89)
• «Computer Espionage: Three 'Wily Hackers' Arrested» (2.03.89)
• «Computer Spy Ring Sold Top Secrets To Russia» (3.03.89)
• «KGB Computer Break-Ins Alleged In West Germany» (3.03.89)
• «News From The KGB/Wily Hackers» (7.03.89)

Загадочный хакер перенаправил звонки в службу пробации на секс-линию

13 июня 1989 года

Ft. Lauderdale News and Sun-Sentinel

> *«Да, вы звучите очень соблазнительно, но мне действительно нужен инспектор службы условного освобождения.»*

ДЕЛРЕЙ-БИЧ, Флорида. В понедельник, 12 июня, позвонившие в службу условного освобождения в Делрей-Биче (Флорида) вместо неё услышали разнообразные сексуальные разговоры от тяжело дышащей женщины по имени Тина.

Представители телефонной компании Southern Bell сообщили, что компьютерный хакер перепрограммировал их оборудование в выходные, перенаправив звонки, адресованные местной службе условного освобождения, на нью-йоркскую секс-линию.

«Люди звонят в Департамент исправительных учреждений и попадают на какой-то секс-дворец», — заявил Томас Сальглафф, пресс-секретарь службы условного освобождения округа Палм-Бич.

Представители Southern Bell сообщили, что это первый случай перепрограммирования их коммутационного оборудования посторонним взломщиком. Southern Bell предоставляет местную телефонную связь во Флориде, Джорджии, Северной Каролине и Южной Каролине.

«Мы крайне обеспокоены», — заявил пресс-секретарь Southern Bell Бак Пассмор. По его словам, для подобного подвига потребовался бы человек с весьма серьёзными знаниями в области

компьютеров.

Последствия подобного взлома весьма значительны. Перехват корпоративных переговоров, раскрытие засекреченных телефонных номеров, а также фальсификация платёжной информации — всё это вполне реальные последствия компьютерных брешей в системе безопасности телефонной компании.

Хакеры прежде уже проникали в системы Southern Bell, однако ни разу не перепрограммировали телефонные линии, подчеркнул Пассмор.

Технические специалисты по безопасности из Southern Bell и AT&T пытаются отследить источник взлома, сообщил Пассмор.

Взлом ради конкурентного преимущества

12 мая 1989 года

По материалам Los Angeles Times

Двум бывшим руководителям отдела новостей одной из телевизионных станций Тампы (Флорида) предъявлены обвинения в незаконном подключении к телефонным линиям и компьютерам конкурирующей станции с целью получить преимущество в подаче новостей. Бывшему директору отдела новостей Терри Коулу и его заместителю Майклу Шапиро с телестанции WTSP-TV предъявлено 17 пунктов обвинения в компьютерном взломе и сговоре с целью хищения информации с телестанции WTVT-TV через телефонные компьютерные линии, сообщили власти. Их предварительное слушание было назначено на 19 мая.

В случае осуждения каждому из них грозит максимальное тюремное заключение сроком до 85 лет. Оба были уволены из WTSP после того, как станция узнала о предполагаемых кражах. Взломы начались в ноябре 1988 года, однако обнаружены не были вплоть до 12 января 1989 года, когда утренний продюсер WTVT обнаружил пропажу файлов, сообщили власти.

Компьютерные эксперты установили, что злоумышленник просматривал файлы. Власти сообщили, что Шапиро досконально знал систему безопасности WTVT, поскольку сам участвовал в её создании, работая там менеджером по заданиям, прежде чем был переманен со станции WTVT в октябре.

Руководители отдела новостей телестанции уволены после обвинений во взломе ресурсов конкурента

Тампа, Флорида. Флоридская телестанция уволила двух руководителей отдела новостей на фоне сообщений о том, что один из них якобы взломал компьютерную систему конкурирующей станции и похитил конфиденциальную информацию.

WTSP-TV (Канал 10), аффилиат ABC в Сент-Питерсберге, объявила об увольнении заместителя директора отдела новостей Майкла Шапиро и директора отдела новостей Терри Коула.

7 февраля Шапиро был арестован по обвинению в тяжком преступлении — якобы он не менее шести раз в январе взломал компьютерную систему WTVT-TV (Канал 13). Прежде он работал в WTVT в должности заместителя менеджера и отвечал за администрирование компьютерных систем станции.

Сотрудники правоохранительных органов изъяли из дома Шапиро персональный компьютер, 200 дискет, а также руководство по эксплуатации и пользовательское руководство к программному обеспечению, применявшемуся на конкурирующей станции.

Ему предъявлено 14 пунктов обвинения в тяжких преступлениях в соответствии с разделом 815 Статутов Флориды, регулирующим преступления, связанные с компьютерами. По каждому пункту предусмотрено максимальное наказание в виде 15 лет лишения свободы и штрафа в размере $10 000.

Винс Баррези, вице-президент и генеральный директор WSTP, отказался комментировать увольнения. Однако в подготовленном заявлении он сообщил, что объявил телезрителям в выпуске новостей в 23:00 в прошлый вторник, что станция предприняла этот шаг, чтобы «избежать любых вопросов относительно объективности нашей работы по информированию общества».

Коул, нанявший Шапиро в сентябре прошлого года, не был привлечён к уголовной ответственности властями Флориды. По сведениям одного из источников, он был уволен в силу того, что как директор отдела новостей несёт в конечном счёте ответственность за действия сотрудников редакции. Шапиро и Коул были недоступны для комментариев.

> *[Ещё одна статья, посвящённая этому делу, — «Television Editor Charged In Raid On Rival's Files» (8 февраля 1989 года). Она была опубликована в Phrack World News, выпуск XXIV/Часть 2. -KL]*

Сведения в Национальном информационном центре по преступности повлекли повторный незаконный арест

14 мая 1989 года

Автор: Джеймс Рэйни (Los Angeles Times)

Из-за ошибок в базе данных NCIC Роберто Пералес Эрнандес за последние три года дважды оказывался под стражей как подозреваемый в краже со взломом в Чикаго в 1985 году. Власти перепутали его с другим Роберто Эрнандесом вследствие единственной записи в Национальном информационном центре по преступности (NCIC) ФБР.

Оба Роберто Эрнандеса — одного роста, примерно одного веса, имеют тёмные волосы, карие глаза, татуировки на левой руке, одну и ту же дату рождения, а их номера социального страхования отличаются лишь одной цифрой!

Незаконно задержанный подал в суд, обвинив полицейское управление Хоторна (Калифорния), округ Лос-Анджелес и штат Калифорния в незаконном лишении свободы, причинении психологической травмы и нарушении гражданских прав в связи с последним арестом, состоявшимся в прошлом году.

Ранее он получил компенсацию в размере $7 000 от округа за 12-дневное заключение под стражей в 1986 году, прежде чем выяснилось, что был задержан не тот человек. В ходе последнего инцидента его держали под стражей семь дней, после чего освободили без каких-либо объяснений.

Ещё один случай незаконного заключения

18 мая 1989 года

В ходе показаний 18 мая 1989 года на заседании Подкомитета по гражданским и конституционным правам Комитета по судебной власти Палаты представителей США по вопросу о Национальном информационном центре по преступности Дэвид Д. Ределл привёл ещё один случай незаконного заключения с участием Роберто Пералеса Эрнандеса, а также ряд более ранних дел, в том числе дело Терри Дина Рогана [см. ниже]:

> *«Лишь на прошлой неделе дело в Калифорнии наглядно продемонстрировало потенциальную пользу от свободного доступа к хранимым изображениям. Джозеф О. Робертсон был арестован, экстрадирован, привлечён к суду и направлен в государственное психиатрическое учреждение на 17 месяцев. Всё это время в базе данных уже хранились фотографии и дактилоскопические карты, ясно свидетельствовавшие о том, что задержан не тот человек, — однако никто не удосужился их проверить.»*

Приведённые материалы — наглядные примеры того вреда и тех проблем, которые порождает эта «супербаза» данных. Такие люди, как Уильям Бэйз (директор ФБР по техническим службам) и Уильям Сешнс (директор ФБР), либо не осознают этого, либо, возможно, им просто всё равно (пока нечто подобное не произойдёт с ними самими).

Для тех, кто хочет изучить эту тему подробнее: первая статья об этой базе данных NCIC называлась «'Big Brotherish' Data Base Assailed» (21 ноября 1988 года). Она была опубликована в Phrack World News, выпуск XXII/Часть 3.

Ещё один инцидент, схожий с описанными выше случаями, произошёл с Ричардом Лоуренсом Скларом — профессором политологии Калифорнийского университета в Лос-Анджелесе. Компьютер спутал его с беглецом, разыскиваемым по делу о махинациях с недвижимостью в Аризоне. Прежде чем ФБР выяснило, что задержан не тот человек, Склар, которому было 58 лет, провёл двое суток в условиях унизительного обыска, перемещался из одного места содержания в другое и был закован в наручники вместе с членами банд и другими лицами, совершившими насильственные преступления. Подробнее об этом деле и деле Терри Дина Рогана см. «FBI National Crime Information Center Data Bank» (13 февраля 1989 года), опубликованную в Phrack World News, выпуск XXIV/Часть 2 (а также в Washington Post).

TRW и Администрация социального обеспечения

12 мая 1989 года

Кредитное бюро TRW сотрудничало с Администрацией социального обеспечения (SSA) с целью верификации её базы данных, содержащей 140 миллионов имён и номеров социального страхования. Для покрытия расходов TRW выплачивает SSA $1 миллион, тогда как SSA вносит равнозначный $1 миллион со своей стороны.

Поскольку SSA запрашивает увеличение бюджета на компьютерные и телекоммуникационные системы, ряд законодателей возмущён тем, что она тратит $1 миллион на этот негосударственный проект. Назвав проект «настолько далёким от миссии Администрации социального обеспечения, насколько мне вообще доводилось видеть», сенатор Дэвид Прайор (демократ, Арканзас) поставил под сомнение компетентность и честность комиссара SSA Доркас Р. Харди и потребовал расследования со стороны генерального инспектора Министерства здравоохранения и социальных служб.

Кроме того, ряд законодателей, в том числе Дэйл Бамперс (демократ, Арканзас), считает проект нарушением гражданских свобод. Бамперс заявил: «Я против того, чтобы любое государственное

учреждение разглашало личные данные граждан». Американское юридическое управление Исследовательской службы Конгресса уже пришло к выводу о том, что проект нарушает Закон о конфиденциальности 1974 года.

> *[Связанная статья «Verifying Social Security Numbers» (11 апреля 1989 года) была опубликована в Phrack World News, выпуск XXVI/Часть 3 (а также в New York Times в тот же день). -KL]*

Краткие заметки Phrack World News XXVII

1. Сети BITNET и CSNET объединяются в новую сеть, которой присвоено текущее название ONENET.

---

2. **Присвоение кода NPA 903 Северо-Восточному Техасу (10 мая 1989 года).** Объявлено, что те части кода 214, которые не относятся к Далласу, будут переведены на код 903 осенью 1990 года.

После присвоения кода 708 Чикаго, 903 — Техасу и 908 — Нью-Джерси до изменения формата нумерации остаётся распределить лишь 909 и 917.

---

3. **Подробности о новом коде зоны 510 (6 июня 1989 года).** Пресс-релиз Pacific Bell, процитированный в San Francisco Chronicle, сообщает поэтапные сроки введения нового кода NPA 510.

Запуск запланирован на 7 октября 1991 года с четырёхмесячным переходным периодом, в течение которого для затронутых номеров по-прежнему будет действовать код NPA 415. Окончательный перевод запланирован на 27 января 1992 года.

Код 510 охватит округа Аламеда и Контра-Коста, в которых в настоящее время насчитывается 842 388 абонентов из 2 005 687 текущих абонентов кода NPA 415.

---

4. **Разделение кода зоны Нью-Джерси (27 апреля 1989 года).** Разделение не должно произойти раньше 1991 года. Новый код NPA будет 908, и он в основном охватит южную «половину» нынешней зоны 201. Затронутые округа: Уоррен, Хантердон, Мидлсекс, Юнион, Манмут и Оушен, а также юго-западный угол Морриса. В зоне 201 останутся округа Сассекс, Пассейик, Берген, Эссекс, Хадсон и большая часть Морриса.

New Jersey Bell также начнёт требовать набора кодов зоны при звонках в Нью-Йорк и Пенсильванию, которые считались частью местной зоны вызовов Нью-Джерси. Это, по-видимому, вступит в силу 2 октября и освободит около 25 позывных. Информация из Asbury Park Press.

> *[Последняя строка в некоторой мере противоречит первой в отношении сроков. Дополнительная информация по мере поступления. — KL.]*

---

5. **Новые коды зон для Лондона (27 апреля 1989 года).** British Telecom объявила, что 6 мая 1990 года код зоны Лондона будет изменён в связи с возросшим количеством линий, необходимых в столице.

Действующий код — 01-; вводимые новые коды: 071- для центра города и 081- для пригородов. В Evening Standard был опубликован список, в котором указано, в какую зону войдёт каждая АТС.

---

6. **Член клуба убеждается на горьком опыте: American Express ведёт наблюдение (4 мая 1989 года).** Статья из San Jose Mercury News рассказывает о том, как American Express позвонила одному из своих клиентов, чтобы выразить обеспокоенность его возможной неспособностью оплатить последний счёт. American Express получила доступ к его текущему счёту и установила, что на нём меньше средств, чем причитается компании. Его карта была временно «деактивирована» после того, как клиент отказался предоставить какие-либо финансовые сведения, кроме обещания оплатить счёт наличными при его получении.

Как выяснилось, заявка на получение карты в мелком шрифте содержит оговорку: «[American Express оставляет за собой] право доступа к счетам для проверки вашей платёжеспособности». После нескольких споров с компанией клиент резюмирует: «Я усвоил урок: моя жизнь не так приватна, как я думал».

---

7. **QuickSource от Southwestern Bell (24 апреля 1989 года).** Southwestern Bell Telephone Company проводит годовой эксперимент (март 1989 — март 1990) с двумя информационными службами: QuickSource (аудиотекс) и Sourceline (видеотекс). Для последней требуется терминал, тогда как первая доступна с любого тонального телефона. Номер QuickSource — 323-2000, однако он недоступен через 1+713+: SWBTCo заблокировала доступ «из зоны метрополитена Хьюстона, обслуживаемой SWBTCo», согласно тексту, который зачитывает оператор при запросе помощи (713-865-5777; не заблокирован). Служба помощи вышлет вам бесплатный справочник QuickSource.

---

8. **Объединение почтовых служб Telemail, MCI и AT&T Mail (16 мая 1989 года).** Дочерняя компания U.S. Sprint — Telenet — объявила о соглашении о взаимодействии между Telemail (продуктом электронной почты Telenet), MCI Mail и AT&T Mail.

Новая схема, которая должна заработать ближайшим летом, позволит 300 000 пользователям Telemail по всему миру, 100 000 пользователям MCI Mail и 50 000 пользователям AT&T Mail беспрепятственно обмениваться электронными письмами.

---

9. **Illinois Bell не работала четыре часа! (18 мая 1989 года).** Более 40 000 абонентов Illinois Bell в северо-западных пригородах Чикаго остались без связи примерно на четыре часа из-за неполадок в компьютере коммутационного центра.

Телефоны не работали или не принимали входящие и исходящие вызовы с 9:30 до 13:40 вследствие программного сбоя в центральном офисе в Хоффман-Эстейтс (штат Иллинойс). Наибольшие неудобства испытали жители Хоффман-Эстейтс, Шаумбурга, Арлингтон-Хайтса, Хановер-Парка и Стримвуда (штат Иллинойс).

Точный характер неисправности представитель Bell не раскрыл, сообщив лишь, что сбой был устранён. Очевидно, резервная система, которая должна была автоматически включиться, также вышла из строя.

---

10. **Институт Стэнфордского исследовательского института (SRI) атакован белками-камикадзе (29 мая 1989 года).** Похоже, система электроснабжения SRI, в Data Defense Network заявленная как система «без единой точки отказа», потерпела крах от рук, вернее, лап белки. Электричество отсутствовало примерно 9 часов; аппаратных повреждений при этом выявлено не было. Это произошло как минимум в третий раз, когда именно белка стала

виновником инцидента в SRI.

---

11. **Бесплатные звонки с телефонов-автоматов New York Telephone (10 июня 1989 года)** (San Francisco Chronicle, стр. 2). 24 таксофона вдоль шоссе Long Island Expressway оказались фактически бесплатными из-за программного/базоданного сбоя. Ими активно пользовались для международных звонков те, кто обнаружил упущение, — в том числе для многочисленных звонков в Пакистан (когда полиция прибыла на место после сообщения о стрельбе, она обнаружила 15 пакистанцев, пользовавшихся этими телефонами). Оценки суммы невозмещённых расходов на звонки не поступало.

*** *КОНЕЦ* ***