Phrack RU issue 024

Русская версия Phrack, выпуск 024. 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; веб-безопасность, PHP, CTF и прикладные атаки на сервисы.

Материалы выпуска: Содержание номера; Phrack Pro-Phile XXIV; Limbo To Infinity — От Лимбо до Бесконечности; Frontiers — За пределами Bitnet лежит бесконечность; Администрирование центра управления расширенной службой 911 для центров специальных услуг и крупных клиентов; Терминологический словарь службы Enhanced 911; Advanced Bitnet Procedures; Специальные коды зон; Срываем покров тайны с Ma Bell; Прогресс сетевых технологий; Phrack World News; Shadow Hawk приговорён к тюремному заключению — 17 февраля 1989 года; Контракт Иуды исполнен — 24 января 1989 года.

Содержание номера

Автор: Taran King и Knight Lightning

---

25 февраля 1989 года

Добро пожаловать в Phrack Inc., выпуск 24. Мы рады сообщить, что в последнее время нам удаётся соблюдать заявленные даты выхода — в отличие от прошлых задержек.

Необходимо внести небольшую ясность. Мы получали вопросы о том, почему номер тома всего лишь 2, тогда как по годам он должен быть около 4. По нашему мнению, том состоит из 12 выпусков, в идеале — по одному в месяц. К сожалению, в прошлом нам не всегда удавалось выдерживать этот темп. Если вы ждёте смены тома, следите за выпуском 25 — он откроет Том 3 Phrack Inc.

В Phrack World News XXIV опубликовано краткое объявление о SummerCon '89; подробности появятся по мере их поступления.

Как всегда, мы просим всех, у кого есть доступ к сети, написать нам на адреса Bitnet или Internet (см. подпись ниже).

В этом выпуске мы публикуем завершение Future Transcendent Saga, а также дополнительный файл к ней — Advanced Bitnet Procedures, предоставленный VAXBusters International. Надеемся, вам понравится!


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

Phrack Pro-Phile XXIV

Автор: Taran King

Написано 3 февраля 1989 года

Добро пожаловать в Phrack Pro-Phile XXIV. Phrack Pro-Phile создан для того, чтобы рассказывать сообществу о людях, отошедших от дел или сыгравших важную, а порой и спорную роль в его истории. В этом выпуске я представляю одну из редкостей в мире фрикинга и хакинга... девушку! Она была умеренно активна и поддерживала контакты с людьми, тесно связанными с сообществом...

Chanda Leir

```
Chanda Leir
~~~~~~~~~~~
```

Ник: Chanda Leir
Зовут: Karen
Прошлые ники: Нет
Происхождение ника: Тётя Карен в детстве хотела взять это имя, если когда-нибудь станет знаменитой.
Дата рождения: 8 мая 1970 года
Нынешний возраст: Почти 19
Рост: 5' 6" (около 168 см)
Вес: 125 фунтов (около 57 кг) — если «первокурсная пятнашка» ещё не успела сказаться
Цвет глаз: Зелёно-серые
Цвет волос: Светлые
Компьютеры: Отец Карен — риелтор, поэтому она начала на терминале TI 700 (терминале системы MLS)... просто модем, клавиатура и рулон БУМАГИ)... затем перешла на папин рабочий компьютер — KAYPRO II... Сейчас пользуется Mac'ами, системами Sun и IBM RT, установленными в CMU.

Карен начала звонить на BBS в районе Вашингтона в 1983 году (в нежном возрасте 13 лет). Некий Hack-Man (по её предположению, это был «оригинальный» H-M) держал борду на мёртвой линии местного петлевого номера 678. Её знакомство с телефонным «делом» началось в тот день, когда она позвонила на «борду» и вместо несущей обнаружила 30 человек на конференц-линии.

Она была ошарашена, и — будучи девушкой — тридцать парней на конференции оказались готовы и рады снабдить её информацией о происхождении петель, конференций, боксинге и прочем. Скотт (Hack-Man) впоследствии рассказал ей всё остальное, дал ещё номеров и тому подобного — вот так всё и началось.

Среди памятных фрикеров и хакеров, с которыми Карен довелось познакомиться, — Cheshire Cat, Tuc, Bioc Agent 003 и все остальные, кто присутствовал на встрече TAP в День Благодарения 1984 года.

Свой опыт она приобретала, задавая МАССУ вопросов множеству озабоченных парней, которые охотно делились с ней всякой информацией именно потому, что она была девушкой. Сама она объясняет свои познания преимущественно тем, что просто впитывала и запоминала всё, что ей

говорили.

Две борды, которые Карен назвала незабываемыми, находились в Фоллс-Чёрч, штат Вирджиния: Mobius Strip и Xevious II.

В настоящее время она — первокурсница Университета Карнеги — Меллона в Питтсбурге (или, как она сама любит его называть, COMPUTER U.). Её специализация, по всей видимости, — «Политика и менеджмент».

Главное её достижение — она, вероятно, была самой юной девушкой, когда-либо побывавшей на встрече TAP (в 14 лет), и, по всей видимости, одной из немногих, кто пришёл туда вместе с мамой, папой и тётей Линдой (какой конфуз).

Одной из причин, по которым она бросила мир фрикинга/хакинга, стал визит агентов Секретной службы в феврале 1985-го... хотя на самом деле пришли они не за ней... «Друг», которого разыскивали за мошенничество с кредитными картами, позвонил ей, пока его линия была подключена к пин-регистратору.

В те же выходные, когда он позвонил Карен, проходили торжества по случаю Инаугурации, и они с братом набирали петлевой номер 456 (Белый дом) что-то около 21 раза за четыре дня... Как бы то ни было, агенты Секретной службы охотились за Эриком, и когда её номер всплыл в двух местах, они решили провести расследование. Родители были в панике!

Настоящая же причина её ухода из мира фрикинга/хакинга заключалась в том, что в 1985 году она сменила школу, стала одной из «популярных» и обзавелась светской жизнью, утратив время и интерес к компьютерам.

Интересы Chanda Leir

МУЗЫКА... в первую очередь harDCore... (то есть панк-рок из Вашингтона, округ Колумбия). Большинство её друзей состоят или состояли в вашингтонских группах: The Untouchables, Teen Idles, Minor Threat, Youth Brigade (DC), Grey Matter, Government Issue и прочие.

УЖАСЫ... романы, фильмы, комиксы... Клайв Баркер, Arcane Comix (издателем которых является её друг Стив), Питер Страуб, Дин Кунц, Уитли Стрибер и т.д... весь этот жанр...
И Фланнери О'Коннор — это отдельная история...

Самые памятные впечатления

Родители Карен имели обыкновение «заставлять» её организовывать конференц-звонки всякий раз, когда у кого-то из родственников был день рождения. Они собирали всю семью на линии и болтали. Всем казалось, что это жутко круто...

Другим весёлым занятием было то, как папа доставал свою телефонную книгу Министерства обороны (DoD) и они перебирали номера в поисках модемных линий...

В апреле 1985 года Tuc приехал к её бабушке, после чего они пошли смотреть фильм «В отчаянных поисках Сьюзен»...

Слова благодарности

«Пожалуй, только Taran King — за это интервью — и Knight Lightning... оба они связались со мной здесь, в CMU... и TUC... и ...?»

И конечно... традиционный финальный вопрос Phrack Pro-Phile... Большинство фрикеров и хакеров, с которыми вы встречались, — компьютерные гики? «ДА... без сомнений.»

Спасибо за уделённое время, Карен.

Taran King

Limbo To Infinity — От Лимбо до Бесконечности

Глава Третья «Саги о Грядущем Трансцендентном»

Traversing The Barriers For Gateway Communication — Преодоление барьеров для шлюзовой связи

Автор: Knight Lightning

11 февраля 1989 г.

За пределами Bitnet существуют другие глобальные сети. Об этих сетях мы расскажем подробнее в главе четвёртой. Сейчас же давайте разберёмся, как устанавливать связь с этими другими мирами.

Отправка почты в другие сети — шлюзовая связь

Bitnet, как вы уже знаете, не единственная компьютерная сеть в мире. Возможно, вас удивит следующее: имея доступ к Bitnet, вы одновременно получаете доступ ко многим другим сетям. К сожалению, методы общения с людьми в этих других сетях не столь просты, как те, что были описаны ранее.

Связи Bitnet с другими сетями открывают вам доступ к людям и сервисам, с которыми иначе вы бы не смогли связаться (или смогли бы лишь ценой больших усилий). Уже одно это делает изучение данной темы вполне оправданным.

В первой главе этой серии я показал, как некоторые имена узлов Bitnet можно разбить на аббревиатуры штатов. Сделаем ещё один шаг: представьте Bitnet как страну, а связи между её узлами — как шоссейные дороги. Другая сеть (или страна в нашем примере) подключена к этой дорожной системе в одной точке, которая называется «шлюзом» (gateway). Через эти границы не пропускают интерактивные сообщения и файлы — через шлюз проходит только почта.

Люди в этих других сетях имеют адреса, похожие на ваш, однако для доставки им почты необходимо указывать кое-что дополнительное. Адрес вида `userid@node` недостаточен, поскольку он не сообщает почтовому ПО Bitnet, в какой сети находится данный узел. Поэтому мы расширяем сетевой адрес кодом, идентифицирующим сеть назначения. В следующем примере сеть назначения — ARPAnet (сеть, о которой вы наверняка немало слышали), а её код — ARPA:

```
TARAN@MSP-BBS.ARPA
+---- +------ +---
|     |       |
|     |       +-------------------- сеть
|     |
|     +---------------------------- узел
|
+---------------------------------- идентификатор пользователя
```

Это, пожалуй, простейший из адресов другой сети. Как правило, они значительно сложнее. Из-за разнообразия сетей нет универсального примера «типичного» адреса. Впрочем, беспокоиться об

этом особо не стоит. Если кто-то сообщает вам, что его сетевой адрес — C483307@UMCVMB.MISSOURI.EDU, просто используйте его именно в таком виде в своём почтовом ПО. Главное — понимать, что письмо идёт в другую сеть и время доставки может быть больше обычного (хотя на практике я неоднократно замечал, что почта на EDU-адреса доставляется значительно быстрее, чем письма внутри Bitnet). Особых проблем возникнуть не должно.

Подробнее о шлюзах

В предыдущем разделе я упомянул шлюзы, не вдаваясь в детали, — тема порой бывает весьма запутанной. На самом деле понять принцип работы шлюзов несложно, а вот интерпретировать сетевые адреса, в которых они используются, — уже сложнее.

В предыдущем примере адрес получателя в другой сети выглядел так:

```
TARAN@MSP-BBS.ARPA
```

Суффикс .ARPA в адресе сообщает вашему сетевому ПО, что письмо предназначено для другой сети. Возможно, вы не знаете, что ваше ПО «знает»: адрес шлюза в сеть ARPA находится, скажем, на узле INTERBIT. Оно может расширить адрес примерно до такого вида:

```
TARAN%MSP-BBS.ARPA@INTERBIT
+---- +------ +--- +-------
|     |       |    |
|     |       |    +--------------- узел шлюза
|     |       |
|     |       +-------------------- сеть
|     |
|     +----------------------------- узел
|
+---------------------------------- идентификатор пользователя
```

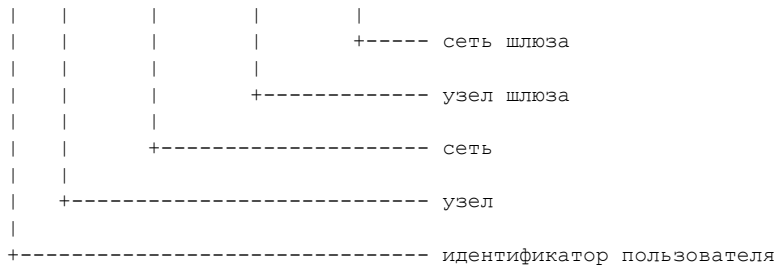
Шлюз — это серверная машина (userid@node), передающая файлы между двумя сетями. В данном случае это ARPA@INTERBIT. Обратите внимание: символ % заменяет @ из предыдущего примера. Это объясняется тем, что почтовое ПО Bitnet не умеет обрабатывать адреса с более чем одним знаком @. Когда письмо достигнет шлюза, часть @INTERBIT будет отброшена, а % снова превратится в @.

Итак, вы спросите: «Если всё это происходит автоматически, зачем мне вообще это знать?» Во многих случаях ваше сетевое ПО недостаточно «умно», чтобы знать, что шлюз в SCONNET находится на узле STLMOVM. В таком случае вам придётся вводить полный адрес со всеми специальными символами вручную.

Например, иногда нужно немного преобразовать адрес. Допустим, я разговариваю с Lex Luthor, и он называет мне свой адрес lex@plover.COM. Я обнаружил, что для отправки на такой адрес реально используется plover!lex@RUTGERS.EDU. Это лишь конкретный пример работы именно моей системы — другие системы (не говоря уже о других сетях) будут работать иначе (данное руководство предназначено для пользователей Bitnet). COM-адреса (коммерческие) не распознаются почтовиком на UMCVMB, поэтому мне приходится маршрутизировать их через Rutgers University. В главе четвёртой я расскажу о некоторых других взаимосвязанных сетях.

Во многих случаях шлюз в нужную сеть может находиться в другой сети. В следующем примере мы отправляем письмо пользователю RED на узел KNIGHT в сети HDENNET. Шлюз в эту сеть расположен, допустим, в ARPAnet. Наше ПО достаточно умно, чтобы знать расположение шлюза ARPA, поэтому адрес будет выглядеть примерно так:

```
RED%KNIGHT.HDENNET@SRI-NIC.ARPA
+-- +----- +------ +------ +---
```



Как видите, адреса могут быть весьма длинными и неудобными для ввода. Пожалуй, единственное утешение — что ваш адрес, скорее всего, выглядит столь же устрашающе для получателей в сети назначения.

Различные фонды и службы

Подобно тому, как в Bitnet есть серверы и сервисы, в других сетях имеются их аналоги. На нескольких других сетях доступны многочисленные электронные дайджесты и серверы, схожие с серверами Bitnet.

Шлюзы в нестандартные сети — Intermail

Intermail — пожалуй, наиболее интересное исключение из стандартных шлюзов. Проще показать на примере, чем давать техническое описание процесса. С помощью Intermail можно получить доступ к сетям, которые, вероятно, вы никогда не считали доступными.

Ниже приведены инструкции по использованию системы Intermail для передачи компьютерной почты между пользователями системы MCI-Mail, системы GTE Telemail, системы Compmail/Dialcom 164 и системы NFS-Mail/Dialcom 157 и системой ARPA-Mail. Система Intermail может использоваться в обоих направлениях.

Почта, предназначенная для MCI Mail, GTE Telemail, Compmail или NSF-Mail, отправляется в почтовый ящик «Intermail» на локальной почтовой системе. Система Intermail работает следующим образом: программный сервис обслуживает почтовые ящики как в локальной, так и в целевой почтовой системе. Если в начале сообщения указана нужная информация, программа перенаправляет эти сообщения в другую почтовую систему.

Чтобы сообщение было доставлено в почтовый ящик другой почтовой системы, в начале текста каждого сообщения необходимо указывать информацию для пересылки. Она сообщает программе-пересыльщику, в какую почтовую систему направить сообщение и в какие почтовые ящики его доставить. Формат такой информации:

```
Forward: <почтовая система>
To: <почтовый ящик пользователя>
<пустая строка>
```

Синтаксис строки `To:` соответствует синтаксису системы, в которую выполняется пересылка. В ARPA-Mail также можно указывать список получателей CC в любой из шлюзуемых почтовых систем. Подробности — в примерах ниже.

В обоих направлениях поле `Subject` (тема) локального сообщения для Intermail используется в качестве поля `Subject` сообщения, доставляемого в другую почтовую систему.

Отправка в нестандартные сети из Bitnet

При такой схеме интернет-пользователь должен сначала отправить письмо в почтовый ящик Intermail в сети ARPA-Internet. Адрес «Intermail» — `INTERMAIL@ISI.EDU`. Затем в начале текста каждого сообщения необходимо добавить информацию для пересылки. Названия почтовых ящиков: `MCI-MAIL`, `TELEMAIL` (для GTE Telemail), `COMPMAIL` и `NSF-MAIL`.

Формат информации:

```
Forward: <введите название почтового ящика>
To: <допустимый адрес в системе, куда выполняется пересылка>
<пустая строка>
<Текст сообщения...>
```

Примечание: CompuServe (CIS), Telex и FAX доступны из MCI-Mail, однако шлюз Intermail эти сервисы не поддерживает. Тем не менее существует шлюз Bitnet–CompuServe, о котором речь пойдёт в следующем разделе.

Отправка в Bitnet из нестандартных сетей

Если у вас есть аккаунт в MCI-Mail, GTE Telemail, Compmail или NSF-Mail и вы хотите отправить письмо кому-либо в Bitnet, адресуйте письмо по одному из следующих адресов:

- "`INTERMAIL`" (MCI-ID `107-8239`) в MCI-Mail
- "`INTERMAIL/USCISI`" в GTE Telemail
- "`164:CMP00817`" в Compmail/Dialcom 164
- "`157:NSF153`" в NSF-Mail

После этого введите следующие две строки в самом начале письма:

```
Forward: ARPA
To: KNIGHT%MSPVMA.BITNET@CUNYVM.CUNY.EDU
<пустая строка>
<Текст сообщения...>
```

В этом примере KNIGHT — идентификатор пользователя, MSPVMA — узел Bitnet. CUNYVM.CUNY.EDU — интернет-шлюз в ARPAnet. Всё действительно так просто.

По вопросам и проблемам, связанным с использованием Intermail, обращайтесь по адресу `Intermail-Request@ISI.EDU`.

CompuServe

На момент написания этой статьи шлюз ещё не введён в эксплуатацию. Тестирование несколько задержалось из-за высокоприоритетных проектов внутри CompuServe. Тем не менее, вероятно, к тому времени, как вы это читаете, шлюз уже готов.

Конкретная реализация такова: шлюзовая машина — 3B2/400 по имени Loquat — считает, что у неё есть UUCP-сосед «compuserve», который периодически к ней подключается. На самом деле

UUCP-соединение — полная иллюзия, однако шлюз запускается ежечасно, просматривает очередь UUCP, находит почту для CompuServe и на лету генерирует командный скрипт, пригодный для утилиты Xcomm 2.2, чтобы та позвонила в CompuServe, скачала ожидающую почту и выгрузила почту из очереди.

Выполняется соответствующая корректировка заголовков, благодаря которой CompuServe выглядит как обычная RFC-совместимая единица в интернете, а интернет с точки зрения абонента CompuServe выглядит как ещё одна шлюзованная система — потребовалась лишь незначительная модификация стандартного синтаксиса их почтовика, но этот проект стал стимулом для обобщения механизма, в чём до сих пор не было нужды.

На этом пока всё. Loquat взаимодействует с машинами в Университете штата Огайо. В настоящее время существует проблема, препятствующая прохождению почты за пределы взаимодействия CompuServe — Ohio State, пока не завершены разработка и тестирование. Кроме того, часть корректировки заголовков направлена на правильное отображение идентификаторов CompuServe в интернете — стандартный формат `7xxxx,yyy` создаёт трудности из-за запятой.

Easynet

Шлюз для обмена почтой между Easynet и сетью UUCP, а также интернетом DARPA (включая CSNET) предоставляется Western Research Laboratory в Пало-Альто, Калифорния. Будем надеяться, что этот сервис обеспечит улучшенную связь между сообществом DEC и сообществами Usenet и Internet.

Отправка из узла Bitnet в узел Easynet

Чтобы отправить письмо из интернет-узла в узел Easynet (например, MSPVAX), введите:

```
To: user%mspvax.dec.com@decwrl.dec.com
```

Ряд других форматов по-прежнему принимается из соображений обратной совместимости, но их использование не рекомендуется и здесь они не описываются.

Отправка из Easynet в Bitnet

Следующая информация может пригодиться пользователям Easynet, желающим написать в Bitnet.

Шлюз поддерживает подключение к Bitnet с использованием синтаксиса псевдодоменов. Эти адреса преобразуются шлюзом в надлежащий формат для адресации шлюза в Bitnet. Для отправки пользователям Bitnet введите:

```
To: DECWRL::"user@host.bitnet"
```

(Пример: `To: DECWRL::KNIGHT@MSPVAX.BITNET`*)*

Mailnet

Шлюз Bitnet–Mailnet прекратил существование. Служба Mailnet компании EDUCOM была закрыта 30 июня 1987 года по договорённости с MIT.

DASnet

DASnet — одна из сетей, подключённых к AppleLink.

Отправка в DASnet из Bitnet

1. В поле `TO` укажите адрес шлюза DASnet: `XB.DAS@STANFORD.BITNET`
2. В поле `SUBJECT` укажите идентификатор пользователя DASnet (например, `[1234AA]joe`)

Пример (0756AA — адрес DASnet, randy — пользователь в этой системе):

```
To: XB.DAS@STANFORD.BITNET
Subject: [0756AA]randy
```

3. Если после адреса в поле `SUBJECT` поставить `!`, можно добавить комментарий, однако строка темы должна быть не длиннее 29 символов.
Пример: `Subject: [0756AA]randy!Networks are cool`

Отправка в Bitnet из DASnet

1. В поле `TO` укажите BITNET-адрес с суффиксом `@dasnet`
2. Поле `SUBJECT` используйте для комментариев.

Пример:

```
To: knight@umcvmb.bitnet@dasnet#M
Subject: Gateways
```

Не запутайтесь: здесь два символа `@` и символ `#M` в конце.

Шлюзы между Bitnet и другими сетями

```
 _____________________________________________________
|               |                     |               |
| "u" = UserId | "h" = Host (Node) | "d" = Node (Host) |
|_____________|___________________|___________________|
```

Из Bitnet:

"u" = UserId	"h" = Host (Node)	"d" = Node (Host)
_____	_____	_____

В Bitnet из других сетей:

ACSNET (Домены: A: oz.au)	<u>%<d>.A@<g>
UUCP	h1!h2!<h>!<u>@psuvax1
JUNET (Домены: J: junet)	<u>%<d>.J@csnet-relay.csnet

JANET (альтернативный формат)	<u>%U.<d>@ac.uk

Заключение

Теперь, когда вы разобрались, как отправлять почту в другие сети через шлюзы, мы перейдём к изучению самих этих сетей. Поскольку Bitnet — моя основная область знаний, остальные сети я освещу менее подробно. Если они вас заинтересуют, уверен, вы найдёте способ узнать о них больше. Итак, читайте Главу Четвёртую «Саги о Грядущем Трансцендентном» — Frontiers.

:Knight Lightning

Frontiers — За пределами Bitnet лежит бесконечность

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                                <>
<>                          Frontiers                             <>
<>                          ~~~~~~~~~                             <>
<>         Chapter Four of The Future Transcendent Saga           <>
<>                                                                <>
<>                  Beyond Bitnet Lies Infinity                   <>
<>                                                                <>
<>                 Presented by Knight Lightning                  <>
<>                       February 12, 1989                        <>
<>                                                                <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Автор: Knight Lightning

Глава четвёртая «Саги о Будущем Запредельном»
12 февраля 1989 года

Добро пожаловать в заключительную главу «Саги о Будущем Запредельном»... или нет? Может ли у будущего вообще быть заключительная глава? Так или иначе, я собрал информацию о ряде других сетей, с которыми вы, возможно, столкнётесь, используя Bitnet. Эти описания скорее носят характер краткого обзора, нежели подробного руководства (каковым была «Утопия» для Bitnet). Тем не менее, я уверен, что представленная здесь информация окажется вам полезной. Большая часть материала основана на исследованиях, проводившихся в июле 1987 года. За любые неточности, вызванные прогрессом технологий и прошедшим временем, приношу свои извинения.

В данном файле рассмотрены правительственные сети ARPANET, MILNET, MFENET и NSFnet, а также сети, созданные пользователями: CSNET, HEANET, SPAN, TEXNET, UUCP и USENET.

Этот файл не претендует на роль хакерского руководства — он представляет собой лишь справочник по ряду сетей.

И ещё один момент: основные домены верхнего уровня в Интернете:

```
.EDU   Учебные заведения
.COM   Коммерческие организации
.GOV   Государственные структуры
.MIL   Военные организации
.ORG   Прочие организации (не вписывающиеся в другие категории)
```

Правительственные сети

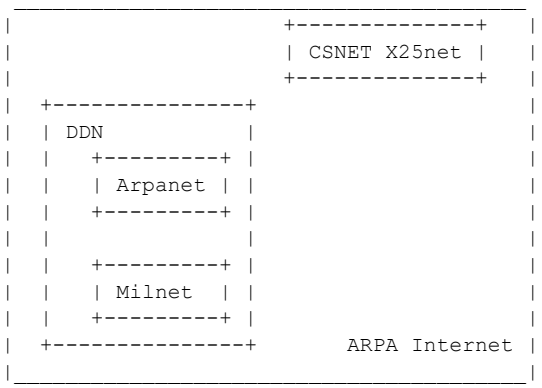
ARPANET и MILNET

В 1969 году Агентство перспективных исследовательских проектов Министерства обороны США (DARPA) приступило к исследовательской программе по развитию компьютерных сетей. Экспериментальная сеть с коммутацией пакетов, созданная в её рамках, получила название ARPANET; она позволяла компьютерам различных типов эффективно обмениваться данными. На базе технологии ARPANET в 1982 году была создана Сеть оборонных данных (DDN — Defense Data

Network), объединившая существующую сеть ARPANET и другие компьютерные сети Министерства обороны США (DoD). DDN использует набор протоколов DoD Internet Protocol Suite, включая TCP/IP (протокол управления передачей/протокол Интернет) и связанные прикладные протоколы.

Разделение ARPANET было начато в 1983 году и завершено в 1984-м. В результате возникли две сети: экспериментальная исследовательская сеть ARPANET и несекретная оперативная военная сеть MILNET. Обе сети соединены между собой шлюзами. Основу каждой из них составляют узлы коммутации пакетов (PSN — Packet Switched Nodes), большинство из которых связаны наземными линиями со скоростью 56 Кбит/с. По состоянию на январь 1987 года ARPANET насчитывала 46 PSN, а MILNET — 117 в США и 33 в Европе и Тихоокеанском регионе.

ARPANET и MILNET входят в состав DDN; вместе с другими сетями, использующими те же протоколы, DDN образует ARPA Internet. Пример сети, принадлежащей ARPA Internet, но не входящей в DDN, — CSNET X25net, использующая протоколы TCP/IP через публичную сеть X.25.



Политику, контроль доступа и финансирование ARPANET обеспечивает Управление методов обработки информации (IPTO) агентства DARPA. Эксплуатацией и управлением ARPANET и MILNET занимается Управление программы DDN (DDN PMO) Агентства оборонных коммуникаций.

Использование ARPANET ограничено лицами, занятыми экспериментальными исследованиями по заказу правительства США или спонсируемыми правительством исследованиями в университетах. Поскольку сеть не предназначена для конкуренции с коммерческими сетями, она не рассчитана на удовлетворение оперативных коммуникационных нужд или использование широкой публикой.

Сервисы ARPANET и MILNET включают удалённый вход, передачу файлов, электронную почту, время и дату. Адресация почты в обеих сетях осуществляется в формате user@domain, где domain — полное доменное имя, состоящее из одной или нескольких поддоменных строк, разделённых точкой и завершающихся доменом верхнего уровня. Примеры доменов верхнего уровня: edu, com, gov, mil, net, org, jp, au, uk. Примеры полных доменных имён: kentarus.cc.utexas.edu, relay.cs.net, icot.jp.

DDN финансирует Центр сетевой информации (NIC), расположенный в SRI International в Менло-Парке, Калифорния. Центр оказывает пользовательские услуги через электронную почту (NIC@SRI-NIC.ARPA), по телефону (800-235-3155) и почтой США: DDN Network Information Center, SRI International, Room EJ291, 333 Ravenswood Avenue, Menlo Park, CA 94025. Телефонная поддержка доступна с понедельника по пятницу с 7:00 до 16:00 по тихоокеанскому времени.

Обширная информация также доступна в режиме онлайн на SRI-NIC.ARPA через telnet или анонимный ftp (логин `anonymous`, пароль `guest`). Файл NETINFO:NETINFO-INDEX.TXT содержит указатель онлайн-файлов.

MFENET

MFEnet — сеть Министерства энергетики США (DOE) для исследований в области магнитного синтеза. Она была создана в середине 1970-х годов для обеспечения доступа к суперкомпьютеру MFE Cray 1 в Национальной лаборатории Лоуренса Ливермора. Сеть использует спутниковые каналы со скоростью 56 Кбит/с и предназначена для предоставления терминального доступа к системе разделения времени Cray (CTSS), также разработанной в Ливерморской лаборатории. В настоящее время сеть поддерживает доступ к суперкомпьютерам Cray 1, Cray X-MP/2, Cray 2 и Cyber 205. В ней используется специализированное сетевое программное обеспечение, разработанное в Ливерморе; помимо терминального доступа, оно обеспечивает передачу файлов, удалённую постановку в очередь вывода, электронную почту, а также ряд специализированных прикладных процедур для интерактивных графических терминалов и локального редактирования на персональных компьютерах. Доступ к сети в целом ограничен исследователями, финансируемыми DOE. Несколько лет назад сеть была расширена за счёт суперкомпьютера, финансируемого DOE в Университете Флориды. MFEnet финансируется DOE и управляется Ливерморской лабораторией.

MFEnet успешно обслуживает пользователей суперкомпьютеров DOE. Однако специализированная природа коммуникационных протоколов теперь создаёт трудности для исследователей, которым необходимы передовые графические рабочие станции под управлением операционной системы UNIX BSD 4.2 с протоколами TCP-IP в локальных сетях. По этим и другим причинам DOE рассматривает наилучшие пути миграции MFEnet на протоколы TCP-IP, а впоследствии — на протоколы OSI.

Сочетание операционной системы CTSS и протоколов MFEnet создаёт эффективную интерактивную вычислительную среду для исследователей, работающих на суперкомпьютерах Cray. По этой причине два из новых национальных суперкомпьютерных центров NSF — Сан-Диего (SDSC) и Иллинойс — выбрали операционную систему CTSS. В случае SDSC для поддержки сети консорциума SDSC были также выбраны протоколы MFENET. В случае Иллинойса программой NSFnet финансируется проект реализации протоколов TCP-IP для операционной системы CTSS; результаты разработки будут переданы SDSC (и DOE) для обеспечения пути миграции консорциумной сети SDSC.

Почту пользователям MFEnet можно направлять в следующем формате:

```
user%site.MFENET@NMFEDD.ARPA
```

NSFNET

NSFnet возник в 1986 году как коммуникационная сеть для обеспечения доступа к национальным суперкомпьютерным центрам, финансируемым NSF. Постепенно он превращается в универсальную сеть Интернет для обмена исследовательской и научной информацией. Сеть имеет трёхуровневую структуру: магистраль, несколько автономно администрируемых территориальных сетей и кампусные сети. Магистраль включает следующие суперкомпьютерные центры:

• Национальный центр суперкомпьютерных приложений, Иллинойсский университет в Урбане-Шампейн (UIUC)
• Национальный суперкомпьютерный центр Корнелла, Корнелльский университет (Cornell)
• Национальный суперкомпьютерный центр имени Джона фон Неймана, Принстон, Нью-Джерси (JVNC)
• Суперкомпьютерный центр Сан-Диего, Калифорнийский университет в Сан-Диего (SDSC)

• Суперкомпьютерный центр Питтсбурга (Westinghouse Electric Corp, Университет Карнеги — Меллон, Питтсбургский университет)
• Отдел научных вычислений Национального центра атмосферных исследований, Боулдер, Колорадо (NCAR)

На магистрали NSFnet применяются протоколы верхнего уровня TCP/IP. Магистраль стала работоспособной в июле 1986 года и состояла из семи каналов со скоростью 56 Кбит/с между шестью IP-шлюзами на базе систем LSI 11/73. В конце 1987 года была осуществлена модернизация с переходом на каналы T1 (1,544 Мбит/с). Планируется переход на сетевые протоколы OSI по мере появления соответствующего программного обеспечения.

Компонентные сети, финансируемые NSF:

```
BARRNET    — Региональная исследовательская сеть залива Калифорнии (Bay Area)
MERIT      — Мичиганская образовательная исследовательская сеть
MIDNET     — Сеть Среднего Запада
NORTHWESTNET — Северо-западные штаты
NYSERNET   — Образовательно-исследовательская сеть штата Нью-Йорк
SESQUINET  — Техасская сеть к 150-летию штата
SURANET    — Сеть ассоциации исследовательских университетов юго-востока
WESTNET    — Юго-западные штаты
JVNCNET    — Консорциумная сеть JVNC
SDSCNET    — Консорциумная сеть SDSC
PSCAAnet   — Консорциумная сеть суперкомпьютерного центра Питтсбурга
```

Часть компонентных сетей появилась раньше NSFnet, часть — создана недавно. Каждая из них подключена к магистрали. Информацию о состоянии любой из компонентных сетей NSFnet можно получить в Центре сетевых услуг NSFnet (NNSC). Ежемесячные отчёты о состоянии магистрали и компонентных сетей доступны онлайн через CSNET Info-Server. Для их получения следует направить сообщение на адрес info-server@sh.cs.net со следующим телом письма:

```
REQUEST: NSFNET
TOPIC: NSFNET-HELP
REQUEST:END
```

Эти отчёты также можно получить через анонимный ftp (логин `anonymous`, пароль `guest`) с хоста sh.cs.net из каталога `nsfnet`. [FTP — протокол передачи файлов.]

К магистрали NSFnet подключены и другие автономные сети: ARPANET, BITNET, CSNET и USAN (Университетская спутниковая сеть Национального центра атмосферных исследований).

Среди интересных проектов, связанных с NSFnet: реализация демона маршрутизации gated, поддерживающего протоколы RIP, EGP и HELLO и работающего под управлением 4.3BSD, Ultrix TM, GOULD UTX/32 TM, SunOS и VMS TM (Теоретический центр Корнелльского университета); реализация TCP/IP для операционной системы CTSS с поддержкой TELNET и FTP (Иллинойсский университет); спутниковый эксперимент по обеспечению каналов 56 Кбит/с между удалёнными сегментами Ethernet с использованием технологии Vitalink (NCAR).

Управление NSFnet осуществляется в переходном режиме: обязанности распределены между Иллинойсским университетом, Корнелльским университетом, Институтом информационных наук Университета Южной Калифорнии и Университетской корпорацией атмосферных исследований. Проект NSFnet администрируется Отделом сетей, коммуникационных исследований и инфраструктуры в составе Директората компьютерных и информационных наук и технологий NSF.

Дополнительную информацию можно получить в Центре сетевых услуг NSFnet (NNSC): BBN Laboratories Inc., 10 Moulton Street, Cambridge, MA 02238; по электронной почте: nnsc@nnsc.nsf.net; по телефону: 617-497-3400. NNSC работает под управлением Bolt, Beranek and Newman и является финансируемым NSF проектом Университетской корпорации атмосферных исследований.

Сети, созданные пользователями

CSNET

В 1980 году в Национальный научный фонд было представлено предложение о финансировании компьютерной сети для исследований в области вычислительных наук, которая должна была объединить любые университеты, коммерческие и государственные организации, занимающиеся исследованиями или передовыми разработками в области компьютерных наук и вычислительной техники. NSF предоставил финансирование на период с 1981 по 1985 год, и сеть CSNET была создана. Сегодня эта единая логическая сеть объединяет около 200 компьютеров в трёх физических сетях: Phonenet, X25net и подмножестве ARPANET. Phonenet — сеть с промежуточным хранением, использующая программное обеспечение MMDF через публичные телефонные линии для предоставления услуг электронной почты. X25net использует публичную пакетную сеть X.25 Telenet с интерфейсом TCP/IP для предоставления электронной почты, передачи файлов и удалённого входа. Часть хостов ARPANET также является членами CSNET. Компьютеры, объединённые CSNET, расположены в США, Европе, Канаде, Израиле, Корее и Японии. Адресация в CSNET осуществляется в доменном стиле ARPA Internet.

В 1981 году был заключён договор с компанией Bolt, Beranek and Newman, Inc. на предоставление информационных, пользовательских и технических услуг для CSNET; был создан Координационный и информационный центр CSNET (CIC). CIC осуществляет ежедневное управление сетью; общий надзор обеспечивается Исполнительным комитетом CSNET. Сеть существует на членские взносы.

CIC ведёт базу данных сервера имён пользователей, доступную через команду `ns` на хостах CSNET с соответствующим программным обеспечением или через telnet к сервисному хосту sh.cs.net (логин `ns`, пароль не требуется). Обширная информация также доступна через анонимный ftp на sh.cs.net (логин `anonymous`, пароль `guest`), особенно в каталоге `info`. Информационный сервер также предоставляет средства получения этой информации. Для использования сервера направьте письмо на infoserver@sh.cs.net со следующими строками в теле:

```
REQUEST:  INFO
TOPIC:  HELP
REQUEST:  END
```

Онлайн-информация включает программное обеспечение, документы о политике, сведения о других сетях, списки узлов и архивы рассылок.

Зарубежные партнёры CSNET и их шлюзы:

• **CDNNET** — Канадская академическая сеть, Университет Британской Колумбии.
• **SDN** — Сеть системных разработок (SDN), компьютерная сеть для R&D-сообщества Республики Корея; шлюз находится в KAIST, Корейском передовом институте науки и технологий, Сеул. Имеет соединение по электронной почте с CSNET/Internet, USENET/EUNET/UUCP Net и рядом стран Тихоокеанского региона: Австралией, Индонезией, Гонконгом, Сингапуром и Японией.
• **SUNET** — Шведская университетская сеть, Технологический университет Чалмерса, Гётеборг.
• **CHUNET** — Швейцарская университетская сеть, ETH-Zentrum, Цюрих.
• **Inria** — Французская университетская сеть, Национальный институт исследований в области информатики, Рокенкур.
• **DFN** — Deutsches Forschungsnetz, GWD-Gesellschaft für Mathematik und Datenverarbeitung, Schloss Birlinghoven, Санкт-Августин.
• **JUNET** — Японская университетская сеть, Токийский университет.
• Финская университетская сеть, Хельсинкский университет, Хельсинки.
• **AC.UK** — Академическое сообщество Великобритании, Университетский колледж Лондона.

• **ACSNET** — Академическая сеть на основе UUCP в Австралии, Мельбурнский университет.
• Новозеландская академическая сеть, Университет Вайкато, Гамильтон.
• Израильская академическая сеть, Еврейский университет в Иерусалиме.

За дополнительной информацией обращайтесь: CSNET CIC, BBN Laboratories Inc., 10 Moulton Street, Cambridge, MA 02238; или по электронной почте: cic@sh.cs.net (cic@csnet-sh.arpa). Также работает круглосуточная горячая линия: (617) 497-2777.

HEANET

HEAnet — сеть, объединяющая университеты и национальные институты высшего образования Ирландской Республики. В HEANET входят следующие учреждения:

```
NIHED:  Национальный институт высшего образования, Дублин
NIHEL:  Национальный институт высшего образования, Лимерик
MAY:    Колледж Святого Патрика, Мейнут
TCD:    Тринити-колледж, Дублин
UCC:    Университетский колледж, Корк
UCD:    Университетский колледж, Дублин
UCG:    Университетский колледж, Голуэй
```

Аббревиатуры слева используются для формирования сетевых адресов хостов каждого учреждения. Адреса имеют вид:

```
host.institution.IE  (например, VAX2.NIHED.IE)
```

HEANET подключена к EARN/Bitnet/Netnorth через шлюз в Университетском колледже Дублина. Почту для HEANET следует отправлять как BSMTP «задание» на MAILER по адресу IRLEARN.

SPANet

Сеть анализа космической физики (SPAN — Space Physics Analysis Network) начала работу в 1981 году как результат пилотного проекта в Центре космических полётов имени Маршалла, финансируемого NASA (Отдел космической плазменной физики, Управление космических наук). Сеть представляет собой испытательный стенд системы данных, не привязанной к конкретным миссиям; её цель — решение проблем обмена данными (необработанными и обработанными), аналитическим программным обеспечением, графическими изображениями и корреспонденцией между исследователями в нескольких дисциплинах: физике солнечно-земных связей, межпланетной и планетной физике, астрофизике, атмосферных науках, океанологии, климатологии и науках о Земле. Создание SPAN было мотивировано осознанием того, что в 1980-х годах возрастёт значение межотраслевых коррелятивных исследований в гелиофизике, что в научных базах данных не хватало стандартов и что необходима поддержка отображения аппаратно-независимых графических изображений. SPAN был создан для содействия анализу космических данных и решения нерешённых задач обмена научными данными и их корреляции.

Руководство и рекомендации по политике для SPAN вырабатывает Рабочая группа пользователей систем данных, образованная в 1980 году. Ежедневную эксплуатацию сети обеспечивают сетевой и проектный менеджер, проектный учёный, менеджеры центров маршрутизации и менеджеры локальных узлов.

Узлы SPAN взаимодействуют с использованием различных сред передачи данных (волоконная оптика, коаксиальный кабель, арендованные телефонные линии) и протоколов нижних уровней (ethernet, X.25, DDCMP); почти все хосты SPAN используют протоколы верхних уровней DECnet TM.

Планируется переход на формирующиеся протоколы OSI по мере появления программного обеспечения.

В настоящее время SPAN объединяет более 1200 компьютеров по всем Соединённым Штатам, Европе, Канаде и Японии (что служит источником различных инцидентов, связанных с хакерской деятельностью в сети, — например, инцидента с Mathias Speer). Магистраль сети в США состоит из резервированных каналов по 56 Кбит/с между пятью центрами маршрутизации DECnet:

1. Космический центр NASA имени Джонсона (Хьюстон, Техас)
2. Лаборатория реактивного движения NASA и Caltech (Пасадена, Калифорния)
3. Центр космических полётов NASA имени Маршалла (Хантсвилл, Алабама)
4. Центр космических полётов NASA имени Годдарда (Гринбелт, Мэриленд)
5. Исследовательский центр NASA имени Эймса (Моффетт-Филд, Калифорния)

Замыкающие каналы соединяют организации-члены SPAN с ближайшим центром маршрутизации — как правило, по арендованным линиям со скоростью не менее 9,6 Кбит/с.

SPAN имеет шлюзы к CSNET, ARPANET, BITNET, GTE Telenet, JANET и пакетной коммутационной системе NASA (NPSS). SPAN соединена с TEXNET, HEPnet и другими территориальными сетями DECnet TM. Сервисы, доступные узлам SPAN: электронная почта, удалённая передача файлов и удалённый вход.

Дополнительную информацию можно получить в Информационном центре сети SPAN (SPAN-NIC), расположенном в Национальном центре космических научных данных, Центр космических полётов NASA имени Годдарда, Гринбелт, Мэриленд 20771. Помощь также доступна по электронной почте: NSSDCA::SPAN_NIC_MGR.

TEXNET

Большая часть TEXNET стала работоспособной в 1986 году, хотя отдельные её фрагменты существовали и ранее. Назначение сети — объединение компьютеров техасских университетов, работающих с протоколами верхних уровней DECnet TM. Протоколы нижних уровней: ethernet (IEEE 802.3) и DDCMP (Digital Data Communication Message Protocol — протокол цифровых коммуникационных сообщений). В настоящее время TEXNET объединяет более 450 машин в 14 городах. Магистраль сети состоит из маршрутизаторов DECnet TM и ряда синхронных каналов, соединённых по арендованным линиям со скоростями 9600 бит/с и 56 Кбит/с.

Существуют шлюзы из TEXNET в SPAN, BITNET и ARPA Internet. Предоставляемые сервисы: электронная почта, передача файлов и удалённый вход.

Эксплуатационным и политическим управлением сетью занимается неформальная управляющая группа, сформированная по принципу консенсуса из менеджеров каждого учреждения-члена.

Члены TEXNET:

```
Университет Бейлора
Исследовательский центр Хьюстонского района
Панамериканский университет
Государственный университет Сэма Хьюстона
Государственный университет Юго-Западного Техаса
Техасский университет A&M
Хьюстонский университет
Техасский университет в Арлингтоне
Техасский университет в Остине
Техасский университет в Эль-Пасо
Техасский университет в Далласе
Техасский университет на плато Пермиан-Бейсин
Техасский университет в Сан-Антонио
```

```
Техасский университет в Тайлере
Медицинский центр Техасского университета в Тайлере
Медицинский научный центр Техасского университета в Далласе
Медицинский научный центр Техасского университета в Хьюстоне
Медицинский научный центр Техасского университета в Сан-Антонио
Медицинское отделение Техасского университета в Галвестоне
Онкологический центр системы Техасского университета
Центр высокопроизводительных вычислений системы Техасского университета
Управление земельными ресурсами системы Техасского университета
```

UUCP и USEnet

Сеть UUCP была основана в 1970-х годах для обеспечения электронной почты и передачи файлов между UNIX-системами. Это сеть с промежуточным хранением на основе хостов, использующая коммутируемые телефонные каналы. Принцип работы: каждый узел-участник дозванивается до следующего UUCP-хоста и обменивается файлами и почтовыми сообщениями. Адресация строится на основе физического маршрута, образованного последовательностью таких соединений. UUCP открыта для любой UNIX-системы, желающей участвовать в работе сети. Между UUCP и ARPANET, BITNET или CSNET существуют «неофициальные» шлюзы электронной почты, позволяющие пользователям любой из этих сетей обмениваться почтой.

USENET — новостная служба UNIX, основанная на инфраструктуре UUCP и предоставляющая сервис электронных досок объявлений. USENET имеет как академических, так и коммерческих участников, а также партнёров в Европе, Азии и Южной Америке. Ни UUCP, ни USENET не имеют централизованного управления: добровольцы поддерживают и распространяют таблицы маршрутизации для сети. Каждый узел несёт собственные расходы и берёт на себя обязательство передавать трафик. Несмотря на опору на взаимное сотрудничество и анархический стиль управления, сеть функционирует и предоставляет своим участникам полезный — пусть и несколько ненадёжный — низкобюджетный сервис. На протяжении многих лет сеть выросла до масштабов всемирной, объединяя тысячи компьютеров.

«Будущее — уже сейчас»

Администрирование центра управления расширенной службой 911 для центров специальных услуг и крупных клиентов

Автор: The Eavesdropper

Март, 1988

Описание службы

Центр управления службой экстренного вызова 911 назначается в соответствии с действующими стандартными руководящими принципами одному из следующих центров:

• Центр специальных услуг (Special Services Center, SSC)
• Центр крупных клиентов (Major Accounts Center, MAC)
• Центр обслуживания и тестирования (Serving Test Center, STC)
• Центр управления межгородской связью (Toll Control Center, TCC)

В данном документе обозначение SSC/MAC используется взаимозаменяемо для любого из этих четырёх центров. Центры специальных услуг (SSC) или центры крупных клиентов (MAC) назначены точками приёма сообщений о неисправностях для всех неполадок, о которых сообщают клиенты E911 (PSAP). Абоненты, столкнувшиеся с неполадками при вызове E911, по-прежнему обращаются в местную службу ремонта (CRSAB), которая при необходимости перенаправляет сообщение в SSC/MAC.

Ввиду критической важности службы E911 необходимы контроль и своевременное устранение неисправностей. Являясь основной точкой контакта с клиентами E911, SSC/MAC занимает уникальное положение для мониторинга статуса неисправности и обеспечения её устранения.

Обзор системы

Номер 911 задуман как универсальный общенациональный телефонный номер, обеспечивающий населению прямой доступ к Пункту приёма экстренных вызовов (Public Safety Answering Point, PSAP). PSAP также называют Бюро экстренных служб (Emergency Service Bureau, ESB). PSAP — это агентство или учреждение, уполномоченное муниципалитетом принимать вызовы и реагировать на обращения в полицию, пожарную охрану и/или скорую медицинскую помощь. В учреждениях PSAP дежурят один или несколько операторов для приёма и обработки экстренных вызовов в соответствии с требованиями местного муниципалитета.

Важным преимуществом экстренной службы E911 является сокращение времени реагирования. Кроме того, E911 обеспечивает тесную координацию между агентствами, предоставляющими различные экстренные службы.

Коммутатор 1A ESS используется в качестве транзитного узла сети E911 для маршрутизации всех вызовов 911 на соответствующий (основной) PSAP, назначенный для обслуживания вызывающей станции. Функция E911 была разработана прежде всего для обеспечения маршрутизации на правильный PSAP всех вызовов 911. Избирательная маршрутизация позволяет направлять вызов

911, поступающий с конкретной станции в определённом районе, зоне или населённом пункте, на основной PSAP, назначенный для обслуживания данной абонентской станции, независимо от границ зон обслуживания. Таким образом, избирательная маршрутизация устраняет проблему несовпадения границ зон обслуживания с границами административных районов или иными политическими границами.

Функция E911 включает следующие услуги:

• Принудительное разъединение (Forced Disconnect)
• Альтернативная маршрутизация (Alternative Routing)
• Ночной режим (Night Service)
• Избирательная маршрутизация (Selective Routing)
• Автоматическое определение номера (Automatic Number Identification, ANI)
• Избирательный перевод (Selective Transfer)
• Автоматическое определение местоположения (Automatic Location Identification, ALI)
• Маршрутизация по умолчанию (Default Routing)

Руководящие принципы предварительной подготовки и установки

После подписания договора на систему E911 отдел сетевого маркетинга обязан сформировать комитет по вводу системы в эксплуатацию, в состав которого должен входить представитель SSC/MAC. В обязанности группы внедрения E911 входит координация всех этапов развёртывания системы E911 и формирование постоянно действующего субкомитета по техническому обслуживанию E911.

Маркетинг обязан предоставить SSC/MAC следующую информацию, специфичную для клиента, до начала сквозного тестирования вызовов:

• Все PSAP (наименование, адрес, местный контакт)
• Все идентификаторы каналов PSAP
• Заявка 1004 на услугу 911, включая сведения по каждому PSAP (разделы 1004 K, L, M)
• Конфигурация сети
• Сведения о подрядчиках (наименование, номер телефона, оборудование)

SSC/MAC необходимо знать, кто обслуживает оборудование и аппараты на PSAP — операционные компании Bell (BOC), независимая компания, сторонний подрядчик или их комбинация. Эта информация вносится в карточки профиля PSAP и ежеквартально проверяется на предмет изменений, дополнений и удалений.

Маркетинг получает Основной номер учётной записи (Major Account Number, MAN) и передаёт его в отдел корпоративных коммуникаций, чтобы начальные сервисные наряды содержали MAN и могли отслеживаться SSC/MAC через CORDNET. Каналы PSAP по определению являются официальными услугами.

Все сервисные наряды, необходимые для установки системы E911, должны содержать MAN, присвоенный городу/округу, приобретшему систему.

В соответствии с базовой стратегией SSC/MAC по обеспечению услуг, SSC/MAC будет выступать в роли Общего координационного центра (Overall Control Office, OCO) для всех каналов от узла до PSAP (официальные услуги) и любых других услуг для данного клиента. Для всего персонала SSC/MAC, задействованного в проекте, необходимо запланировать обучение на предварительном этапе.

Группа внедрения E911 должна сформировать постоянно действующий субкомитет по техническому обслуживанию до первоначального ввода системы E911 в эксплуатацию. Этот субкомитет разработает процедуры обеспечения качества после ввода в эксплуатацию, чтобы система E911 продолжала предоставлять качественные услуги клиенту. Вопросы обучения клиентов и сотрудников компании, интерфейсы для подачи заявок на устранение неисправностей для клиентов, телефонной компании и любых задействованных независимых телефонных компаний должны быть согласованы и внедрены до переключения E911. Наилучшим образом этими функциями может заниматься субкомитет группы внедрения E911, который разрабатывает руководящие принципы и получает обязательства по обслуживанию от взаимодействующих организаций. Руководитель SSC/MAC должен возглавлять этот субкомитет, в состав которого входят следующие организации:

1. **Центр управления коммутацией (Switching Control Center)**
• Трансляции E911
• Транкинг
• Аппаратное и программное обеспечение конечных узлов и транзитных коммутаторов

2. **Центр администрирования памяти последних изменений (Recent Change Memory Administration Center)**
• Ежедневное обновление последних изменений для трансляций TN/ESN
• Обработка ошибок достоверности и отказов

3. **Администрирование линий и номеров (Line and Number Administration)**
• Верификация трансляций TN/ESN

4. **Центр специальных услуг / Центр крупных клиентов (SSC/MAC)**
• Единая точка контакта по всем неполадкам PSAP и каналов узел–хост
• Регистрация, отслеживание и мониторинг статуса всех заявок на устранение неисправностей
• Передача, отслеживание и эскалация заявок
• Уведомление клиента о статусе и восстановлении
• Анализ «хронических» неисправностей
• Тестирование, установка и обслуживание каналов E911

5. **Установка и техническое обслуживание (SSIM/I&M)**
• Ремонт и обслуживание оборудования PSAP и аппаратов, принадлежащих телефонной компании

6. **Центр технического обслуживания мини-ЭВМ (Minicomputer Maintenance Operations Center)**
• Обслуживание каналов E911 (там, где применимо)

7. **Региональный инженер по техническому обслуживанию (Area Maintenance Engineer)**
• Техническая помощь при неисправностях сети E911, связанных с голосовой связью (CO–PSAP)

Руководящие принципы технического обслуживания

CCNC будет тестировать канал узла от устройства 202T на хост-площадке до устройства 202T на площадке узла. Поскольку каналы «хост–узел» (CCNC–MMOC) являются официальными услугами компании, CCNC передаёт все заявки по неисправностям каналов узла в SSC/MAC. SSC/MAC отвечает за тестирование и контроль восстановления этих каналов.

Несмотря на то что каналы «узел–PSAP» являются официальными услугами, MMOC передаёт заявки по неисправностям каналов PSAP в соответствующий SSC/MAC. SSC/MAC отвечает за тестирование и контроль восстановления неисправностей каналов PSAP.

SSC/MAC также получает сообщения от CRSAB/IMC о неисправностях абонентского вызова 911, которые не являются неисправностями линии. SSC/MAC отвечает за тестирование и устранение этих неисправностей.

Ответственность за техническое обслуживание распределена следующим образом:

Подразделение	Зона ответственности
SCC	Голосовая сеть (от ANI до PSAP); SCC отвечает за транзитный коммутатор
SSIM/I&M	Оборудование PSAP (модемы, CIU, аппараты)
Подрядчик	Оборудование PSAP (при наличии CPE)
SSC/MAC	Каналы PSAP–узел и голосовые каналы транзитный–PSAP (EMNT)
MMOC	Площадка узла (модемы, кабели и т.д.)

Примечание: все перечисленные рабочие группы обязаны устранять неисправности во взаимодействии с соответствующими рабочими группами.

Центр управления коммутацией (SCC) отвечает за трансляции E911/1AESS в транзитных центральных коммутаторах. Эти трансляции обеспечивают маршрутизацию вызовов E911, избирательный перевод, маршрутизацию по умолчанию, ускоренный набор и т.д. для каждого PSAP. SCC также отвечает за устранение неисправностей в голосовой сети (от инициации вызова до транзитного оборудования конечного узла).

Например, сбои ANI в инициирующих узлах находятся в зоне ответственности SCC.

Центр администрирования памяти последних изменений (RCMAC) выполняет ежедневные обновления трансляций транзитного узла (последние изменения) для маршрутизации отдельных телефонных номеров.

Последние изменения формируются на основе деятельности по сервисным нарядам (новое подключение, смена адреса и т.д.) и ежедневно компилируются в файл центром E911 (ALI/DMS E911 Computer).

SSIM/I&M отвечает за установку и ремонт оборудования PSAP. Оборудование PSAP включает контроллер ANI, контроллер ALI, наборы данных, кабели, аппараты и прочее периферийное оборудование, не принадлежащее подрядчику. SSIM/I&M отвечает за создание комплектов для технического обслуживания PSAP с запасными частями, включая контрольно-измерительные приборы, наборы данных и комплектующие для контроллеров ANI/ALI.

Центр специальных услуг (SSC) или центр крупных клиентов (MAC) является точкой приёма сообщений о неисправностях для всех неполадок (PSAP), о которых сообщает клиент. SSC/MAC направляет заявки в соответствующие организации и отслеживает статус неисправностей, при необходимости инициируя эскалацию. SSC/MAC закрывает заявки совместно с клиентом, а также анализирует и отслеживает «хронические» неисправности PSAP.

Центр корпоративных сетей и коммуникаций (CCNC) тестирует и передаёт заявки по неисправностям всех каналов «узел–хост». Все каналы E911 классифицируются как официальная собственность компании.

Центр технического обслуживания мини-ЭВМ (MMOC) обслуживает аппаратное обеспечение ЭВМ E911 (ALI/DMS) на хост-площадке. Этот MMOC также отвечает за мониторинг системы и сообщение

об определённых проблемах PSAP и системы в местные MMOC, SCC или SSC/MAC. Персонал MMOC также управляет программами, поддерживающими базу данных TN под руководством центра E911. Обслуживание ЭВМ NODE (интерфейса между PSAP и ЭВМ ALI/DMS) — функция MMOC на площадке NODE. MMOC на площадках NODE могут также участвовать в тестировании каналов «NODE–хост». MMOC также оказывает помощь при неисправностях «хост–PSAP» и сети передачи данных, не устранённых в ходе стандартных процедур.

Центр установки и технического обслуживания (IMC) отвечает за передачу заявок о неисправностях абонентов E911, не связанных с абонентской линией.

Центр E911 — выполняет функции системного администрирования и отвечает за общую работу программного обеспечения ЭВМ E911. Центр E911 проводит комплексный анализ неисправностей от А до Я и предоставляет статистическую информацию о производительности системы.

Этот анализ включает обработку запросов (заявок об ошибках) PSAP и передачу сетевых неисправностей. Центр E911 также выполняет ежедневную обработку последних изменений транзитного узла и предоставляет информацию в RCMAC для ввода в транзитный коммутатор. Центр E911 отвечает за ежедневную обработку базы данных ЭВМ ALI/DMS и предоставляет файлы ошибок и т.д. в отдел обслуживания клиентов для расследования и исправления. Центр E911 участвует во всех вводах системы в эксплуатацию и постоянной работе по техническому обслуживанию, а также оказывает помощь в разработке процедур, обучении и информировании всех групп.

Любая группа, получившая заявку по неисправности 911 от SSC/MAC, должна закрыть её в SSC/MAC или предоставить статус, если заявка была передана в другую группу. Это позволит SSC/MAC предоставить клиенту информацию о статусе или инициировать эскалацию по мере необходимости.

Любая группа, получившая заявку с хост-площадки (MMOC или CCNC), должна закрыть её обратно в этой группе.

MMOC должен уведомить соответствующий SSC/MAC о полном или частичном отказе хоста, узла или всех каналов узла, чтобы SSC/MAC мог отвечать на сообщения клиентов, которые могут поступать от PSAP. Это позволит избежать дублирования заявок о неисправностях. При полных отказах MMOC инициирует процедуры эскалации для узла через два (2) часа и для PSAP — через четыре (4) часа. Кроме того, MMOC уведомляет соответствующий SSC/MAC о том, что хост, узел или все каналы узла неработоспособны.

PSAP сообщает в SSC/MAC о неисправностях E911. Сотрудник, сообщающий о неисправности E911, может не знать идентификатора канала и поэтому называет наименование и адрес PSAP. Многие неисправности PSAP не привязаны к конкретному каналу. В случаях, когда звонящий не может предоставить идентификатор канала, SSC/MAC обязан определить его по профилю PSAP. Ни при каких обстоятельствах SSC/MAC не вправе отказаться принять заявку. Неисправность E911 должна быть обработана как можно быстрее, при этом SSC/MAC должен оказывать максимальную помощь при приёме заявки от звонящего.

SSC/MAC выполняет проверку/тестирование неисправности для определения соответствующей организации-получателя на основе следующих критериев:

• **Проблема с оборудованием PSAP:** SSIM/I&M
• **Проблема с каналом:** SSC/MAC
• **Проблема голосовой сети:** SCC (указать номер группы транков)
• **Проблема, затрагивающая несколько PSAP (нет отчёта ALI от всех PSAP):** Перед дальнейшим тестированием следует связаться с MMOC для проверки возможных неисправностей NODE или хост-ЭВМ.

SSC/MAC отслеживает статус поступивших заявок и при необходимости инициирует эскалацию. SSC/MAC закрывает заявки клиентов/компании с инициатором обращения. Группы с конкретными обязанностями по техническому обслуживанию, определёнными выше, по запросу SSC/MAC и постоянно действующего субкомитета по техническому обслуживанию расследуют «хронические» неисправности.

Все неисправности E911, относящиеся к категории «вне обслуживания», являются приоритетными заявками первого типа. Обрыв одного канала к PSAP считается неисправностью первого приоритета и должен обрабатываться так, как если бы PSAP был изолирован.

PSAP сообщает в SSC/MAC о неисправностях контроллера ANI, контроллера ALI или аппаратного оборудования.

ОТСУТСТВИЕ ANI: Если PSAP сообщает об отсутствии ANI (экран цифрового дисплея пуст), необходимо уточнить, наблюдается ли это состояние на всех экранах и при всех вызовах. Важно различать пустые экраны и экраны, отображающие «911-00XX» или все нули.

Если PSAP сообщает о данном состоянии на всех экранах при всех вызовах, необходимо уточнить, есть ли голосовой контакт с вызывающими абонентами. При отсутствии голосового контакта заявка должна быть немедленно передана в SCC, поскольку вызовы 911 не проходят, что может потребовать альтернативной маршрутизации на другой PSAP.

Если PSAP сообщает о данном состоянии на всех экранах, но не при всех вызовах, и при этом голосовой контакт с вызывающими имеется, заявка должна быть передана в SSIM/I&M для выезда. SSC/MAC перед выездом SSIM должен убедиться в SCC, что ANI передаётся импульсами.

Если PSAP сообщает о данном состоянии на одном экране при всех вызовах (остальные работают нормально), заявка должна быть передана в SSIM/I&M для выезда, поскольку неисправность изолирована в одном устройстве на площадке клиента.

Сбой ANI (т.е. все нули) свидетельствует о том, что ANI не получен PSAP от транзитного узла или был утрачен контроллером ANI PSAP. PSAP может получать аварийные сигналы «02», которые могут быть вызваны тем, что контроллер ANI зафиксировал более трёх подряд сбоев «все нули» на одном и том же транке. PSAP получил инструкцию сообщать об этом состоянии в SSC/MAC, поскольку оно может свидетельствовать о неисправности оборудования PSAP, которая может затрагивать всех абонентов, звонящих в PSAP. Когда при всех вызовах фиксируется состояние «все нули» или продолжают поступать аварийные сигналы «02», специалист по тестированию должен проанализировать ситуацию для определения надлежащих действий. Перед запросом на выезд специалист должно провести совместное тестирование с SCC при наличии признаков неисправности на транках «транзитный–PSAP».

При единичных случаях состояния «все нули» SSC/MAC должен направить SSIM/I&M для планового обслуживания оборудования в рамках «хронической» проверки.

PSAP получает инструкцию сообщать о единичных сбоях ANI в BOC на бланке запроса PSAP (бумажном), который направляется в группу E911 обслуживания клиентов и при необходимости передаётся в центр E911. Как правило, это касается только конкретного телефонного номера и не является состоянием, требующим обращения в SSC/MAC. Множественные сбои ANI, поступающие из одного конечного узла (XX обозначает конечный узел), свидетельствуют о возможной устойчивой неисправности в конечном узле или транках «конечный узел–транзитный». PSAP сообщит об этом в SSC/MAC, а SSC/MAC должен передать заявку в SCC, отвечающий за транзитный узел, для расследования и устранения. *Примечание: XX — это ESCO (номер экстренной службы), связанный с входящими транками 911 в транзитный коммутатор. Важно, чтобы C/MAC сообщил SCC, что отображается на PSAP (например, 911-0011), что указывает SCC на неисправный конечный узел.*

Примечание: *Необходимо, чтобы PSAP заполнял форму запроса по каждому сбою ANI.*

PSAP сообщает о неисправности каждый раз, когда адрес не отображается на дисплее адреса (пустой экран) при вызове E911. (Если запись отсутствует в базе данных 911 или произошёл сбой ANI, экран выведет соответствующее уведомление.) SSC/MAC должен уточнить у PSAP, наблюдается ли состояние «НЕТ ALI» на одном экране или на всех экранах.

Если состояние наблюдается на одном экране (остальные экраны получают информацию ALI), SSC/MAC направит SSIM/I&M для выезда.

Если ни один экран не получает информацию ALI, как правило, имеет место неисправность канала между PSAP и хост-ЭВМ. SSC/MAC должен провести тестирование и направить заявку на восстановление.

> ***Примечание:*** *Если SSC/MAC получает вызовы от нескольких PSAP, ни один из которых не получает ALI, проблема связана с узлом, каналами «узел–хост» или самой хост-ЭВМ. Прежде чем передавать заявку, SSC/MAC должен позвонить в MMOC для выяснения, не неисправен ли узел или хост.*

Аварийные сигналы на цифровом дисплее контроллера ANI в PSAP должны сообщаться сотрудниками PSAP. Эти аварийные сигналы могут свидетельствовать о различных неисправностях, поэтому SSC/MAC должен уточнить у PSAP, не нарушена ли работа какой-либо части системы E911.

SSC/MAC должен убедиться у оператора PSAP, что основная функция оборудования — приём вызовов E911. Если это так, SSC/MAC должен запросить выезд SSIM/I&M. Если оборудование не используется в первую очередь для E911, SSC/MAC должен рекомендовать PSAP обратиться к поставщику CPE.

> ***Примечание:*** *Эти неисправности могут вызывать серьёзную путаницу, когда в PSAP смешано вендорское оборудование и оборудование, обслуживаемое BOC.*
> *Представитель маркетинга должен предоставить SSC/MAC информацию о необычных или исключительных случаях, когда PSAP должен обращаться к своему поставщику.*
> *Эта информация должна быть включена в карточки профиля PSAP.*

Отказ контроллера ANI или ALI: Если хост-ЭВМ фиксирует отказ оборудования PSAP и оно не восстанавливается, MMOC сообщает о неисправности в SSC/MAC; поскольку оборудование PSAP вышло из строя, потребуется выезд специалиста.

Обрыв канала (линии) PSAP: MMOC предоставит SSC/MAC идентификатор канала, который хост-ЭВМ указывает как неисправный. Несмотря на то что каждый PSAP имеет два канала, обрыв любого из них должен рассматриваться как аварийная ситуация, поскольку отказ второго канала приведёт к изоляции PSAP.

Любые проблемы, выявленные MMOC на участке от узла до хост-ЭВМ, будут решаться непосредственно с соответствующими MMOC/CCNC.

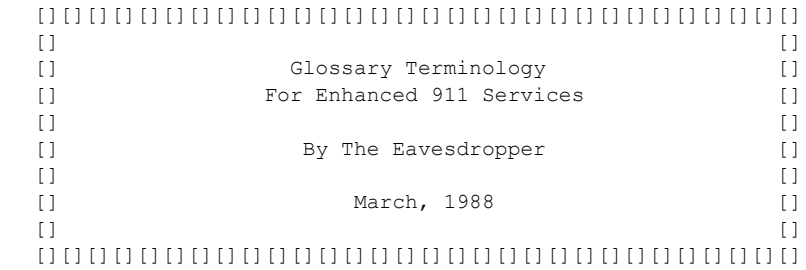
> ***Примечание:*** *Клиент обращается только тогда, когда неисправность очевидна для PSAP. При обрыве только одного канала к PSAP клиент может не знать о неисправности, хотя один канал неработоспособен, — на экране PSAP должно появиться соответствующее уведомление. Заявки, поступившие в SSC/MAC от MMOC или другого сотрудника компании, нельзя закрывать путём звонка в PSAP, так как это может привести к тому, что клиент ответит, что у него нет неисправности. Эти заявки могут быть закрыты только после получения подтверждения устранения неисправности и проверки у сотрудника компании, сообщившего о ней. Персонал MMOC может подтвердить устранение неисправности, проверив распечатку с хоста.*

Когда CRSAB получает жалобу абонента (например, невозможность дозвониться по 911), RSA должен получить как можно больше информации, пока клиент находится на линии.

Например: что произошло, когда абонент набрал 911? Заявка автоматически направляется в IMC для тестирования абонентской линии. Если неисправности линии не обнаружено, IMC передаёт неисправность в SSC/MAC. SSC/MAC связывается с группой E911 обслуживания клиентов, проверяет возможность вызова абонентом 911 и получает ESN. SSC/MAC проверяет ESN через 2SCCS. При совпадении обоих верификаций SSC/MAC передаёт заявку в SCC, отвечающий за транзитный узел 911, для расследования и устранения. MAC отвечает за отслеживание неисправности и уведомление IMC об её устранении.

Для получения дополнительной информации обратитесь к глоссарию терминов E911.

Терминологический словарь службы Enhanced 911



Автор: The Eavesdropper

Термины и определения

E911 — Enhanced 911 (Расширенная служба 911): Доступные функции включают избирательную маршрутизацию, избирательную переадресацию, фиксированную переадресацию, альтернативную маршрутизацию, маршрутизацию по умолчанию, автоматическое отображение номера, автоматическую идентификацию местоположения, ночной режим обслуживания, маршрутизацию по умолчанию и запись детализации вызовов.

End Office (Конечная АТС): Телефонная центральная станция, предоставляющая гудок вызова абоненту, набравшему 911. «Конечная АТС» передаёт ANI (автоматическую идентификацию номера) в транзитную станцию.

Tandem Office (Транзитная АТС): Телефонная центральная станция, выступающая в роли транзитного узла (или концентратора) для всех вызовов 911. Должна быть станцией типа 1AESS. Таблицы маршрутизации транзитной АТС содержат связки TN/ESN, обеспечивающие маршрутизацию вызовов 911 на нужный PSAP. Транзитная АТС выполняет поиск ANI (TN), полученного от конечной АТС, и находит ESN (информацию маршрутизации), соответствующий семизначному номеру, по которому осуществляется вызов на PSAP.

PSAP — Public Safety Answering Point (Пункт приёма экстренных вызовов): Как правило, службы полиции, пожарной охраны и/или спасения, определяемые местными органами самоуправления. «Входящий» PSAP без поддержки ANI или ALI просто принимает вызовы или переадресованные вызовы от другого PSAP.

ESN — Emergency Service Number (Номер экстренной службы, XXX): Присваивается телефонному номеру абонента в таблицах маршрутизации транзитной АТС. ESN представляет собой семизначный номер, по которому транзитная АТС направляет вызов на соответствующий PSAP. PSAP с поддержкой ALI также получают на дисплее информацию ESN, указывающую, какие службы полиции, пожарной охраны и спасения обслуживают телефонный номер, позвонивший на 911. ESN — уникальная комбинация служб полиции, пожарной охраны и спасения для целей маршрутизации вызова E911.

ANI — Automatic Number Identification (Автоматическая идентификация номера): Соответствует семизначному телефонному номеру абонента. ANI отображается в PSAP на цифровой консоли отображения ANI.

ALI — Automatic Location Identification (Автоматическая идентификация местоположения): Обеспечивает отображение адреса абонента, позвонившего на 911. При наличии ALI PSAP получает отображение ANI и ALI на экране. Дисплей ALI включает адрес абонента, населённый

пункт, штат, тип услуги, а если это организация — её наименование. PSAP также получает отображение информации соответствующего ESN (полиция, пожарная охрана, спасение).

Selective Routing (Избирательная маршрутизация): Возможность направить вызов на конкретный PSAP, обслуживающий адрес, связанный с TN, с которого поступил вызов на 911. Избирательная маршрутизация достигается построением таблиц трансляции TN/ESN в транзитной центральной станции. Эти таблицы формируются на основе базы данных E911, которая присваивает ESN каждому телефонному номеру исходя из адреса абонента. Деятельность по обработке сервисных заявок поддерживает базу данных E911 в актуальном состоянии. База данных E911, в свою очередь, генерирует изменения в транзитную АТС (через SCC или RCMAC) для обновления таблиц трансляции TN/ESN в базе данных транзитной АТС.

Selective Transfer (Избирательная переадресация): Предоставляет PSAP возможность переадресовать входящий вызов 911 в пожарную службу или службу спасения для конкретного номера, с которого поступил вызов, нажатием одной кнопки — «пожар» или «спасение». Например, если входящий вызов 911 сообщает о пожаре, оператор PSAP нажимает кнопку пожарной службы на консоли ANI; вызов возвращается на транзитную АТС, которая выполняет поиск семизначного номера, связанного с пожарной службой, для ESN, назначенного вызывающему TN, и автоматически направляет вызов в эту пожарную службу. Это отличается от «фиксированной» переадресации, которая направляет каждый вызов на один и тот же номер пожарной службы или спасения при нажатии соответствующей кнопки. Оборудование PSAP настраивается на поддержку фиксированного или избирательного режима переадресации.

Alternate Routing (Альтернативная маршрутизация): Обеспечивает заранее определённую маршрутизацию вызовов 911 в случаях, когда транзитная АТС не может направить вызовы по транкам 911 на конкретный PSAP из-за неисправностей или полной занятости транков.

Default Routing (Маршрутизация по умолчанию): Обеспечивает маршрутизацию вызовов 911 при сбое ANI. Вызов направляется на «дефолтный» ESN, связанный с NNX, из которого звонит абонент. Дефолтные ESN заранее задаются в таблицах маршрутизации и, как правило, соответствуют преобладающему ESN для данного проводного центра.

Night Service (Ночной режим обслуживания): Ночной режим работает аналогично альтернативной маршрутизации: вызовы, поступающие на конкретный PSAP, автоматически перенаправляются на другой заранее заданный PSAP, когда все транки переводятся в режим «занято» в связи с закрытием PSAP на ночь.

Call Detail Record (Запись детализации вызова): После завершения вызова 911 оператором PSAP ANI автоматически распечатывается на телетайпе, расположенном в PSAP. В распечатке указываются: время поступления вызова на PSAP, время его принятия оператором, номер оператора, время переадресации вызова (если применимо), время завершения вызова и номер группы транков, связанной с вызовом. Распечатки данных ALI также доступны, если PSAP приобрёл необходимое оборудование.

ANI Failure (Сбой ANI): Сбой конечной АТС при идентификации вызова и передаче ANI (телефонного номера) в транзитную АТС; либо сбой ANI между транзитной АТС и PSAP.

Misroute (Неверная маршрутизация): Любое условие, приводящее к тому, что вызов 911 поступает не на тот PSAP. Вызов может быть неверно маршрутизирован, если ESN и связанная с ним информация маршрутизации неверны в базе данных E911 и/или базе данных транзитной АТС. Вызов также может быть неверно маршрутизирован в случае сбоя ANI, при котором автоматически применяется маршрутизация по умолчанию.

Anonymous Call (Анонимный вызов): Если абонент ошибочно набирает семизначный номер, связанный с позицией PSAP, вызов поступает напрямую, а ANI отображается как 911-0000, что ALI идентифицирует как анонимный вызов. Семизначные номера, связанные с позициями PSAP, не

публикуются даже самим PSAP.

Spurious 911 Call (Ложный вызов 911): Иногда на PSAP поступает вызов, не связанный с тем, что абонент набрал 911 в экстренной ситуации. Это может быть абонент, который не набирал 911, но дозвонился до PSAP, набирая другой номер, или просто снял трубку и оказался соединён с PSAP. Подобные проблемы связаны с оборудованием — особенно когда вызовы исходят из электромеханических или шаговых АТС — и сообщаются центром E911 в службу сетевых операций по получении запроса от PSAP о неисправности. PSAP может принять вызов, а никого на линии не будет; при обратном звонке номер может оказаться отключённым или никто не отвечает. Это тоже сетевые неисправности, требующие расследования. Беспроводные телефоны также могут генерировать «ложные» вызовы на PSAP. Как правило, PSAP слышит разговор на линии, но абоненты не звонят на 911. PSAP может сообщить о ложных вызовах в службу устранения неисправностей, если они становятся навязчивыми, — например, когда один и тот же номер непрерывно вызывает.

No Displays (Отсутствие изображения на дисплее): Состояние, при котором экран ALI PSAP пуст. О таком сбое следует немедленно сообщать в SSC/MAC. Если все экраны в PSAP пусты, это указывает на проблему в цепях от PSAP до компьютера E911. Если отсутствие изображения наблюдается более чем на одном PSAP, возможна неисправность компьютера узла или компьютера E911. SSC/MAC должен связаться с MMOC для оценки работоспособности HOST-компьютера.

Record Not Found (Запись не найдена): Если хост-компьютер не может выполнить поиск по запросу ANI от PSAP, он отправляет сообщение «Record Not Found» на экран ALI PSAP. Это вызвано тем, что данные сервисной заявки для конкретного абонента не были внесены в базу данных E911, либо системными проблемами HOST-компьютера, из-за которых запись в данный момент недоступна.

No ANI (Отсутствие ANI): Это состояние означает, что PSAP принял вызов, но на консоли ANI не отображается телефонный номер. О таком состоянии PSAP должен немедленно сообщить в SSC/MAC.

PSAP Not Receiving Calls (PSAP не принимает вызовы): Если PSAP не может принимать вызовы или запрашивать данные от хост-компьютера E911 — например, из-за обрыва кабеля, — вызовы, поступающие на этот PSAP, необходимо перенаправить на другой PSAP. Для перенаправления вызовов в таблицах трансляции E911 транзитной АТС необходимо уведомить Центр управления коммутацией (Switching Control Center).

MSAG — Master Street Address Guide (Основной справочник уличных адресов): Журналы MSAG контролируются муниципалитетом, приобретшим услугу E911 ALI: именно муниципалитет определяет, какие службы полиции, пожарной охраны или спасения будут обслуживать конкретную улицу и диапазон номеров домов. Для этого ESN присваивается каждому диапазону улиц — чётному, нечётному, населённому пункту — в пределах обслуживаемого округа или муниципалитета. Эти MSAG используются затем как фильтр для обработки сервисных заявок в базе данных компьютера E911 с целью присвоения ESN отдельным записям TN. Это гарантирует, что каждый абонент будет направлен в правильную службу в соответствии со своим адресом. В округе без ALI телефонная компания использует коды TAR для присвоения ESN и округ не контролирует назначение ESN. Коды TAR представляют налоговый орган для данного абонента, которому должны соответствовать его службы полиции, пожарной охраны и спасения. Метод MSAG, разумеется, точнее, поскольку использует фактический адрес обслуживания абонента для маршрутизации вызова и обеспечивает округу бóльшую гибкость при назначении пожарных и спасательных районов и т. д. Группа E911 службы работы с клиентами ведёт базу данных компьютера E911 и взаимодействует с округом (заказчиком) по всем вопросам MSAG и деятельности с базой данных.

Advanced Bitnet Procedures

Автор: VAXBusters International

Приветствую! Я нашёл время и написал файл о некоторых более сложных операциях в Bitnet. Надеюсь, вам понравится! :-)

•----------

Вы можете отправить несколько сообщений одному пользователю user@node под VAX/VMS и JNET, просто набрав:

```
$ SEND/REMOTE <host> <user>
```

Это позволит собирать сообщения с терминала до тех пор, пока не будет введена пустая строка или CTRL-Z.

Под Unix пакет UREP широко используется для подключения Unix-машин к Bitnet. Основные команды пользователя выглядят следующим образом:

Сообщения

```
netwrite user@host
```

Отправить одно или несколько сообщений указанному пользователю Bitnet. Netwrite читает сообщения со стандартного ввода до достижения EOF. Если вызывается с терминала, netwrite завершается также при вводе пустой строки.

Когда вы получаете сообщения Bitnet на Unix-хосте, UREP ищет исполняемый файл с именем `.exwrite` в вашем домашнем каталоге. Если такого файла нет, сообщение просто выводится на ваш терминал. Если `.exwrite` присутствует, UREP запускает эту программу (которая может быть shell-скриптом) с пятью параметрами:

```
<To System> <To User> <From System> <From User> <Tty>
```

Параметр ` указывает терминал, на который UREP хотел отправить сообщение. Затем UREP передаёт сообщения в .exwrite` через стандартный ввод. Формат стандартного ввода следующий:

```
<count (1 байт)><message (<count> байт)>
```

Для отображения этих сообщений необходима программа на «C», поскольку shell-скрипт не способен без проблем обрабатывать отдельные байты. В конце этого файла я привожу свой exwrite.c для начала работы.

Как правило, `.exwrite` используется для журналирования всех входящих сообщений Bitnet. Разумеется, его можно расширить, чтобы отправлять сообщения обратно отправителю, когда вы уходите на обед, и т.д. Кстати, `.exwrite` вызывается с идентификатором пользователя принимающего пользователя, так что это не представляет реальной угрозы безопасности.

```
netcopy user@host [ options ]
```

Копировать файл указанному пользователю Bitnet. Наиболее важная опция — `"name=."`, с помощью которой можно указать имя файла, которое будет использоваться на машине получателя. Подробности — на странице руководства.

Когда вы получаете файлы Bitnet на Unix-машине с запущенным UREP, они будут помещены в ваш домашний каталог под именем `:.`. Эти файлы представлены в формате NETDATA, и их необходимо преобразовать в текстовые файлы ASCII, прежде чем использовать под Unix. Это можно сделать командой:

```
netdata [ <input_file> [ <output_file> ] ]
```

Если `` ` `` не указан, используется стандартный ввод. Если `` ` `` не указан, используется стандартный вывод.

Команды Bitnet

Хотя Bitnet не поддерживает удалённый вход, вы можете выполнять ограниченный набор команд на удалённых хостах. Эти команды можно использовать для запроса состояния узла, списков вошедших пользователей, времени и некоторых других вещей.

Это работает следующим образом:

```
JNET:   $ SEND/COMMAND <host> [ <command> ]
UREP:   % netexec <host> [ <command> ]
CMS:    SMSG <server> CMD <host> <command>
```

`` в CMS — это управляющий процесс Bitnet. В Европе он обычно называется «EARN». В США это может быть «BITNET» или «RSCS». Здесь придётся разобраться самостоятельно.

`` ` `` — это имя хоста Bitnet, на котором вы хотите выполнить `.` В JNET и UREP вам будет предложено ввести несколько команд, если оставить поле `` ` `` пустым. Опять же, ввод завершается по EOF или пустой строке.

Следующие команды я нашёл полезными в повседневной жизни:

```
CPQ N           Получить список пользователей, вошедших в систему на <host>.
                Эта команда должна существовать на каждом хосте Bitnet,
                однако некоторые системные администраторы ограничивают её
                по соображениям безопасности. На хостах JNET и UREP
                команда FINGER выполняет аналогичную, но более подробную функцию.

CPQ T           Заставить <host> сообщить вам текущее время в его местоположении.

Q <otherhost>   Заставить <host> сообщить вам, каков следующий прыжок до
                <otherhost>. Полезно, когда вас интересует топология сети.

Q <ohost> A     Заставить <host> сообщить, какой файл в данный момент активен
                (передаётся) для <ohost>. Работает только для машин,
                напрямую подключённых к <host>.

Q <ohost> Q     Заставить <host> показать очередь файлов, ожидающих передачи
                в <ohost>. Полезно, когда нужно отследить отправленный
                в сеть файл.

Q SYS           Заставить <host> сообщить об имеющихся у него RSCS-связях.
```

К сожалению, MVS-хосты не понимают ни одну из этих команд и просто выдают сообщение об ошибке. Их можно распознать по строке «HASP» где-либо в сообщении об ошибке.

Приятной работы!

exwrite.c для Unix-хостов с UREP

```
/* exwrite.c - formatter for UREP rscs messages                          */

include <stdio.h>
```

```
include <sysexits.h>
include <pwd.h>
include <ctype.h>

main(argc, argv)

        int             argc;
        char            *argv[];
       struct  passwd  *pw;
        char            fname[255];
        FILE            *term;
        FILE            *log;
        int             count;
        char            buf[1024];
        char            *from_user;
        char            *from_host;
        char            *to_user;
        char            *to_host;
        char            *to_tty;
        char            *home_dir = "/tmp";

        if (argc != 6)
                fprintf(stderr, "%s: Invalid arguments\n", argv[0]);
                exit(EX_USAGE);


        /* initialise variables                                         */
        to_host = argv[1];
        to_user = argv[2];
        from_host = argv[3];
        from_user = argv[4];
        to_tty = argv[5];

        /* convert the receiving user to lowercase.  Under Unix, all    *
         * user names normally are lower case, and we need a valid      *
         * user name to determine the home directory                    */
        for (; *to_user; to_user++)
                *to_user = tolower(*to_user);
        to_user = argv[2];

        /* get the home directory of the receiving user                 */
        if (pw = getpwnam(to_user))
                home_dir = pw->pw_dir;

        /* open the terminal, exit if the open fails                    */
        sprintf(fname, "/dev/%s", to_tty);
        if (!(term = fopen(fname, "w")))
                exit(EX_OSERR);

        /* open the rscs log file                                       */
        sprintf(fname, "%s/.rscslog", home_dir);
        log = fopen(fname, "a");

        /* if the message is not coming from the relay, write the       *
         * sending user and host name to the specified terminal         */
        if (strcmp(from_user, "RELAY"))
                fprintf(term, "From %s@%s:\r\n", from_user, from_host);

        /* read in the RSCS messages and send them to the terminal      *
         * and to the logfile if it has been opened.                    *
         * In the log file, all lines are preceded by the sending user  *
         * and host name.                                               */
        while ((count = getchar()) != EOF)
                if ((count = fread(buf, 1, count, stdin)) > 0)
                        fwrite(buf, 1, count, term);
                        fprintf(term, "\r\n");
                        if (log)
                                fprintf(log, "%s@%s: ", from_user, from_host);
                                fwrite(buf, 1, count, log);
                                fprintf(log, "\n");
        exit(EX_OK);
```

Специальные коды зон

Автор: >Unknown User<

3 января 1989 г.

Приветствую! Я собрал информацию о SAC (специальных кодах зон) для вашего ознакомления; сюда входят коды 700, 800 и 900.

Большинство телефонных пользователей в Соединённых Штатах хорошо знакомы со службой 800: это номер, по которому они звонят и не несут НИКАКИХ расходов (даже без тарификации по единицам сообщений в большинстве районов).

Затем есть служба 900 — то, что большинство людей воспринимают как «добавленную стоимость»: то есть вы платите за информацию больше, чем за передачу звонка. Стоимость обычно варьируется от 35 центов до нескольких долларов — либо за тарифицированную по времени услугу, либо за услугу с произвольной продолжительностью. Служба 900 бывает двух разновидностей: AT&T и «все остальные».

Наконец, существует служба 700, которую многие помнят как Alliance Teleconferencing. Это третий «канонический» SAC. С небольшими ограничениями данный SAC полностью отдан на усмотрение IEC.

Рассмотрим их подробнее.

Служба 800

Служба 800 предоставляется различными IEC. Каждый NXX в SAC 800 закреплён за определённым оператором, который отвечает за распределение номеров из этого блока клиентам и обеспечивает трансляцию десяти цифр.

Оператор должен иметь подключение Feature Group D для инициирования звонков из исходящего коммутатора (напрямую или через транзитный узел доступа).

В будущем, когда CCIS получит широкое распространение, в базе данных будет выполняться запрос [Кто обслуживает 1-800-985-1234?] и вызов будет маршрутизирован соответствующим образом. Поясню: сейчас оператор определяется по NXX. В будущем оператор будет определяться по всем 7 цифрам.

Аналогичная ситуация со службой 900. Каждый оператор может резервировать NXX у BellCore (организации, которая среди прочего занимается выдачей префиксов и кодов зон). Это недёшево! Получить сам номер бесплатно (существуют требования, которые я здесь не рассматриваю), но для его «активации» в рамках LATA придётся заплатить — в зависимости от:

1. Количества запрашиваемых префиксов;
2. Того, является ли это службой 800 или 900;
3. Количества транзитных/оконечных узлов в LATA.

Для КАЖДОГО узла требуется отдельный объём работ, поскольку КАЖДАЯ таблица маршрутизации должна быть изменена. Подробнее о службе 900 я расскажу далее в этом файле.

Когда вы, как обычный абонент, набираете 1-800-222-1234 (вымышленный номер, прошу не беспокоить), инициируется следующая последовательность:

1. Если вы звоните из электронного коммутатора (DMS-100, DMS-200, 1A ESS, 5 ESS), то 800-222 будет транслировано в «AT&T» и система начнёт искать свободный канал в транковой группе, помеченной для исходящих вызовов 800. Если такой не найдётся — переход к шагу 3.

2. Если вы звоните из неэлектронного коммутатора (SxS, XB и некоторые варианты ESS), вызов поступит на транзитный узел доступа, к которому «привязан» ваш коммутатор, где 800-222 будет транслировано в «AT&T».

Примечание: если на этом этапе у номера нет трансляции, вы получите сообщение об ошибке от CO.

3. Найти канал в транковой группе, помеченной для исходящих вызовов 800. Если не найдётся — воспроизвести абоненту сообщение «В связи с перегрузкой сети ваш звонок на номер 800 не может быть завершён», или отбой, или что-то ещё (зависит от фазы луны и т.д.).

4. Оконечный коммутатор отправит следующий импульсный поток (в MF):

```
KP + II + 3/10D + ST + KP + 800 222 1234 + ST
```

Примечание: это упрощение; существуют тонкости передачи ANI, выходящие за рамки данного файла.

II = 2 информационных цифры. Типичные значения:

• `00` — обычная ANI .. следуют 10 цифр
• `01` — линия ONI ... следует NPA
• `02` — сбой ANI ... следует NPA

3/10D = 3 или 10 цифр. Либо NPA, либо полный десятизначный номер. KP и ST — управляющие тональные сигналы.

5. Оператор получает всё это (и, вероятно, отправляет ANI в мусорную корзину) и транслирует номер 800 в так называемый PTN, или Plant Test Number (например, 617-555-9111). Затем вызов маршрутизируется так, как если бы абонент набрал этот десятизначный номер напрямую. Разумеется, данные о тарификации помечаются как звонок на номер 800, поэтому абонент, принимающий звонок, платит соответствующую сумму.

Из 800 возможных NXX в настоящее время назначены 409. Оператор дальней связи может получить один номер 800 и четыре номера 900 просто за оформление документов. Но для получения большего количества нужно доказать 70%-ную загруженность имеющихся и обосновать реальную необходимость в дополнительной ёмкости.

Ниже приведена полная таблица соответствия 800-NXX и операторов дальней связи. Обратите внимание, что не каждый NXX действителен во всех регионах.

Таблица трансляции 800/OCN (пересмотренная)

Действует с 10 октября 1988 г.

[Таблица из 409 записей — опущена]

Примечания к таблице 800

`*1` — Зарезервировано для будущего использования

*2 — Эти коды NXX, как правило, зарезервированы для тестовых приложений; они могут резервироваться для тестирования транзитных узлов доступа из оконечных коммутаторов.

Также следует отметить: следующие NXX зарезервированы для RCCP (радиопейджинг общего пользования) по усмотрению местного оператора коммутируемой связи:

202, 212, 302, 312, 402, 412, 502, 512, 602, 612, 702, 712, 802, 812, 902 и 912.

Справочник OCN

ADG - Advantage Network, Inc.
ALG - Allnet Communication Services
AAM - ALASCOM
ARZ - AmeriCall Corporation (Calif.)
ATX - AT&T
BUR - Burlington Tel.
CAN - Telcom Canada
CQU - ConQuest Comm. Corp
CUX - Compu-Tel Inc.
DCT - Direct Communications, Inc.
EDS - Electronic Data Systems Corp.
EXF - Execulines of Florida, Inc.
FDN - Florida Digital Network
FST - First Data Resources
GTS - Telenet Comm. Corp.
ITT - United States Transmission System
LDL - Long Distance for Less
LNS - Lintel Systems
LTQ - Long Distance for Less
MCI - MCI Telecommunications Corp.
MEC - Mercury, Inc.
MIT - Midco Communications
NLD - National Data Corp.
NTS - NTS Communications
ONE - One Call Communications, Inc.
PLG - Pilgrim Telephone Co.
RBW - R-Comm
SAN - Satelco
SDY - TELVUE Corp.
SLS - Southland Systems, Inc.
SNT - SouthernNet, Inc.
TBQ - Telecable Corp.
TDX - Cable & Wireless Comm.
TEM - Telesystems, Inc.
TET - Teltec Savings Communications Co
THA - Touch America
TKC - TK Communications, Inc.
TMU - Tel-America, Inc.
TOM - TMC of Montgomery
TSF - SOUTH-TEL
TTH - Tele Tech, Inc.
TXN - Tex-Net
UTC - U.S. Telcom, Inc. (U.S. Sprint)
VST - STAR-LINE
WUT - Western Union Telegraph Co.

AGN - AMRIGON
AMM - Access Long Distance
ARE - American Express TRS
ATC - Action Telecom Co.
BML - Phone America
CAB - Hedges Communications
CNO - COMTEL of New Orleans
CSY - COM Systems
CYT - ClayDesta Communications
DLT - Delta Communications, Inc.
ETS - Eastern Telephone Systems, Inc.
FDG - First Digital Network
FDT - Friend Technologies
GCN - General Communications, Inc.
HNI - Houston Network, Inc.
LDD - LDDS-II, Inc.
LGT - LITEL
LSI - Long Distance Savers
MAL - MIDAMERICAN
MDE - Meade Associates
MIC - Microtel, Inc.
MTD - Metromedia Long Distance
NTK - Network Telemanagement Svcs.
ONC - OMNICALL, Inc.
PHE - Phone Mail, Inc.
PRO - PROTO-COL
RTC - RCI Corporation
SCH - Schneider Communications
SIR - Southern Interexchange Services
SNH - Sunshine Telephone Co.
SOC - State of California
TDD - Teleconnect
TED - TeleDial America
TEN - Telesphere Network, Inc.
TGN - Telemanagement Consult't Corp.
TID - TMC South Central Indiana
TLS - TELE-SAV
TNO - ATC Cignal Communications
TOR - TMC of Orlando
TSH - Tel-Share
TTU - Total-Tel USA
USL - U.S. Link Long Distance
VOA - Valu-Line
WES - Westel

Примечание: там, где местные телефонные компании, например Illinois Bell, предоставляют службу 800, они приобретают блоки номеров у AT&T на префиксах, закреплённых за AT&T. Однако они вправе приобретать блоки номеров у любого оператора по своему выбору.

Этот список также распространяется на таблицу трансляции 900/OCN (приведённую далее в этом файле).

Служба 900

Как я упоминал ранее, существует два варианта службы 900: AT&T и «все остальные». «Все остальные» обрабатываются точно так же, как служба 800, описанная выше, за исключением того, что IEC, вероятно, будет использовать информацию ANI для выставления вам счёта (напрямую или через BOC — в каждом случае в соответствии с применимыми тарифами и договорными отношениями между IEC и BOC).

AT&T 900 — весьма любопытное явление. Она была разработана как служба «массового завершения вызовов». Когда вы набираете номер 900 от AT&T (например, номер для прослушивания аудио с миссии космического шаттла), вы попадаете на один из двенадцати «узлов», разбросанных по всей стране. Каждый из этих узлов способен принимать 9000 вызовов >В СЕКУНДУНЕ< «кто оплачивает звонок» (существуют и бесплатные номера 900), а «сколько человек может обслужить одновременно». IP отвечает за предоставление программного аудиоконтента. AT&T запрещено предоставлять услуги аудиопрограмм (т.е. записанные сообщения). Как и у любого правила, здесь тоже есть исключения.

Ниже приведена полная таблица соответствия 900-NXX и операторов дальней связи.

Таблица трансляции 900/OCN (пересмотренная)

Действует с 10 октября 1988 г.

Обратите внимание, что эта таблица отличается от таблицы 800, поскольку значительно меньше NXX кода 900 назначено.

[Таблица из ~130 записей — опущена]

Служба 700

Последний SAC, который мы рассмотрим, — это 700. Я видел рекламу на ночном телевидении для службы Group Access Bridging (GAB) с номерами 700 и громоздкой последовательностью набора. Один из примеров — 10041-1-700-777-7777. Если набрать 1-700-555-4141, вы услышите запись с сообщением о вашем оператора равного доступа. (Некоторые операторы игнорируют последние четыре цифры, и любой номер 700-555 воспроизведёт это объявление.)

Сигнализация такая же, как у службы 800, и тарификация может как применяться, так и не применяться — полностью на усмотрение IEC. В штате Нью-Йорк согласно тарифу PSC можно оформить блокировку номеров 900 и/или 700, а также блокировку 976, 970, 550 и 540 в различных комбинациях.

То, что у одного оператора может быть горячей линией клиентского сервиса (наберите 1-700-I AM LOST), у другого может оказаться коммерческим продуктом. Стандартизация использования 700 от одного IEC к другому практически ОТСУТСТВУЕТ.

Последний способ набора, о котором стоит упомянуть, — так называемый «сквозной набор» (cut through dialing). Попробуйте набрать 10220. Если Western Union работает в вашем городе, вы услышите гудок готовности к набору в стиле FG-A. Предположительно, имея карточку Western Union «Calling Card», вы могли бы осуществить вызов.

Глоссарий

ANI — Автоматическая идентификация номера (Automatic Number Identification). Последовательность MF, идентифицирующая вашу линию для информации о тарификации. Часто путают с ANAC (Automatic Number Announcement Circuit) — схемой, которая воспроизводит ваш номер синтезированным голосом.

BOC — Дочерняя компания Bell (Bell Operating Company). Часто употребляемый не по назначению термин, который в общем использовании означает «ваш местный оператор коммутируемой связи». Поскольку большинство телефонов в стране обслуживались тем, что раньше называлось системой Bell, мы склонны использовать этот термин. Однако правильным термином в данном случае является «оператор коммутируемой связи [EC]». Они предоставляют услуги в пределах вашего LATA.

FG-A — Feature Group A. Завершение на стороне линии для операторов дальней связи. Старый способ набора: 555-1234 для Widget Telephone Company, затем код доступа и номер — это и называется FG-A.

FG-B — Feature Group B. Завершение на стороне транка для операторов дальней связи (также известна как ENFIA B). Служба 950. Это сервис в масштабах LATA, не требующий оплаты единиц сообщений от абонента. ANI передаётся только при завершении транков в оконечном коммутаторе (в отличие от транзитного узла доступа).

FG-D — Feature Group D. Завершение на стороне транка. Обеспечивает набор 10xxx, подписку с набором 1+, а также службы равного доступа 800/900. Доступна только в электронных коммутаторах и некоторых коммутаторах 5XB (через устройство под названием Adjunct Frame).

GAB — Групповое аудиомостирование (Group Audio Bridging). Несколько человек звонят на один и тот же номер, чтобы общаться с другими звонящими на тот же номер. «Вечеринки» или линии «чата».

IEC — Межузловой оператор связи (Inter-Exchange Carrier). Тот, кто фактически передаёт вызовы из одного места в другое. AT&T, Sprint, MCI — всё это IEC.

IP — Информационный провайдер (Information Provider). Тот, кто продаёт услугу с добавленной стоимостью по телефону. Когда вы платите за ИНФОРМАЦИЮ, которую получаете, а также за ТРАНСПОРТИРОВКУ звонка.

NXX — Нотационное соглашение для того, что раньше называлось «префиксом». N обозначает цифры от 2 до 9, X — цифры от 0 до 9. Существует 800 допустимых комбинаций NXX, но некоторые зарезервированы для местного использования (411 — справочная, 611 — служба ремонта, 911 — экстренный вызов и т.д.).

ONI — Идентификация номера оператором (Operator Number Identification). В районах с некоторыми видами услуг с разделением линии CO не может определить, кто вы, и оператор выходит на линию и спрашивает: «С какого номера вы звоните?». Вы можете солгать — оператор вынужден вам доверять. Впрочем, оператор МОЖЕТ знать, с какого ПРЕФИКСА вы звоните.

PTN — Заводской тестовый номер (Plant Test Number). Обычный десятизначный номер, присваиваемый вашей входящей линии WATS. Этот номер МОЖЕТ быть недоступен для набора из местного CO. (У знакомого есть линия WATS в Амхерсте, штат Массачусетс [413-549], — нельзя набрать PTN локально, но можно, если заходить через транковую линию дальней связи.)

SAC — Специальный код зоны (Special Area Code). Термин BellCore для кодов зон, которые на самом деле не являются географическими местами, а обозначают классы обслуживания.

Срываем покров тайны с Ma Bell

Новый взгляд на базовые телефонные системы

Автор: VaxCat

Хотя телефон появился значительно раньше радиосвязи, он далеко не так прост, каким кажется на первый взгляд. Некоторые аспекты телефонных систем весьма интересны и поистине изобретательны. В этом файле я опишу ряд наиболее любопытных и, пожалуй, менее известных сторон телефонных систем. Прежде чем продолжить, хочу оговориться и заранее извиниться: часть информации в этом файле может быть не вполне полной, устаревшей или не совсем точной.

Я не работаю ни в одной телефонной компании и потому не имею неограниченного доступа к внутренней документации. Кроме того, практически нет книг или журналов, описывающих устройство телефонных систем США. Большая часть изложенного собрана по крупицам из множества источников: книг, популярных журналов, изданий по компьютерным системам передачи данных, справочников и, порой, просто слухов.

Я старался по возможности увязать все эти разрозненные фрагменты в связную картину, но убедиться в правильности каждой мелкой детали невозможно. Воспринимайте эту статью как исторический роман — в целом достоверный и увлекательный, независимо от того, верен ли он в каждой частности. С этим разобравшись, продолжим.

Абонент и центральная станция

Вас как клиента принято называть «абонентом». Ваш телефон соединяется с центральной станцией (ЦС) двухпроводным кабелем, который может тянуться на многие километры и обладать сопротивлением в сотни и даже тысячи ом. По существу, этот кабель представляет собой симметричную линию с характеристическим сопротивлением около 900 Ом, хотя оно существенно варьируется в зависимости от типа кабеля, погодных условий и конкретного соединения. Именно поэтому так сложно добиться точного баланса гибридного телефонного патча.

Основным источником питания центральной станции служат аккумуляторные батареи на 48 вольт, постоянно поддерживаемые в заряженном состоянии капельным зарядом. Эта батарея подключается к вашей линии через абонентское реле и балансный звуковой трансформатор. Реле достаточно чувствительно, чтобы фиксировать даже очень слабые токи в линии.

Принцип работы телефонного аппарата

Кнопки, выступающие из корпуса телефона при поднятии трубки, управляют рычажным переключателем. Название, вероятно, восходит ко временам, когда трубка (или ещё раньше — только наушник) висела на крюке сбоку аппарата. В любом случае, когда трубка лежит на аппарате, говорят, что телефон «на крюке» (on hook), а когда вы поднимаете её для звонка — «снят с крюка» (off hook).

При положенной трубке линия соединена только со звонком (звонковой цепью). Поскольку в звонковой цепи имеется конденсатор, постоянный ток через телефон не течёт. Вследствие этого абонентское реле на ЦС обесточено, что сигнализирует станции о том, что трубка положена.

Раз через линию и телефон не течёт ток, нигде нет и падения напряжения — поэтому, измерив напряжение на телефонной линии у своего аппарата, вы увидите все 48 вольт (или даже больше, если аккумуляторы ЦС хорошо заряжены).

Положительный (заземлённый) провод называется «tip» (наконечник), отрицательный — «ring» (кольцо); эти названия соответствуют наконечнику и кольцу трёхконтактного телефонного штекера.

Установка соединения

Когда вы снимаете трубку, телефон переходит в режим «снят с крюка». Это замыкает цепь постоянного тока через диск, микрофон и гибридную схему — по существу, сложный трансформаторный узел.

В этот момент начинает течь ток из батареи через вашу линию и телефон, и абонентское реле на ЦС срабатывает. Напряжение на линии у вашего аппарата падает до нескольких вольт, поскольку линия нагружена малым сопротивлением телефона. ЦС ищет свободные схемы набора номера и, найдя их, посылает на ваш телефон сигнал «готово к набору» (гудок). Услышав его, вы начинаете набирать номер.

Импульсный набор

Поговорим о дисковом (импульсном) наборе — том типе телефона, диск которого вращается пальцем (о тональном наборе поговорим позже). При наборе цифры диск работает как короткое замыкание до тех пор, пока вы не отпустите его и встроенная пружина не вернёт диск в исходное положение. В процессе возврата диск начинает размыкать и замыкать цепь в определённой последовательности, соответствующей набранной цифре. При наборе «1» цепь разрывается один раз, при наборе «9» — девять раз. По мере возврата диска абонентское реле на ЦС размыкается и замыкается синхронно, что позволяет станции распознать нужный номер.

После окончания набора диск становится простым короткозамкнутым контактом, пропускающим ток через микрофон и гибридную схему. Поскольку микрофон угольный, ему необходим этот ток для работы. Получив полный номер, ЦС начинает обработку вызова. Если вы набрали номер другого абонента в том же районе, станция может соединить вас напрямую с его линией. Звонки на несколько более далёкие аппараты могут маршрутизироваться через другую ЦС, тогда как звонки на дальние расстояния могут проходить через один или несколько транзитных узлов (tandem) и, возможно, через множество ЦС, прежде чем достигнуть адресата. По завершении этого процесса вы можете услышать либо сигнал вызова (означающий, что аппарат на другом конце звонит), либо один из нескольких видов сигналов «занято», либо просто тишину — если где-то что-то пошло не так.

Двустороннее аудио и тональные сигналы

В процессе разговора кабель одновременно переносит звук в обоих направлениях. Ваш угольный микрофон изменяет ток в цепи, и это изменение фиксируется балансным трансформатором на ЦС. Одновременно звук, приходящий к вашему аппарату, поступает через гибридную схему на ваш наушник. В терминологии телефонных компаний микрофон принято называть «передатчиком», а наушник — «приёмником».

Возможно, вас заинтересует состав различных тональных сигналов, которые можно услышать в телефоне. Эти сигналы важны, в частности, для разработчиков систем компьютерной передачи данных, которым нужно создавать оборудование, распознающее тональный набор и иные сигналы:

• **Гудок готовности (dial tone):** в старых АТС — комбинация 120 и 600 Гц, в новых — комбинация 350 и 440 Гц. В начале гудка нередко наблюдается небольшое изменение постоянного напряжения на линии, которое тоже можно детектировать.

• **Сигнал «занято»:** комбинация 480 и 620 Гц, чередующаяся по полсекунды включено / полсекунды выключено (то есть 60 прерываний в минуту) при занятости вызываемого абонента.

• **Занятость межстанционных или межгородских линий:** тот же сигнал, но с прерываниями 30 или 120 раз в минуту. Это стандарт, принятый международной организацией по телекоммуникациям МККТТ (CCITT), однако иногда применяются другие частоты — до 2 кГц. Звук, напоминающий сирену и изменяющийся от 200 до 400 Гц, нередко используется для других сигналов об ошибках.

• **Сигнал вызова (ringback tone):** слышен вам, когда телефон на другом конце соединения звонит. В наши дни чаще всего представляет собой комбинацию 440 и 480 Гц, хотя между ЦС существуют большие различия. Нередко используется более высокая частота — например, 500 Гц, прерываемая с частотой 20 Гц; встречаются и другие тоны. Обычно сигнал длится 2 секунды, после чего следует пауза 4 секунды.

• **Вызывной ток (ringing current):** фактически приводит в действие звонок телефона. Поскольку в цепи звонка есть конденсатор, необходимо переменное напряжение. Разные компании используют разные параметры, но наиболее распространён ток 90 вольт, 20 Гц. Так как типичный телефон может находиться на расстоянии тысяч метров от ЦС, тонкие провода обладают довольно большим сопротивлением, и через звонок может протекать лишь относительно небольшой ток — явно недостаточный для звонка уровня дверного. Проблема решается тем, что звонок механически настраивается в резонанс на частоту вызова: даже небольшой мощности хватает, чтобы боёк начал двигаться достаточно энергично для воспроизведения громкого звука. Именно поэтому применяется переменный ток низкой частоты. Хотя это создаёт определённые трудности с генерацией сигнала 20 Гц при достаточно высоком напряжении, данный подход обеспечивает преимущество: звонок откликается на вызывной ток лишь тогда, когда его частота близка к собственной резонансной. Если изготовить два звонка — один резонансный на 20 Гц, другой на 30 Гц — и подключить их к одной линии, можно звонить в каждый по отдельности, подавая вызывной ток нужной частоты. Это удобно при организации одного звонка на общей абонентской линии (party line).

Конструкция телефонного аппарата

Рассмотрим компоненты самого телефона. Остановимся на наиболее распространённом тогдашнем аппарате — модели 500 C/D производства Western Electric, используемой компаниями, аффилированными с Bell System. Это стандартный настольный телефон с современными скруглёнными формами, как правило, с трубкой G1 или G3. Он был разработан около 1950 года и

пришёл на смену более старым аппаратам серии 300 с трубкой F1 и более острыми углами. Был и промежуточный вариант: старый корпус серии 300 в новом корпусе, по виду напоминающем 500-ю серию, но с прямой задней стенкой — она шла строго вертикально сразу за гнездом трубки, тогда как у настоящей 500-й серии сзади есть характерный выступ за гнездом.

Если вы до сих пор не уверены, какой телефон у вас: регулятор громкости звонка у 500-й серии выполнен в виде колёсика, у 300-й — в виде рычага. В глухой провинции вам, возможно, попадётся аппарат серии 200 (иногда называемый «ovalbase») или даже настольный «подсвечник» с микрофоном наверху и наушником, свисающим с бокового крюка.

Ни в одном из этих аппаратов нет встроенного звонка, так что, скорее всего, у вас есть отдельная коробка звонка на стене. Если у вашего телефона есть рукоятка сбоку, которую нужно крутить для вызова оператора — нижеследующее к нему не относится.

Звонковая цепь

Рассмотрим звонковую цепь, состоящую из двухкатушечного звонка и конденсатора ёмкостью 0,5 мкФ. В аппаратах Western Electric конденсатор расположен внутри сетевого блока, на котором также имеется большое количество винтовых зажимов — точек подключения практически для всего внутри телефона. Мне так и не удалось выяснить, почему у звонка две катушки с неодинаковым сопротивлением, но, по всей видимости, это как-то связано с определением того, кто из абонентов общей линии осуществляет тот или иной вызов.

В большинстве телефонов жёлтый и зелёный провода соединены вместе на настенном клеммном блоке, так что звонок подключён непосредственно поперёк телефонной линии; отключив жёлтый провод, можно отключить звонок (хотя иногда соединение выполнено внутренне — чёрный провод звонка подключён напрямую к клемме L1, и тогда жёлтый провод не задействован).

Провода «tip», «ring» и «yellow»: назначение

Возникает вопрос: зачем вообще нужен жёлтый провод, если используются только два? Действительно, в дом снаружи приходят лишь два провода — tip и ring. На индивидуальной линии (не общей) вызывной ток и все речевые напряжения подаются между tip и ring, и для дискового телефона в принципе безразлично, какой из проводов телефона соединяется с tip, а какой — с ring. Для тонального набора полярность важна: чтобы транзисторная схема диска работала правильно, зелёный провод должен идти к tip, а красный — к ring.

Жёлтый провод обычно используется для общих линий (party line). На двухабонентской линии вызывной ток от ЦС подаётся не между двумя проводами, а между одним проводом и землёй. В таком случае жёлтый провод идёт к земле, а другой конец звонка (красный провод) подключается либо к tip, либо к ring — в зависимости от абонента. Это позволяет одновременно звонить только одному из абонентов общей линии.

Варисторы и переключатели

Остальные элементы внутри телефона — варисторы. Телефонные компании, по всей видимости, являются крупнейшими потребителями этих устройств: варисторы — переменные резисторы, сопротивление которых падает с ростом приложенного напряжения. В телефонном аппарате они служат для шунтирования части схемы при чрезмерно высоком напряжении.

Рычажный переключатель (hook switch) имеет три группы контактов: два нормально разомкнутых (разомкнутых при положенной трубке), которые замыкают цепь постоянного тока при снятии трубки, и один нормально замкнутый контакт, подключённый напрямую параллельно наушнику. Функция этого контакта — шунтировать наушник в момент размыкания или замыкания цепи постоянного тока, предотвращая неприятный громкий щелчок в наушнике.

У диска два контакта. Первый — импульсный, нормально замкнутый, размыкающийся только в процессе набора на обратном ходу диска после того, как вы его отпустили. Второй контакт (контакт «вне нормы») шунтирует наушник сразу же при начале вращения диска и снимает шунт лишь после возврата диска в исходное положение. Тем самым вы не слышите щелчков диска при наборе.

Гибридная схема (hybrid network)

Наконец, в телефоне имеется гибридная схема — четырёхобмоточный трансформатор с набором резисторов, конденсаторов и варисторов. Её основная функция — ослаблять ваш собственный голос, снижая его громкость в наушнике.

Простейший телефон можно собрать из одной последовательной цепи: диск, микрофон, наушник. Но сигналы от собеседника значительно слабее ваших собственных: наушник, достаточно чувствительный для чёткого и громкого воспроизведения голоса другого человека, оглушил бы вас звуком вашего же голоса. Задача гибридной схемы — частично подавлять сигнал местного микрофона, пропуская при этом весь принятый сигнал на наушник. Этот принцип аналогичен применению гибридного телефонного патча с VOX-схемой, когда требуется направить голос телефонного собеседника на передатчик, но не пропустить сигнал приёмника на тот же передатчик.

Помимо элементов гибридной схемы, сетевой блок содержит ряд дополнительных компонентов (например, RC-цепь, подключённую параллельно импульсным контактам диска) и служит единым узлом подключения всего телефона.

Тональный набор (Touchtone)

Тональный телефон аналогичен дисковому, за исключением того, что дисковый механизм заменён тональной клавиатурой. Помимо транзисторного генератора тонов, стандартная тональная клавиатура имеет аналогичные контакты отключения наушника — с той разницей, что вместо полного шунтирования, как у дискового телефона, она включает резистор, лишь частично заглушающий аппарат.

Частоты тонального набора (DTMF) достаточно широко известны, но повторить их не лишне. Каждая цифра образована одной частотой из низкой группы и одной из высокой. Например, цифра «6» формируется одновременной подачей низкого тона 770 Гц и высокого тона 1477 Гц. Американские тональные клавиатуры генерируют оба тона на одном транзисторе, тогда как европейские (да, они тоже существуют) используют два транзистора — по одному на каждый тон.

В дополнение к трём стандартным высоким тонам принят четвёртый — 1633 Гц, дающий ещё четыре комбинации. В тот период он ещё не использовался, хотя стандартную тональную клавиатуру легко модифицировать для его генерации: необходимый отвод на индуктивности уже предусмотрен — нужен лишь дополнительный контакт переключателя.

Мало кто знает, что Военно-воздушные силы США использовали другой набор тональных частот — в диапазоне от 1020 до 1980 Гц. Поскольку многие телефонные аппараты, поступавшие в продажу, происходили с излишков Министерства обороны, можно ожидать, что подобные аппараты со временем появятся в свободном обращении.

Ещё одна тональная клавиатура, применявшаяся радиолюбителями, собрана из тонкой эластомерной переключательной панели производства Chomerics Corporation (77 Dragon Court, Woburn, Mass. 01801) и гибридной интегральной схемы на толстой плёнке производства Microsystems International (800 Dorchester Boulevard, Montreal, Quebec). Панель — Chomerics ER-20071, размером около 57×76 мм и толщиной около 5 мм (Chomerics также выпускает меньшую модель ER21289, но она крайне неудобна в использовании и, по имеющимся сведениям, ненадёжна). Microsystems International выпускает несколько схожих ИС серии ME8900, различающихся потреблением мощности и уровнем выходного сигнала. Некоторые из них содержат защитные диоды на случай неправильной полярности. Ввиду большого числа моделей перед заказом рекомендуется запросить технические данные у производителя. Среди американских дистрибьюторов — Newark Electronics, Milgray и Arrow Electronics (Нью-Йорк).

Одна из проблем любого ИС-генератора — зависимость частоты от воздействия радиочастотных помех. Многие радиолюбители испытывают трудности с установкой таких плат на двухметровые портативные радиостанции. Решение, кажется, наметилось: компания Mostek разрабатывает ИС-генератор тонов DTMF с дешёвым внешним кварцем 3,58 МГц в качестве опорного генератора, с последующим делением этой частоты триггерами для получения нужных тонов. Такой подход обещает быть более устойчивым к радиопомехам и дешевле в производстве — без необходимости дорогостоящей лазерной подстройки компонентов, как в ИС Microsystems International.

Декодирование тонального набора на ЦС

На другом конце телефонной цепи — в ЦС — различные схемы декодируют набранную цифру в сигналы, необходимые для выполнения коммутации. В дисковых системах декодирование осуществляется релейными схемами — шаговыми искателями. Эти схемы рассчитаны на набор со скоростью 10 импульсов в секунду при скважности примерно 60% разомкнуто / 40% замкнуто. Минимальная пауза между цифрами — около 600 мс, хотя несколько большая пауза безопаснее, поскольку снижает вероятность ошибок.

На практике многие ЦС принимают набор со значительно меньшей или большей скоростью, и нередко встречаются диски, ускоренные заменой механического регулятора на работающий примерно вдвое быстрее — всё зависит от типа оборудования ЦС.

Декодирование тональных сигналов обычно выполняется фильтровыми схемами, выделяющими тоны с помощью полосовых фильтров и управляющими реле через транзисторные схемы. Широко распространённый декодер 247B предназначен для небольших дисковых коммутаторных систем, устанавливаемых в помещениях предприятий для внутренней связи между добавочными номерами. В его состав входят: ограничительный усилитель, семь фильтров с драйверами реле (по одному на каждый из семи стандартных тонов) и схемы синхронизации и контроля. Каждое из семи реле имеет несколько контактов, которые соединяются в различных последовательно-параллельных комбинациях для обеспечения заземления одного из десяти

выходных контактов при получении соответствующей цифры. Стандартный 247B не распознаёт символы «*» и «#», однако при наличии принципиальной схемы его несложно модифицировать.

Декодер 247B не обладает высокой избирательностью и легко может срабатывать от голоса, если к его выходу не подключены дополнительные схемы задержки, требующие удержания контакта реле не менее заданного минимального времени. Несколько более сложные декодеры со встроенными задержками — приёмники тонального набора типов A3 и C. Оба используются в автоматических коммутаторах, принадлежащих клиентам, когда внешний абонент (через телефонную сеть общего пользования) хочет напрямую дозвониться до конкретного добавочного номера.

Приёмник типа C схож с 247B: он также имеет десять выходов — по одному на каждую цифру. Приёмник типа A3 выходных реле не имеет, вместо этого у него семь выходов напряжения — по одному на каждый из семи основных тонов — для управления внешними реле на 48 вольт. Блок A3 идеально подходит для управления кодером DTMF, который затем можно использовать для регенерации тональных цифр при зашумлённом исходном сигнале. Это может быть весьма полезно в репитерном автопатче для очистки тональных сигналов перед их подачей в телефонную сеть.

Помимо перечисленных, существуют и другие типы декодеров, специально разработанных для ЦС, однако информация о них практически недоступна. Декодер DTMF несложно собрать и самостоятельно. Хотя все стандартные декодеры телефонных компаний построены на фильтровых схемах, значительно проще (пусть и, возможно, менее надёжно) применить ИС с фазовой автоподстройкой частоты NE567.

Преимущества тонального набора

Любопытная особенность тонального набора в том, что он существенно ускоряет процесс соединения. С тональной клавиатурой можно набрать номер примерно в 3–5 раз быстрее, чем дисковым методом. Поскольку оборудование ЦС, принимающее и декодирующее номер, занято вашей линией лишь в течение набора, оно может быть переключено на следующий вызов раньше и, следовательно, обслуживает больше звонков. По сути, вся система тонального набора была изобретена ради оптимизации работы ЦС и сокращения необходимого оборудования. Знаменательно, что с клиентов берут дополнительную плату за услугу, которая не только не стоит телефонной компании ничего, но ещё и экономит ей деньги.

Частные телефонные аппараты и дело Carterfone

Ещё одна практика, которая может или не может стоить компании денег, — подключение частных добавочных телефонов. Их можно встретить в продаже по почте и в розничных магазинах. Телефонные компании утверждают, что подключение таких аппаратов к их линиям наносит им убытки и может повредить оборудование. Есть и противоположная точка зрения: доступность добавочных телефонов лишь способствует росту числа звонков ввиду удобства, и компании в действительности только выигрывают. Вопрос о вреде оборудованию тоже не имеет однозначного ответа: большинство добавочных аппаратов полностью совместимы с сетью, а нередко представляют собой ту же самую модель, что и сами телефонные компании.

До решения FCC по делу Carterfone о праве подключения к телефонным сетям сторонних устройств в 1968 году все телефонные компании заявляли, что подключение любого оборудования

к их линиям незаконно. Это было некоторым преувеличением: никаких конкретных законов против этого не существовало. Вместо этого каждая местная телефонная компания была обязана подать тариф в комиссию по общественным службам штата, и одним из условий этого тарифа был запрет на подключение какого-либо внешнего оборудования. Утверждая тариф, комиссия придавала запрету неявный квазиправовой статус.

Однако в деле Carterfone FCC постановила, что подключение внешнего оборудования должно быть разрешено. Телефонные компании скорректировали формулировки своих тарифов: подключение внешнего оборудования отныне допускалось при условии использования специального согласующего устройства, предоставляемого телефонной компанией для защиты её оборудования от повреждений. Хотя это решение было оспорено в нескольких штатах, таково, по всей видимости, нынешнее положение дел. Примечательно, что одни телефонные компании разрешают подключение клиентского оборудования без каких-либо трудностей, тогда как другие создают клиентам всевозможные препятствия.

Прогресс сетевых технологий

Автор: Dedicated Link

Январь 1989 года

Данный материал представляет общий обзор того, как сети эволюционировали от телефонных линий до линий T1.

Существует множество причин для совместного использования сетевой инфраструктуры. Концепция сетевого взаимодействия состоит в оптимизации всех аспектов передачи голоса и данных, а также в максимальном использовании пропускной способности линий связи.

Не так давно компании пользовались коммутационными мощностями AT&T для всех местных звонков. Это означало применение Centrex — системы, при которой местные звонки коммутировались силами AT&T (что обходилось значительно дороже, чем собственная коммутация). Затем крупные организации начали устанавливать АТС (PBX, Private Branch Exchange), позволяющие коммутировать местные звонки (5-й класс ESS) без участия AT&T. Использование PBX (или компьютеризированной офисной АТС — CBX, Computerized Branch Exchange) оказывается гораздо эффективнее при высокой нагрузке телефонного трафика. Это и стало отправной точкой в развитии локальных вычислительных сетей (LAN). Как только организация обзаводилась собственной LAN, она могла сдавать в аренду свободную пропускную способность другим компаниям — ведь платить за неё приходилось в любом случае. Ещё один способ обойтись без услуг AT&T — использовать линию иностранного обмена (FX, foreign exchange): это выделенная долгосрочная линия точка-точка на дальних расстояниях, оплачиваемая по фиксированному тарифу. Линию FX можно приобрести у AT&T или у многих других поставщиков. Такие частные линии (PL, private lines) используются как для голосовой, так и для передачи данных. При этом к качеству канала передачи данных предъявляются более высокие требования, чем к голосовому: любой незначительный сбой может привести к серьёзным и дорогостоящим ошибкам в обрабатываемых данных.

Одним из наиболее эффективных способов передачи данных является линия T1, обеспечивающая скорость 1,544 Мбит/с. Для передачи данных применяются микроволновые, спутниковые и волоконно-оптические системы. Все эти технологии уплотняют несколько каналов в один, увеличивая общую пропускную способность. Уплотнённая линия содержит 24 канала, которые могут быть разделены в соответствии с требованиями каждой конкретной передачи (например, простая голосовая передача с полосой около 300–3000 Гц занимает лишь небольшую долю уплотнённой линии). Существует два вида мультиплексирования: временное разделение каналов (TDM) и частотное разделение каналов (FDM). Мультиплексирование с временным разделением делит каналы на отдельные временные слоты. Мультиплексирование с частотным разделением разграничивает каналы посредством различных полос пропускания. Как правило, данные передаются через цифровые системы, а не через аналоговые, — и всё современное оборудование сегодня является цифровым.

При обмене данными между компьютерами необходим стандартный протокол взаимодействия внутри сети. Протокол — это набор правил, которым должен соответствовать удалённый компьютер, чтобы подключиться к данному узлу. Стандартным способом такого взаимодействия служит ASCII (American Standard Code for Interface Interexchange — американский стандартный код для межсистемного обмена). Помимо этого, используются коды шифрования, применяемые в целях безопасности. Ключи шифрования могут меняться ежечасно, ежедневно, еженедельно или ежемесячно — в зависимости от требуемого уровня защиты.

Передаваемая информация организуется методом пакетной коммутации. Наиболее распространённой разновидностью пакетной коммутации является X.25 — интерфейс, рекомендованный CCITT (Comité Consultatif International Téléphonique et Télégraphique) для соединения оконечного оборудования данных (DTE, Data Terminal Equipment) с оборудованием завершения канала данных (DCE, Data Circuit-terminating Equipment).

В такой сети принципиально важно наличие программного обеспечения, реализующего автоматический выбор маршрута (ARS, Automatic Route Selection). В процесс передачи должен быть встроен ARS, обеспечивающий выбор пути с наименьшей стоимостью. Задача системного аналитика или оператора — назначить корректную стоимость каждого пути, по которому может пройти передача, чтобы пакет следовал по маршруту с наименьшей стоимостью (LCR, Least Cost Route).

Пакет проходит путь от источника до конечного получателя. Системный аналитик или оператор обязан точно знать длину основного маршрута, длину первого альтернативного маршрута и длину второго альтернативного маршрута. Длина маршрута измеряется в хопах (скачках), соответствующих числу каналов между центральными узлами. Системный администратор должен установить максимально допустимое число хопов, которое маршрут не вправе превышать. Это и есть реальная стоимость канала, назначаемая для каждого возможного пути. Знание стоимостей каналов необходимо системному администратору для эффективного программирования ARS.

Вышеизложенное представляет лишь некоторые из основ, лежащих в основе передачи информации по сети. Надеюсь, это оказалось полезным!

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 XXIV/Part 1            PWN
PWN                                             PWN
PWN                February 25, 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

Снова и снова

Приветствую всех! Этот выпуск Phrack Inc. ознаменовал завершение плана, задуманного мной чуть более года назад, — «Проект Феникс». Нет, речь идёт не о BBS, которую ведёт The Mentor (хотя название борды и взято из этого плана), а о моей схеме возрождения хакерского сообщества из пепла «Кризиса 1987 года». Мой план состоял из нескольких частей, которым предстояло сойтись воедино.

• Объявить о плане и поднять вокруг него максимальную волну, чтобы разжечь энтузиазм.
• Провести SummerCon '88 в Сент-Луисе, штат Миссури, чтобы свести сегодняшних хакеров лицом к лицу.
• Восстановить контроль над Phrack Inc. и поставить его обратно на ноги.
• Выпустить трилогию Vicious Circle, чтобы обнажить и преодолеть наши проблемы безопасности.
• Провести сегодняшних хакеров в новое тысячелетие через The Future Transcendent Saga (которая помогает объединить хакеров прошлого с настоящим).

И вот теперь...

Объявляем 3-й ежегодный...

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

Дата предварительная, но я полагаю, что она не изменится. За дополнительной информацией обращайтесь к Taran King или Knight Lightning.

Из лёгких новостей: этот выпуск Phrack World News содержит статьи о Shadow Hawk, The Disk Jockey, Compaq, «суперсистеме» баз данных ФБР, австралийско-американском хакерском кольце, Computer Emergency Response Team, StarLink, Xenix Project, The Lost City of Atlantis, BBS The Beehive и многом другом. Читайте и наслаждайтесь.

По любым вопросам, комментариям, статьям для публикации и прочему со мной можно связаться по адресу C483307@UMCVMB.MISSOURI.EDU или C483307@UMCVMB.BITNET, либо на любой BBS, где вам удастся меня найти.

:Knight Lightning

Экспертиза по взрывчатке обнаружена в компьютере — 5 января 1989 г.

Мэтт Ньюфелд (The Washington Times)

Один из четырёх подростков из Бетесды, погибших в результате взрыва в гараже дома атташе посольства Бразилии на прошлых выходных, имел доступ к инструкциям по изготовлению бомб и взрывчатых веществ на одном из местных компьютерных ресурсов — об этом рассказал участник этой системы.

«Он был очень увлечён компьютерами», — сказал оператор об 18-летнем Дове Фишмане, одном из погибших подростков. «Дов ходил к моему другу домой», где они обсуждали различные виды программного обеспечения и компьютерных систем, добавил он.

В разветвлённой сети из примерно 200 частных BBS есть борда под названием «The Lost City of Atlantis», содержащая файлы со следующими именами: «Pipe Bombs», «Gas Tank Bombs», «Make Smoke Bombs», «Soda Bombs», «Explosive Info», «Kitchen Improvised Plastic Explosives» и «Plastic Explosives» — согласно файлам системы, просмотренным The Washington Times накануне.

Файлы Atlantis и других бордов этой сети заполнены сведениями о мелком хулиганстве и различных противоправных действиях. Борда Atlantis значится под заголовком «The Rules of Anarchy».

Файлы на Atlantis — которая функционирует локально, но теоретически доступна владельцам компьютеров по всей стране — содержат информацию и переписку о том, как приобрести различные химические вещества и взрывчатку для изготовления бомб. В других файлах объясняется, как из этих материалов собирать бомбы.

«Некоторые или все из вас, читающих это, возможно, слышали по слухам, что я продаю лабораторные материалы и/или химические вещества», — так начинается одно из сообщений некоего участника системы, действующего под псевдонимом «The Pyromaniac».

«Я могу достать вам почти любое вещество, которое вы захотите или которое вам потребуется», — говорится в том же сообщении далее. «Помните всегда: я гибок; вашим родителям не обязательно знать о химикатах».

Фишман и другие подростки были описаны друзьями и родственниками как высокоинтеллектуальные, трудолюбивые отличники. Они погибли около 3:15 утра в субботу в результате взрыва в доме атташе Веры Мачадо на Верн-стрит, квартал 6200. Расследование полиции округа Монтгомери установило, что причиной стал несчастный случай, вызванный тем, что юноши «экспериментировали с каким-то взрывчатым веществом».

В доме Фишмана были обнаружены нитраты, пероксиды и карбонаты, а также литература об «источниках химических веществ, устройств и рецептов, используемых при изготовлении взрывных устройств», — сообщил представитель пожарного маршала Майк Холл. «Точный характер источников и рецептов следственным отделом не разглашается, поскольку расследование продолжается».

«Мне ничего не известно о том, что использовалась информация из каких-либо компьютерных систем», однако эта возможность будет проверена, заявил г-н Холл. Отец Фишмана, Джоэл, накануне сказал, что его сын и трое других подростков были увлечены компьютерами. Однако, по его словам, он не знал ни о какой связи между компьютерами и взрывом. Дальнейшие вопросы он переадресовал полиции.

Оператор местной компьютерной системы сообщил, что большинству пользователей от 15 до 19 лет. Тем не менее, по его словам, пользователи системы нередко просматривают файлы, не ставя родителей в известность об их содержимом.

Борды и файлы сами по себе законны, а информация о взрывчатых веществах сосредоточена преимущественно на «частных» BBS, созданных лицами, известными как «системные операторы».

Тем не менее любой обладатель домашнего компьютера, телефона и модема может подключиться к этим бордам, получив одобрение конкретных операторов, пояснил оператор.

«Я считаю, что это должно быть разрешено, но не для кого попало из детей», — сказал оператор, являющийся взрослым. По его мнению, «это реально вина родителей», что они не следят за тем, к каким компьютерным ресурсам имеют доступ их дети.

Ещё одна борда в этой сети — «Warp Speed» — также предоставляет сведения о взрывчатке. По словам оператора, эта борда была закрыта между 30 декабря 1988 года и 1 января 1989 года. Она являлась «хостом» для «Damage, Inc.» — «группы людей, сосредоточенных на взрывчатых веществах, способах вредить людям, разрушении», сказал он.

На борде «The Beehive» появляется следующее сообщение от «Mister Fusion»:

```
"low cost explosives are no problem.  make them yourself.  what do
 you want rdx?  detonators, low explosives?  high explosives?  i can
 tell you what to do for some, but I would reccomend (sic) cia black
 books 1-3."
```

Другие борды и файлы в системе содержат информацию о компьютерном хакинге, конструировании устройств для глушения полицейских радаров, вскрытии замков и «фрикинге» — компьютерном жаргоне, обозначающем использование компьютеров для бесплатных телефонных звонков.

Среди этих файлов: «Making LSD», «Listing of common household chemicals», «Info on Barbiturates», «Make a mini-flame thrower», «How to make a land mine», «How to Hot Wire a car», «Home Defense: part II, guns or friends», «How to have fun with someone else's car», «Fun! with Random Senseless Violence», «Picking up little girls» и «How to break into a house».

«В хакерском мире много неверной информации — в частности, о способах победить телефонную компанию», — сказал оператор, занимающийся компьютерами не менее шести лет. «Но информация о взрывчатке в целом достоверна».

В двухстраничном файле «High Explosives» содержатся подробные инструкции по использованию химических веществ — какодила, тетрила и гремучей ртути.

«Эта штука потрясающая», — начинается раздел о какодиле. «Он воспламеняется на воздухе. К тому же выделяет облако густого белого дыма. Этот дым — не что иное, как мышьяк».

В конце файла всё же приводится предупреждение: «Не пытайтесь изготавливать эти вещи, если у вас нет опыта работы с химическими веществами. При ненадлежащем обращении они могут быть очень опасны».

Файл «Kitchen Improvised Plastic Explosives», обучающий пользователей «как сделать пластит из хлорного отбеливателя» и приписываемый некоему Тиму Льюису, предупреждает об опасности химикатов.

Computer Emergency Response Team (CERT) — 23 января 1989 г.

Извлечено из UNIX Today

ВАШИНГТОН. Недавно созданная федеральным правительством группа Computer Emergency Response Team (CERT) рассчитывает привлечь 100 технических экспертов для борьбы с компьютерными вирусами.

CERT, сформированная в прошлом месяце по инициативе Агентства перспективных исследовательских проектов Министерства обороны (DARPA), намерена завербовать добровольцев из федеральных, военных и гражданских ведомств в качестве консультантов для пользователей, столкнувшихся с возможным вторжением в сеть.

DARPA рассчитывает привлечь специалистов из Национального института стандартов и технологий, Агентства национальной безопасности, Института программной инженерии, других финансируемых правительством университетских лабораторий и даже ФБР.

Постоянная группа экспертов по безопасности UNIX придёт на смену специально созданной рабочей группе, которую Пентагон собрал в ноябре прошлого года для борьбы с заражением систем UNIX, предположительно вызванным Робертом Моррисом-младшим, — сообщил правительственный представитель.

Устав CERT также предусматривает информационно-просветительскую программу для обучения пользователей мерам по предотвращению уязвимостей — по словам пресс-секретаря CERT Сьюзан Данкал. Ожидается, что группа подготовит контрольный список «аудита безопасности», которым пользователи смогут руководствоваться при оценке своей уязвимости в сети. Кроме того, группа сосредоточится на устранении существующих уязвимостей в действующем программном обеспечении UNIX.

Для связи с CERT звоните в Институт программной инженерии при Университете Карнеги — Меллон в Питтсбурге: (412) 268-7090; либо используйте адрес электронной почты в сети Arpanet: cert@sei.cmu.edu.

Xenix Project, он же Phoenix Project Phase II — январь 1989 г.

В любимой BBS каждого ожидаются большие перемены.

25 января 1989 года The Mentor стал счастливым обладателем полного дистрибутива SCO Xenix вместе с пакетом разработчика и текстовыми утилитами (вложение в 1200 долларов, но оно того стоит). Он договорился о подключении к UUCP-почте и новостной ленте USENET и работает над запуском на нём программного обеспечения для BBS.

Что это означает для вас? Как я неоднократно показывал на протяжении всей The Future Transcendent Saga и ряда других файлов и площадок, будущее — за глобальными сетями. Так что теперь впервые The Mentor предлагает хакерам дешёвый, *ЛЕГАЛЬНЫЙ* способ получить доступ к гигабайтам информации, доступной через USENET. Почту можно отправлять через шлюзы BITNET, MILNET, ARPANET и INTERNET пользователям по всему миру. Короче говоря, связанность пришла, и будущее становится всё ближе.

Первым делом The Mentor хочет раздобыть второй жёсткий диск. Без него Xenix Project сейчас никак не запустить. Его 40-мегабайтный диск имеет 20-мегабайтный раздел Xenix, из которых 17 мегабайт занимает файловая система /root/. На раздел MS-DOS отведено 12 мегабайт борды плюс все нужные ему программы (Pagemaker, Word, Microsoft C, Brief и т.д.). Для поддержки новостного фида (USENET сгенерировал 50 мегабайт трафика за последние 2 недели) потребуется диск *МИНИМУМ* на 60 мегабайт. Лучше — 100+ мегабайт. Как только будет получен жёсткий диск, система выйдет в онлайн как однолинейная UNIX-машина. Есть надежда, что достаточно быстро удастся собрать средства на вторую телефонную линию и модем. С этого момента система начнёт

развиваться.

Конечная цель The Mentor (в течение 6 месяцев) — иметь 4–6 линий на 300–2400 бод, доступных для дозвона в режиме охоты (hunt group), плюс линию на 19,2 Кбод для получения новостного фида USENET. Предполагаемые стартовые расходы на 5-линейную систему:

```
110 meg hard disk..................... $1000
4 2400 baud modems (I've got 1 already).. $ 525
Installation of 4 phone lines............ $ 450
MultiPort Serial Card.................... $ 300
SCO Xenix Software...................... $1200
                                         ~~~~~
                                         $3475
```

С финансированием возникли трудности. The Mentor уже вложил 1200 долларов в пакет Xenix (плюс первоначальная покупка компьютерной системы), а значит, до «лучшей хакерской системы в мире» ему не хватает ещё 2200 долларов. Он рассчитывает раздобыть средства двумя способами.

A) Пожертвования. Многие пользователи уже сообщили, что готовы прислать от 10 до 100 долларов. Как ни странно, люди, занимающиеся безопасностью на The Phoenix Project, проявили исключительную щедрость. Жертвовать *есть смысл*, поскольку это даёт определённые привилегии — об этом ниже.

B) Ежемесячная оплата. За использование UNIX-части системы будет взиматься от 5 до 12,50 долларов в месяц, однако сама BBS The Phoenix Project останется бесплатной! Вот как это работает:

> ***Уровень 1 — только BBS.*** *Все, кто хочет пользоваться только The Phoenix Project, будут звонить и входить под именем учётной записи «bbs». Их принудительно переведут в программу BBS, где они войдут как обычно. Для них это будет просто смена программного обеспечения с добавлением входного пароля «bbs».*
> ***Уровень 2 — личный аккаунт для почты и новостей.*** *За 5 долларов в месяц пользователь получит собственный приватный аккаунт с полным доступом к UUCP-почте и новостям USENET. Он сможет отправлять письма по всему миру и читать, а также публиковать сообщения в сотнях групп USENET. На этот раз — легально!*
> ***Уровень 3 — личная почта, новости, игры и чат.*** *Пользователь получит все привилегии уровня 2, доступ к играм вроде Rogue, Chase и Greed, а также доступ к многопользовательской системе чата, аналогичной той, что работает на Altos в Западной Германии, — для общения в реальном времени между хакерами в Штатах без необходимости иметь NUI для выхода на Datex-P. Стоимость — 10 долларов в месяц.*
> ***Уровень 4 — полный доступ к оболочке Bourne Shell.*** *Открывает доступ ко всей системе, включая компилятор C и текстовые утилиты, а также к онлайн-лазерному принтеру для печати курсовых работ, важных документов и всего прочего (пересылка по почте потребует небольшой доплаты). Доступ уровня 4 будет ограничен людьми, достаточно технически грамотными, чтобы знать, как пользоваться компиляторами UNIX и как ими не злоупотреблять. Полностью установлена система разработки Xenix Development System и Text Processing Utilities, включая онлайн-справочные страницы. Я буду помогать отлаживать и тестировать код при необходимости. Стоимость — 12,50 долларов в месяц.*

C) Зачем жертвовать? Всё просто: вы получаете скидку. Вот категории учредительного членства:

> ***Contributing (Участник): $20*** *— 6 месяцев доступа уровня 2, экономия $10 по сравнению с ежемесячной оплатой.*
> ***Supporting (Сторонник): $45*** *— 1 год доступа уровня 2 или 6 месяцев доступа уровня 3.*

> ***Sustaining (Попечитель): $75*** *— 1 год доступа уровня 3 или пожизненный доступ уровня 2.*
> ***Lifetime (Пожизненный): $100*** *— пожизненный доступ уровня 4. Взносы менее 20 долларов будут напрямую засчитаны в счёт доступа уровня 2 (например, пожертвование в 10 долларов даёт 2 месяца доступа уровня 2).*

Аппаратные взносы тоже приветствуются в обмен на доступ. Свяжитесь со мной, и мы договоримся.

Информация предоставлена The Mentor

Несколько слов от The Mentor

Друзья, я не пытаюсь на этом заработать. Мог бы — сам купил бы железо. The Phoenix Project всегда стремился предоставлять вам лучшую доступную информацию по хаку и фрикингу и продолжит делать это БЕСПЛАТНО.

Подчёркиваю: даже после перехода The Phoenix Project BBS останется доступна через логин без пароля, под которым может зайти любой. Деньги мне нужны лишь в том случае, если вы хотите войти в мир сетей *ЛЕГАЛЬНЫМ* способом.

Система будет расширяться по мере роста интереса к ней. Если платных пользователей окажется недостаточно для прокладки более одной линии — она и останется однолинейной. Думаю, достаточно много людей оценят преимущества UUCP и USENET и захотят выложить цену шестирack хорошего пива за доступ.

Попутно замечу для UNIX-хакеров: эта система также предоставит отличную площадку для отработки хакерских техник UNIX. В отличие от других систем, которые наказывают за взлом защиты, я буду вознаграждать тех, кто найдёт дыры в моей безопасности. Хотя это в основном касается пользователей уровня 4 (единственных, кто не ограничен в оболочке), за обнаружение лазеек в безопасности будет предоставляться от 3 до 6 месяцев бесплатного доступа. Так что если вы всегда хотели иметь неограниченную среду для изучения и совершенствования техник работы с UNIX — вот она!

Связаться со мной можно по следующим адресам:

```
The Phoenix Project: 512-441-3088
Shadowkeep II:       512-929-7002
Hacker's Den 88:     718-358-9209
```

Пожертвования отправлять по адресу:

```
Loyd
PO Box 8500-615
San Marcos, TX  78666
(все чеки выписывать на имя Loyd)
```

+++The Mentor+++

> *«The Future is Forever!»*

Взлом компьютеров — это преступление, и точка — 4 декабря 1988 г.

Эдвард А. Парриш-мл., бывший президент IEEE Computer Society

Изначально опубликовано в Los Angeles Times

За последние несколько лет было написано немало публикаций, прославляющих подвиги компьютерных хакеров. Вспомним, например, популярный фильм «Военные игры» о подростке, который с помощью домашнего компьютера сумел подключиться к военной компьютерной сети и поиграть с её сердцевиной. Игры вышли из-под контроля, когда он решил сыграть в «термоядерную войну». Подросток, изображённый с невинными намерениями, в итоге сыграл ключевую роль в решении проблемы и предотвращении реального ядерного обмена, выйдя из ситуации героем.

Реальный пример в начале ноября: так называемый компьютерный вирус (самовоспроизводящаяся программа, распространяющаяся через компьютерные сети и другие носители в виде розыгрыша или акта вандализма) едва не парализовал 6000 военных и академических компьютеров.

К сожалению, отчасти потому, что последствия подобных «розыгрышей» кажутся большинству людей далёкими, возникает соблазн воспринимать хакера как своеобразного народного героя — одинокого человека, который, вооружённый лишь собственной смекалкой, способен перехитрить систему. Реальному ущербу, который такие люди могут причинить, уделяется недостаточно внимания. Задумайтесь, каковы были бы последствия аналогичного «розыгрыша», направленного против нашей системы управления воздушным движением, регионального банка или больничной информационной системы. Инцидент, в котором электронный взломщик проник в несекретную компьютерную сеть Пентагона, изменив или уничтожив часть файлов, нанёс потенциально серьёзный ущерб.

Мы на самом деле не знаем всех последствий ноябрьского вирусного инцидента, остановившего множество компьютеров в сети Корнелл — Стэнфорд, однако авторитетные опубликованные оценки ущерба в человеко-часах и машинном времени исчисляются миллионами долларов. Подавляющее большинство профессиональных учёных и инженеров, проектирующих, разрабатывающих и использующих эти сложные сети, подавлено таким полным пренебрежением к этическим нормам и отказом от профессиональной честности.

По иронии судьбы, хакеры, по всей видимости, движимы той же потребностью в исследовании, в проверке технических пределов, которая движет компьютерными профессионалами: они разбирают задачи на части, вникают в их суть и затем преодолевают их. Однако, судя по всему, не все хакеры понимают разницу между проникновением в технические тайны собственного компьютера и проникновением в сеть компьютеров, принадлежащих другим людям. Именно в этом и заключается ключевое различие между компьютерным профессионалом и человеком, который просто много знает о компьютерах.

Очевидно, технический диплом сам по себе не является гарантией этичного поведения. И хакеры — не единственные, кто злоупотребляет силой, заключённой в их знаниях. Что же тогда можно сделать?

Во-первых, мы — широкая общественность — можем повысить собственную осознанность. В частности, когда кто-то вмешивается в чужие данные или программы, каким бы хитроумным ни был способ, нам всем необходимо признать, что подобный поступок как минимум безответственен, а весьма вероятно — уголовно наказуем. То, что правонарушитель не испытывает раскаяния или что вирус имел непредвиденные последствия, не меняет сути беззакония этого акта — по существу, речь идёт о незаконном проникновении. Утверждение о том, что этот акт принёс пользу, поскольку повлёк за собой усиление мер безопасности, столь же несостоятельно, как если бы аналогичный аргумент был выдвинут в защиту любого другого преступления. Если после квартирной кражи я установлю сигнализацию, это оправдывает вора? Конечно нет. Любой подобный поступок должен неукоснительно преследоваться по закону.

На другом фронте профессиональные общества, такие как IEEE Computer Society, могут принимать меры по исключению, временному отстранению или порицанию любого члена, признанного

виновным в таком поведении. Наконец, аккредитационные органы — в частности, Computing Sciences Accreditation Board и Accreditation Board for Engineering and Technology — должны более активно следовать своим стандартам, предусматривающим надлежащее освещение вопросов этики и профессионального поведения в учебных программах университетских факультетов computer science и компьютерной инженерии.

Мы давно вошли в информационный век — эпоху, когда компьютер не менее важен для здоровья, безопасности и выживания нашей нации, чем любой другой отдельно взятый ресурс. Общество должно настаивать на мерах по обеспечению компьютерной безопасности с той же степенью настойчивости, с какой оно требует безопасности других критически важных для жизни технологий.

Shadow Hawk приговорён к тюремному заключению — 17 февраля 1989 года

```
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 XXIV/Part 2                PWN
PWN                                                 PWN
PWN                February 25, 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
```

Автор: Knight Lightning

18-летний телефонный фрик из района Northside/Rogers Park в Чикаго, взломавший компьютеры вооружённых сил США и компании AT&T и похитивший 55 программ, был приговорён к девяти месяцам заключения во вторник, 14 февраля 1989 года, в Федеральном окружном суде Чикаго.

Герберт Зинн-младший, проживающий с родителями на Северной Артезианской авеню в Чикаго, был признан виновным в нарушении Закона о компьютерном мошенничестве и злоупотреблениях 1986 года судьёй Полом Э. Планкеттом. Помимо тюремного срока, Зинн должен выплатить штраф в размере 10 000 долларов и отбыть два с половиной года федерального испытательного срока после освобождения.

Прокурор США Антон Р. Валукас заявил: «Дело Зинна послужит наглядной демонстрацией того направления, которое мы намерены избрать в подобных делах в будущем. Наша цель — агрессивное преследование. Мы взялись за эту проблему несанкционированного проникновения в компьютерные системы — проблему, слишком широко распространённую, трудно раскрываемую и трудно преследуемую в судебном порядке...»

Зинн, бросивший среднюю школу Mather High School в Чикаго, совершил взломы в 16–17 лет, пользуясь домашним компьютером и модемом. Действуя под псевдонимом Shadow Hawk, Зинн взломал компьютер Bell Labs в Напервилле, штат Иллинойс; компьютер AT&T в Берлингтоне, штат Северная Каролина; и компьютер AT&T на авиабазе Роббинс, штат Джорджия. Секретных материалов получено не было, однако правительство считает «крайне секретными» программы, похищенные с компьютера, используемого НАТО и связанного с командованием ракетными силами США. Кроме того, Зинн незаконно получил доступ к компьютеру IBM в Рае, штат Нью-Йорк, а также к компьютерам Illinois Bell Telephone Company и Rochester Telephone Company в Рочестере, штат Нью-Йорк.

Помощник прокурора США Уильям Кук сообщил, что Зинн получил доступ к компьютерам AT&T/Illinois Bell через компьютерные доски объявлений, которые он охарактеризовал как «...высокотехнологичные уличные банды». На слушании дела в январе Зинн выступил в своё защиту, заявив, что брал программы ради самообразования, а не для продажи или передачи другим фрикам. Похищенное программное обеспечение включало весьма сложные программы, связанные с проектированием компьютеров и искусственным интеллектом. Также было похищено программное обеспечение, используемое компаниями BOC (Bell Operating Companies) для расчётов и учёта при международных телефонных переговорах.

Shadow Hawk — то есть Герберт Зинн-младший — оставался незамеченным на протяжении нескольких месяцев в 1986–87 годах, но его погубила неудержимая тяга к хвастовству. По всей

видимости, для фриков и хакеров совершенно естественно рассказывать другим о своих делах. На BBS, печально известной своими сообщениями на тему фрикинга и пиратства, Shadow Hawk публиковал пароли, телефонные номера и технические подробности лазеек, которые он создал в компьютерных системах, в том числе на машине Bell Labs в Напервилле.

Того, чего Shadow Hawk не понял, так это того, что сотрудники AT&T и Illinois Bell тоже любят пользоваться этой BBS и читать чужие сообщения. Представители служб безопасности IBT и AT&T стали регулярно читать комментарии Shadow Hawk, но долго не могли достоверно установить его личность. Shadow Hawk неоднократно хвастался, что «отключит публичную коммутируемую сеть AT&T». Это ещё больше подстегнуло AT&T в стремлении его найти. Когда Зинн наконец рассказал о лазейке, встроенной им в компьютер в Напервилле, AT&T решила устроить в ответ свою собственную ловушку — и уже через несколько дней он в неё угодил. Как только он вошёл в систему, проследить телефонный звонок не составило труда, и его источник обнаружился в подвале семейного дома Зиннов на Северной Артезианской улице в Чикаго, где молодой Герб был занят работой с модемом и компьютером.

Вместо того чтобы действовать немедленно, при возможно недостаточной доказательной базе для уверенного обвинительного приговора, все дали Гербу достаточно верёвки, чтобы повеситься самому. Более двух месяцев все звонки с его телефона тщательно фиксировались. Его противоправная деятельность на компьютерах по всей территории США отслеживалась и протоколировалась. Представители службы безопасности Sprint предоставили материалы своего расследования звонков в их сети. Наконец наступил «великий день»: агенты ФБР, представители служб безопасности AT&T/IBT и детективы Чикагской полиции провели обыск в доме Зиннов. В ходе обыска были конфискованы три компьютера, различные модемы и другая периферийная техника. Рейд в сентябре 1987 года грубо оборвал фрикинг-деятельность Зинна. Последовавшие газетные публикации обернулись унижением и позором для родителей Зинна — людей известных и уважаемых в районе Rogers Park. В момент ареста младшего Зинна его отец в разговоре с властями произнёс: «Такой хороший мальчик! И такой умный — в компьютерах!»

Всё закончилось в то вторничное утро в зале суда судьи Планкетта в Чикаго, когда судья огласил приговор: девять месяцев под стражей Генерального прокурора или его уполномоченного представителя с последующим двухлетним с половиной федеральным испытательным сроком и штрафом в 10 000 долларов. Вынося приговор, судья отметил: «...возможно, этот пример удержит других от несанкционированного проникновения в компьютерные системы». Согласившись с доводами обвинения о том, что Зинн был «просто взломщиком, электронным... членом высокотехнологичной уличной банды», Планкетт добавил, что надеется: Зинн извлечёт урок из этого столкновения с законом и направит свои незаурядные компьютерные способности в законное русло. Судья также призвал Зинна окончить среднюю школу и «стать полезным членом общества вместо того, кем вы являетесь сейчас, сэр...»

Поскольку Зинн согласился сотрудничать с правительством на суде и впредь по его требованию, сторона обвинения не выдвигала суду конкретных рекомендаций по мере наказания. Адвокат Зинна просил суд о снисхождении и назначении испытательного срока, однако судья Планкетт счёл, что определённый срок заключения уместен. Зинн мог бы находиться под стражей вплоть до достижения 21 года.

Его родители покинули зал суда в глубокой печали. Когда их попросили высказаться о сыне, они сказали, что предпочли бы воздержаться от комментариев.

Информация собрана из различных источников

Банк данных ФБР о преступлениях вызывает споры — 13 февраля 1989 года

Автор: Эвелин Ричардс (Washington Post)

«Предлагаемая ФБР компьютерная система учёта преступлений порождает вопросы о точности и неприкосновенности частной жизни — Доклад предупреждает о потенциальной угрозе банка данных для гражданских свобод»

В субботу, незадолго до Рождества, таможенные чиновники США в международном аэропорту Лос-Анджелеса зафиксировали «совпадение».

Проводя стандартную компьютерную проверку пассажиров, сошедших с рейса Trans World Airlines из Лондона, они обнаружили Ричарда Лоуренса Склара — беглеца, разыскиваемого за участие в мошенничестве с недвижимостью в Аризоне.

Согласно инструкциям, таможенники сверили все данные Склара с властями Аризоны — дата рождения, рост, вес, цвет глаз и волос совпадали с данными разыскиваемого.

Задержание Склара стало образцово-показательным примером эффективности компьютеризированной борьбы с преступностью. Власти, находящиеся за тысячи миль от места преступления, могут почти мгновенно опознать и задержать разыскиваемого человека.

Была лишь одна проблема: это был не тот человек. 58-летний пассажир — которого следующие два дня обыскивали донага, перегоняли из одной камеры предварительного заключения в другую и приковывали наручниками к членам банд и другим опасным преступникам — оказался профессором политической науки Калифорнийского университета в Лос-Анджелесе.

Трижды за последние двенадцать лет становившийся жертвой финансовых махинаций самозванца, Склар требует, чтобы ФБР, чей компьютер зафиксировал последнее «совпадение», исправило электронные записи. «Пока этот человек не пойман, меня, скорее всего, ждёт очередной ордер на арест», — заявил Склар.

Нигде преимущества и недостатки компьютеризации не проявляются так наглядно, как в ФБР, которое завершает шестилетнее исследование путей совершенствования своего Национального центра криминальной информации (NCIC) — обширной компьютерной сети, уже связывающей 64 000 правоохранительных органов с базами данных, содержащими 19 миллионов записей, связанных с преступной деятельностью.

Хотя высшие чиновники ФБР ещё не утвердили предложение, действующая версия позволила бы властям передавать более подробную информацию и пользоваться значительно расширенным массивом уголовных записей. Она позволила бы, например, хранить и передавать в электронном виде отпечатки пальцев, фотографии, татуировки и другие физические признаки, которые могли бы предотвратить ошибочный арест. Несмотря на неоднозначность предложения, чиновники ФБР рекомендовали включить в систему банк данных с именами подозреваемых, которые ещё не были привлечены к уголовной ответственности.

Между тем предлагаемая система уже вызвала гнев учёных-компьютерщиков и экспертов по защите частной жизни, которые предупреждают в своём докладе, что система несёт «потенциально серьёзную угрозу неприкосновенности частной жизни и гражданским свободам». Доклад, подготовленный для подкомитета Палаты представителей по гражданским и конституционным правам, также утверждает, что предлагаемая модернизация стоимостью 40 миллионов долларов не устранит проблему точности данных и не обеспечит защиту записей.

Во многом под влиянием подобной критики переработанный проект ФБР по новой системе, известный как план NCIC 2000, представляет собой лишь костяк возможностей, первоначально предложенных сотрудниками правоохранительных органов. Многие их идеи были урезаны по практическим соображениям или из соображений защиты частной жизни.

«Техническая осуществимость не должна автоматически означать допустимость политики», — сказал Марк Ротенберг, один из редакторов доклада и представитель в Вашингтоне организации Computer Professionals for Social Responsibility — калифорнийской организации. Необходимость соблюдать этот баланс — взвешивать преимущества технического прогресса против менее очевидных издержек — становится всё более насущной по мере того, как общенациональные компьютерные сети превращаются в кровеносную систему высокотехнологичного общества.

Для того чтобы технологии оставались под контролем, их пользователям необходимо регулярно проверять точность хранимых данных, а иногда прибегать к старомодным бумажным документам или личному контакту для подтверждения. Ошибки преследовали NCIC долгие годы, но масштабная работа по улучшению ведения записей значительно сократила число проблем, сообщило ФБР.

Действующая система ФБР, задействованная федеральными, штатными и местными органами, обрабатывает около 10 запросов в секунду от тех, кто разыскивает сведения о разыскиваемых лицах, угнанных транспортных средствах и имуществе, уголовных историях и многом другом. Пользуясь существующей системой, патрульный полицейский, остановивший автомобиль, может в течение нескольких секунд узнать, разыскивается ли водитель в каком-либо другом штате, а следователь, просматривающий список подозреваемых, — изучить их прошлые дела.

На определённом этапе предполагалось, что компьютер ФБР будущего будет связан с целым рядом других баз данных, включая кредитные истории, а также базы Службы иммиграции и натурализации, Налогового управления, Администрации социального обеспечения и Комиссии по ценным бумагам и биржам. Один за другим наблюдательные советы урезали эти планы.

«В этих базах данных хранится огромное количество конфиденциальной информации, — сказал лейтенант Стэнли Михалески, начальник отдела документации полиции округа Монтгомери [штат Мэриленд]. — Я не стану уверять вас, что полицейские не будут злоупотреблять этой информацией».

Наиболее спорной частью планируемой системы является существенное расширение в части сведений об уголовных подозреваемых — чья вина ещё не установлена.

Предлагаемая система включала бы сведения о лицах, находящихся под следствием по делам об убийстве, похищении людей или наркотиках. В неё был бы включён так называемый режим «тихого совпадения»: офицер в Техасе, к примеру, не знал бы, что задержанный им за превышение скорости является подозреваемым в убийстве в Вирджинии. Но когда следователи из Вирджинии наутро включат свой компьютер, он уведомит их об остановке в Техасе. Михалески расценил это предложение как «блестящую идею. Информация — вот в чём суть дела». Однако функция «слежки» вызвала возмущение критиков.

«Эта [база данных] может разрастись до угрозы самого разного рода — предполагаемые коммунисты, предполагаемые знакомые гомосексуалов. Этому нет конца, стоит только начать», — заявил конгрессмен Дон Эдвардс (демократ, Калифорния), чей подкомитет инициировал подготовку доклада о системе ФБР.

Начальник технического отдела ФБР Уильям Бэйс защищает предлагаемые файлы, утверждая, что они помогут задерживать преступников, содержа при этом лишь тщательно отобранные имена. «Логика такова: эти люди являются объектами расследований и соответствуют определённым критериям», — пояснил он.

Тема с файлом подозреваемых настолько болезненна, что директор ФБР Уильям Сэшнс, по имеющимся сведениям, может не включить её в свой публичный план по новой системе.

Схожий со случаем Склара был случай Терри Дина Рогана, арестованного пять раз из-за ордеров на арест, вызванных действиями самозванца. В итоге он получил 50 000 долларов в качестве компенсации ущерба.

Австралийские власти ужесточают меры против хакеров — 14 февраля 1989 года

Автор: Джули Пауэр (The Financial Review)

Ожидается, что сегодня федеральный кабинет министров одобрит законопроект, предусматривающий суровые санкции за взлом компьютерных систем Содружества. Предполагается, что генеральный прокурор Лайонел Боуэн предложит ряд жёстких новых законов, в целом соответствующих рекомендациям Министерства генерального прокурора, опубликованным в декабре. Боуэн в срочном порядке запросил этот доклад у Комиссии по пересмотру уголовного законодательства Содружества, которую возглавляет сэр Гарри Гиббс, в связи с растущей необходимостью защиты информации Содружества и обновления действующего законодательства.

Ещё одним поводом может служить необходимость защиты от несанкционированного доступа к налоговым номерам, которые будут храниться в ряде государственных баз данных.

Если рекомендации доклада будут одобрены, взлом компьютеров Содружества будет грозить штрафом в размере 48 000 долларов и десятью годами лишения свободы. Кроме того, уголовным преступлением станет уничтожение, стирание, изменение, вмешательство, создание препятствий и незаконное добавление или внесение данных в компьютерные системы Содружества.

Законодательство не распространяется на частные компьютерные системы. Однако Министерство генерального прокурора рекомендовало признать уголовным преступлением получение доступа к информации, хранящейся в частном компьютере, через средства связи Telecom или иное средство связи Содружества без надлежащих полномочий.

Кража информации на несколько миллиардов долларов — 8 февраля 1989 года

Автор: Боб Митчелл (Toronto Star) (отредактировано для данной публикации)

Мужчина арестован и обвинён в несанкционированном использовании компьютерной информации в результате двухмесячного полицейского расследования. Подозреваемый был сотрудником «очень крупной» торонтской компании: «Компании, которую все знают, с офисами по всей Канаде». Полиция держит название компании в тайне по её просьбе. По их словам, преступник действовал в одиночку.

Пароль, принадлежащий компании, был использован для кражи информации, которую компания оценивает в 4 миллиарда (канадских) долларов. В состав этой информации входят компьютерные файлы американской компании, предположительно содержащие данные многочисленных организаций и используемые крупными канадскими компаниями и правительством Соединённых Штатов.

«Мы не знаем, что этот человек собирался делать с этой информацией, но её потенциал не поддаётся описанию. Я не утверждаю, что у него были такие намерения, но программа содержала

информацию, которую можно было продать другим компаниям», — заявил Льюэрс.

Дальнейшее расследование приведённых выше сведений позволило установить следующее:

Оценка кражи информации на несколько миллиардов долларов опровергнута — 17 февраля 1989 года

Иная версия событий, связанных с кражей информации, была опубликована двумя днями позже.

Информация в данной статье взята из Toronto Globe & Mail. Заголовок материала гласит: «Кражу компьютерной информации обнаружила система безопасности самой компании». Статья начинается следующим образом:

> *«Кража информации из компьютерной программы компании была обнаружена собственной системой компьютерной безопасности фирмы.*
> *Майк Тиллсон, президент HCR Corporation, специализирующейся на разработке программного обеспечения, заявил вчера, что на прошлой неделе в системе компании был замечен нестандартный характер обращений к компьютеру».*

Далее в статье говорится, что данные полицейского доклада, оценивавшего «программу» в 4 миллиарда (канадских) долларов, были названы Тиллсоном грубым преувеличением: «Речь скорее идёт о десятках тысяч долларов». Он также пояснил, что незаконный доступ произошёл лишь неделю назад — никакого двухмесячного расследования не было. На вопрос о возможной перепродаже информации он ответил: «Неясно, как можно было бы на этом заработать. Причин может быть множество — вплоть до праздного любопытства. Не исключено, что никакого преступного умысла и не было».

Поскольку речь шла не о данных клиентов HCR, а Тиллсон отказался уточнить характер информации, в статье вскользь упоминается UNIX, туманно говорится об интеллектуальной собственности AT&T и отмечается, что AT&T «на данном этапе» не является участницей расследования.

Новые аресты в Сиракузах — 6 февраля 1989 года

St. Elmos Fire был арестован после того, как предполагаемый друг донёс на него в полицию и подписал аффидавит. В числе его преступлений — взлом школьного компьютера HP3000, а ФБР и Telenet пытаются привлечь его к ответственности за взлом ещё одного HP3000 в Иллинойсе.

Однако именно этот «друг» в действительности и был ответственен за ущерб, причинённый компьютеру в Иллинойсе. Проблема в том, что Telenet отследила звонки до Сиракуз, штат Нью-Йорк, и в связи со схожестью преступлений власти склонны считать, что оба были совершены одним и тем же лицом.

St. Elmos Fire уже прошёл предварительное слушание, и его адвокат утверждает, что доказательств, связывающих SEF с HP3000 в Сиракузах, крайне мало. Между тем относительно статуса расследования по системе в Иллинойсе на сегодняшний день ничего не известно.

Информация предоставлена Grey Wizard

Из San Jose Mercury News

ТАМПА, Флорида (AP) — Редактору телевизионных новостей, переманенному конкурирующей станцией, предъявлено обвинение в незаконном доступе к компьютерной системе своего прежнего работодателя с целью получения конфиденциальной информации о новостных материалах.

Используя знание системы для обхода защиты, которую он сам помогал создавать, Майкл Л. Шапиро просматривал и уничтожал файлы, связанные с новостными материалами тамповской станции WTVT, — такова суть обвинений, предъявленных во вторник.

Телефонные записи, изъятые при аресте Шапиро в Клируотере, показали, что в прошлом месяце он несколько раз звонил на компьютерную линию WTVT, где работал редактором информационных материалов вплоть до того, как в октябре перешёл на должность помощника редактора новостей к конкуренту — WTSP.

Шапиро, 33 года, предъявлено 14 пунктов обвинения в компьютерных преступлениях, объединённых в три категории уголовных преступлений второй степени тяжести: преступления против интеллектуальной собственности, преступления против компьютерного оборудования и преступления против пользователей компьютеров. Он был освобождён из-под стражи под честное слово.

В случае признания виновным ему грозит до 15 лет лишения свободы и штраф в 10 000 долларов по каждому из пунктов обвинения второй степени тяжести.

Боб Франклин, исполняющий обязанности директора новостного отдела WTVT, рассказал, что руководство станции обнаружило пропажу нескольких компьютерных файлов в прошлом месяце и обратилось к Шапиро за помощью. По словам Франклина, бывший сотрудник заявил, что не знает причин произошедшего.

На пресс-конференции Франклин заявил: «Последующее расследование показало, что как минимум с начала января компьютерная система редакции WTVT неоднократно подвергалась реальным и попытке "взломов". В компьютерах хранится строго конфиденциальная информация о текущих и будущих новостных материалах станции».

По словам директора новостной службы, Шапиро был одним из двух человек, отвечавших за ежедневную эксплуатацию и техническое обслуживание компьютерной системы после её установки около восьми месяцев назад. Второй по-прежнему работает на WTVT.

Терри Коул, директор новостной службы WTSP, сообщил, что Шапиро отстранён от работы. Шапиро не ответил на запросы о комментарии.

Франклин отметил, что Шапиро, проработавший на WTVT с февраля 1986 по сентябрь 1988 года, ушёл, чтобы продвинуться по карьерной лестнице. «Он очень хорошо делал свою работу, — сказал Франклин. — Он уходил по-хорошему».

Контракт Иуды исполнен — 24 января 1989 года

```
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 XXIV/Part 3            PWN
PWN                                             PWN
PWN                February 25, 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

> *«...ещё одно, что меня злило — я считал себя, по крайней мере раньше считал, человеком, который весьма осмотрителен в вопросах доверия. По сути, никто не имел моего домашнего номера, и лишь немногие вообще знали, где я на самом деле живу...»*
> *— The Disk Jockey*

Следующая история, рассказанная от лица The Disk Jockey, — наглядный пример опасностей, которые подстерегают в сообществе фрикеров и хакеров, когда доверяешь тем, кто заключил «контракт Иуды».

•----------

Позвольте вкратце объяснить, как меня поймали...

Хакер по имени Compaq был арестован после того, как кто-то сдал его за использование кодов Sprint. При исполнении ордера на обыск полиция штата обратила внимание на то, что у него находилось чрезмерное количество компьютерного оборудования, происхождение которого Compaq объяснить не смог.

Проверив сведения (полагаю, они проверили серийные номера, которые Compaq не стёр), полиция установила, что оборудование было получено незаконным путём. После этого Compaq заявил полиции, что именно я — Дуг Нельсон (именно так, по его мнению, звали меня) — привёз ему это оборудование. Что было правдой.

Тем временем Compaq общался со мной и уверял, что всё время молчит. Имейте в виду: я знал этого парня достаточно долго и считал, что знаю его хорошо. Я был уверен, что неплохо разбираюсь в людях.

Шло время, а я и не подозревал, что Compaq снова и снова встречается с полицией штата и Федеральным бюро расследований (ФБР), помогая установить мою личность. Он дал им подробное описание, правильно назвал школу, в которой я учился, — однако был УБЕЖДЁН, что моё имя Дуглас Нельсон. А поскольку мой телефон прежде был оформлен на это имя, он считал свою уверенность обоснованной. Полиция запросила Иллинойс, но ни номерных знаков, ни водительского удостоверения на это имя не нашла. Compaq помнил, что на моей машине были иллинойские номера.

Они зашли в тупик — пока Compaq не вспомнил кое-что важное. Однажды мы ходили с ним на ужин, и в разговоре я упомянул, что живу в Блумфилд-Хиллс, штат Мичиган.

После того как Compaq сообщил это полиции штата, они написали в Блумфилд-Хиллс: дали описание и попросили прислать любые фотографии из картотеки, соответствующие этому описанию.

Проблема в том, что несколько лет назад мы с приятелями были задержаны за катание на снегоходе одного из друзей в его отсутствие. Соседи нас не знали и вызвали полицию. Обвинения сняли, но наши отпечатки и фотографии остались в базе.

Блумфилд-Хиллс прислал обратно 12 фотографий, и — как следует из полицейского рапорта — «Кент Л. Гормат (Compaq) без колебаний опознал фотографию № 3 как человека, которого он знает под именем Дуглас Нельсон. Настоящее имя этого человека оказалось Дуглас...»

Ордер на мой арест был выдан и вскоре исполнен силами полиции штата, местной и федеральной властей в 1:47 ночи 27 июня 1988 года.

Какой у меня замечательный друг. За шесть месяцев, проведённых в тюрьме, родители, жившие в 400 милях от меня, не могли приехать на свидание; подруга могла навещать меня в лучшем случае раз в месяц — она тоже была далеко. А Compaq, живший всего в 10 милях, ни разу ко мне не пришёл. Это меня серьёзно разозлило: я решил, что этому «другу» есть о чём мне рассказать.

Как видите, я уже на свободе, однако буду под условным надзором вплоть до 15 декабря 1989 года.

— The Disk Jockey

Афера с поддельными бонусными авиамилями — 13 февраля 1989 года

По материалам Associated Press

Авиационный агент по продаже билетов набрал 1,7 миллиона бонусных авиамиль при помощи компьютера, не покидая земли, а затем продал эти баллы более чем за 20 000 долларов — сообщает пресса.

Ральф Квашни, 28 лет, был задержан в воскресенье, когда явился на работу в международный аэропорт Кеннеди; ему предъявили обвинения в компьютерном мошенничестве и крупном хищении, сообщили власти.

Квашни, агент авиакомпании Lufthansa, прежде работал в American Airlines. По данным полиции, он использовал свой код доступа для создания 18 фиктивных счетов в программе лояльности American Airlines Advantage — накрутив 1,7 миллиона бонусных миль, пишет газета.

Все 18 счетов — пять на имя Квашни и 13 на вымышленные имена — были привязаны к одному и тому же почтовому ящику, отмечает издание.

Вместо того чтобы обменивать бонусные мили на бесплатные перелёты, Квашни продал часть из них брокерам за 22 500 долларов. Те использовали баллы для приобретения нескольких билетов первого класса туда-обратно: из Нью-Йорка в Австралию, между Лондоном и Бермудскими островами, а также между Нью-Йорком и Парижем. Детектив Портовой администрации Чарльз Шмидт уточнил, что продажа личных бонусных миль брокерам является законной.

Квашни создавал счета на распространённые фамилии. Если пассажир с такой фамилией летел рейсом American и не имел счёта в Advantage, его имя удалялось из списка рейса и заменялось именем из фиктивных счетов.

«Пока самолёт отъезжал от выхода, этот парень в буквальном смысле стирал пассажиров», — сказал Шмидт.

Масштабная схема с поддельными банкоматными картами раскрыта — 11 февраля 1989 года

Дуглас Франтц, Los Angeles Times

Секретная служба США пресекла схему применения более 7 700 поддельных банкоматных карт для снятия наличных в Bank of America. После месячного расследования с участием информатора пятеро подозреваемых были арестованы и обвинены в нарушении федерального законодательства о мошенничестве.

«В ходе обыска были изъяты 1 884 готовые поддельные карты, 4 900 частично готовых карт и машина для кодирования карт данными счетов Bank of America, включая строго секретные персональные идентификационные номера клиентов».

Предполагаемым организатором схемы является Марк Кёниг — программист компании Applied Communications, Inc. (Омаха), дочернего предприятия US West. Он временно работал по контракту в дочерней структуре GTE Corporation, которая обслуживает 286 банкоматов в магазинах Калифорнии. Кёниг имел доступ к данным счетов по картам, использовавшимся в банкоматах GTE. Согласно записи телефонного разговора, Кёниг признался, что перенёс данные BofA на свой домашний компьютер. Он намеренно взял лишь информацию Bank of America — «чтобы это выглядело как утечка изнутри банка». Кодировочная машина была из его офиса.

Кёниг и сообщники планировали разъехаться по всей стране на шесть дней в период праздников Дня президентов и снять наличные. Они собирались надевать маскировку, поскольку некоторые банкоматы оснащены скрытыми камерами. Три «тестовые» карты были успешно использованы, однако в ходе проверок снималась лишь небольшая сумма, сообщила Секретная служба.

По оценке прокурора США, потери банка составили бы от 7 до 14 миллионов долларов. Bank of America разослал письма 7 000 клиентам с уведомлением о замене карт.

STARLINK — альтернатива PC Pursuit — 24 января 1989 года

STARLINK — альтернатива сервису PC Pursuit. В часы минимальной нагрузки (с 19:00 до 6:00 и в выходные) можно дозвониться в 91 город в 28 штатах по цене 1,50 доллара в час. Все подключения через сеть Tymnet осуществляются на скорости 2400 бит/с (работает и 1200 бит/с) без доплат; ограничений по максимальному времени нет.

Единовременный взнос за регистрацию составляет 50 долларов, ежемесячная плата за обслуживание счёта — 10 долларов. Пользователи с высокой нагрузкой могут выбрать тариф: 25 долларов в месяц плюс 1,00 доллар в час.

Сервис эксплуатируется компанией Galaxy Telecomm в Вирджиния-Бич, штат Вирджиния; подключиться можно по модему по номеру 804-495-INFO. После регистрации предоставляется 30 минут бесплатного доступа.

Это сервис Galaxy, а не TYMNET. Galaxy закупает большие блоки часов у TYMNET. Чтобы узнать местный номер доступа, позвоните в TYMNET по номеру (800) 336-0149 — круглосуточно. Не спрашивайте их о тарифах и прочем: они не в курсе. Обращайтесь в Galaxy.

Galaxy сообщает, что вскоре у них появится собственный номер 800 для регистрации и информации.

Ниже приведён список основных городов охвата. Есть и другие, до которых можно дозвониться с местной линии из перечисленных.

Восточный часовой пояс

Коннектикут: Блумфилд, Хартфорд, Стэмфорд
Флорида: Форт-Лодердейл, Джексонвилл, Лонгвуд, Майами, Орландо, Тампа
Джорджия: Атланта, Доравилл, Мариетта, Норкросс
Индиана: Индианаполис
Мэриленд: Балтимор
Массачусетс: Бостон, Кембридж
Нью-Джерси: Камден, Инглвуд-Клиффс, Ньюарк, Пеннсокен, Принстон, Саут-Брансуик
Нью-Йорк: Олбани, Баффало, Мелвилл, Нью-Йорк, Питсфорд, Рочестер, Уайт-Плейнс
Северная Каролина: Шарлотт
Огайо: Акрон, Цинциннати, Кливленд, Колумбус, Дейтон
Пенсильвания: Филадельфия, Питтсбург
Род-Айленд: Провиденс
Вирджиния: Александрия, Арлингтон, Фэрфакс, Мидлотиан, Норфолк, Портсмут

Центральный часовой пояс

Алабама: Бирмингем
Иллинойс: Чикаго, Глен-Эллин
Канзас: Уичита
Мичиган: Детройт
Миннесота: Миннеаполис, Сент-Пол
Миссури: Бриджтон, Индепенденс, Канзас-Сити, Сент-Луис
Небраска: Омаха
Оклахома: Оклахома-Сити, Талса
Теннесси: Мемфис, Нашвилл
Техас: Арлингтон, Даллас, Форт-Уэрт, Хьюстон
Висконсин: Брукфилд, Милуоки

Горный часовой пояс

Аризона: Меса, Финикс, Тусон
Колорадо: Аврора, Боулдер, Денвер

Тихоокеанский часовой пояс

Калифорния: Альгамбра, Анахейм, Эль-Сегундо, Лонг-Бич, Ньюпорт-Бич, Окленд, Пасадена, Плезантон, Сакраменто, Сан-Франциско, Сан-Хосе, Шерман-Оукс, Вернон, Уолнат-Крик
Вашингтон: Бельвью, Сиэтл

STARLINK — сервис подразделения Galaxy Telecomm Division, GTC, Inc., издателя BBS Telecomputing News, Galaxy Magazine и других электронных изданий.

Условные сроки за взлом компьютера — 20 февраля 1989 года

По материалам Personal Computing Weekly

«Сотрудники полиции осуждены за незаконное использование Национального полицейского компьютера»

Трое полицейских, нанятых частными детективами для взлома Национального полицейского компьютера, получили условные сроки лишения свободы в Винчестерском коронном суде. Частные детективы также получили условные сроки — от четырёх до шести месяцев.

Полицейским было предъявлено обвинение по Закону о государственной тайне в сговоре с целью получения конфиденциальной информации из Национального полицейского компьютера в Хендоне.

Один из полицейских признал свою вину; двое других и частные детективы заявили о невиновности.

Дело возникло из телевизионного шоу «Тайное общество», в котором частный детектив Стивен Бартлетт был снят на камеру: он рассказывал журналисту Дункану Кэмпбеллу, что имеет доступ к Национальному полицейскому компьютеру, Бюро уголовных записей в Скотленд-Ярде и DHSS (Министерству здравоохранения и социального обеспечения).

Бартлетт заявил, что может получить информацию практически о любом человеке за несколько часов. Доступ, по его словам, обеспечивался через определённых офицеров полиции в Бейзингстоке, Хэмпшир. Хотя расследование показало, что связь с Бейзингстоком оказалась ложной, след привёл к другим полицейским и частным детективам в иных местах.

Большинство полученных с компьютеров сведений использовалось для установления владельцев транспортных средств, проверки кредитной истории, а также для выяснения, где находился тот или иной человек в определённое время — в интересах тех, кто расследовал случаи супружеской неверности.

• -

Разумеется, действия, за которые офицеры и другие лица были осуждены, не являлись компьютерным взломом в строгом смысле — скорее это злоупотребление законным доступом.

Фиктивный вирус вызвал не меньше паники, чем настоящий — 20 февраля 1989 года

По материалам Popular Computing Weekly

«Вирус запущен и работает»

Майкл Бэнбрук изрядно напугал сетевых администраторов своего колледжа, подсадив сообщение о том, что в сети колледжа активен вирус.

Сообщение Бэнбрука появлялось всякий раз, когда пользователь вводил неверный пароль; обычная надпись

> *«Вы не авторизованный пользователь.»*

была заменена на краткую, но зловещую:

> *«Вирус запущен и работает.»*

Когда сообщение обнаружил сетевой администратор колледжа, Бэнброку немедленно запретили доступ к любым компьютерам колледжа Святого Франциска Ксавьера в Клэпхеме, Южный Лондон.

Бэнбрук, 17 лет, рассказал Popular Computing Weekly, что считает реакцию колледжа чрезмерной, а сам он, по существу, лишь обнажил слабость системы безопасности сети колледжа. В колледже установлена 64-узловая сеть RM Nimbus под управлением MS-DOS.

«Всё, что нужно сделать, — это изменить пятистрочный пакетный файл DOS», — говорит Бэнбрук. «Никакой защиты вообще нет».

Бэнбрук признаёт, что его мотивы были связаны с безопасностью лишь отчасти: «Мне просто было скучно, и я начал баловаться. Одни люди рисуют на блокноте, когда им нечего делать, — я рисую

на клавиатуре. Я никак не думал, что кто-то поверит этому сообщению».

Бэнбрук был отстранён от занятий по информатике и лишён права пользоваться компьютерами колледжа на неделю — до тех пор, пока не выяснилось, что никакого вируса нет. После встречи директора колледжа Брайана Скейлуна с родителями Бэнбрука всё, по имеющимся сведениям, «вернулось в норму».

Краткие новости Phrack World News

По вопросу разделения кода NPA 312/708: правильная дата разделения — 11 ноября 1989 года. Однако льготный период набора продолжится как минимум до 9 февраля 1990 года.

Всем, кто хочет знать, как выглядит Роберт Моррис-младший, стоит заглянуть на страницу 66 январского номера журнала Discover за 1989 год.
