Phrack RU issue 033

Русская версия Phrack, выпуск 033. Полный текст статей с кодом и таблицами.

Темы выпуска: сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: Введение в Phrack 33; Shooting Shark; Руководство хакера по Интернету; FEDIX — Информационный сервис онлайн; Справочный список LATA; Международные бесплатные звонки, звонки по местному тарифу и специальные платные услуги; Фрикинг в Германии; Учебник по TCP/IP: За кулисами интернета; Настоящая рабочая схема «Красной коробки»; Хакеры, пришедшие с холода; Phrack World News; Мировые новости Phrack; Пентагон открыт для хакеров!.

Введение в Phrack 33

Автор: Knight Lightning и Dispater

_____

P H R A C K 3 3

15 сентября 1991 года

_____

~Технологии для выживания~

24 декабря 1989 года Taran King и я выпустили тридцатый номер Phrack и приступили к подготовке к новому десятилетию. Будущее Phrack казалось светлым и полным огромного потенциала. Несколько недель спустя Phrack был закрыт Секретной службой США в рамках масштабной атаки на всемирно известную хакерскую группу Legion of Doom.

Легенда о Phrack умерла... или нет? Несколько месяцев спустя появился информационный бюллетень под названием Phrack, обозначенный как выпуск 31, под редакторством Doc Holiday. Разумеется, это был не тот оригинальный Doc Holiday из Теннесси, а один из основателей Comsec Data Security — Скотт Чазин. Он мог называть себя Phrack, но им не являлся.

17 ноября 1990 года была предпринята ещё одна попытка возродить Phrack. Crimson Death и Doc Holiday вернулись, чтобы попробовать снова, на этот раз назвав своё детище «Phrack Classic». Тот выпуск был не совсем ужасен, однако тон статей был выбран неверно. Само введение свидетельствовало об отсутствии ответственности и зрелости в момент, когда они были нужны более всего. Чтобы усугубить положение, Crimson Death так и не выпустил следующий номер Phrack Classic вплоть до 1 сентября 1991 года — почти десять месяцев спустя. Подобное отсутствие предсказуемости и преемственности стало слишком тяжёлым бременем для хакерского сообщества.

Я с гордостью объявляю, что тем самым началась новая эпоха Phrack. Новый Phrack пронумерован как выпуск 33, несмотря на существование сентябрьского выпуска Phrack Classic. Чтобы облегчить переход, новая редакция Phrack заимствовала файлы из PC 33, дабы хронология была выстроена корректно. Даже сам Crimson Death согласился, что настало время вновь передать эстафету.

Новым редактором Phrack стал Dispater; другие участники, работавшие над этим выпуском, — Ninja Master, Circuit и The Not. Само собой, они всегда рады помощи и хорошим статьям. Новый Phrack будет работать несколько иначе, чем прежде. Характер публикуемой в Phrack информации кардинально не изменится, однако Phrack предназначен для тех, кто хочет узнать о типах уязвимостей в системах, которые хакеры могут эксплуатировать. Если вас беспокоит возможность вторжения компьютерных злоумышленников в вашу систему, позвольте хакерам, пишущим для Phrack, указать на недостатки, которые стоит устранить. Phrack по-прежнему твёрдо поддерживает свободный обмен информацией и никогда не будет участвовать в цензуре — за исключением случаев, когда это необходимо для защиты личной тайны конкретного человека. В этой области необходимо найти тонкий баланс, и, будем надеяться, он будет найден. Наберитесь терпения и не судите о новом Phrack, не дав ему возможности исправить ошибки.

Я сказал своё слово, а теперь пришло время передать бразды правления Dispater'у. Желаю ему удачи, а вам, читатели, — надеюсь, новый Phrack понравится вам не меньше, чем предыдущие выпуски.

С уважением,

:Knight Lightning (kl@STORMKING.COM)

Несколько слов от Dispater:

В Phrack появится новая постоянная рубрика, напоминающая раздел «Письма редактору». Она будет публиковаться вторым файлом в каждом выпуске, начиная с выпуска 34. Там будут отвечать на любые вопросы, комментарии и проблемы, которые вы, читатели, хотите обсудить с Phrack публично.

Хочу особо поблагодарить Crimson Death за сотрудничество и помощь в возрождении Phrack. Он один из самых крутых хакеров, с которыми мне доводилось общаться. Без него у нас ничего бы не вышло. Среди других важных людей, заслуживающих упоминания, — The Monk и Twisted Pair.

Благодаря Tuc, Phrack вскоре будет использовать интернет-листсервер. Подробности — в Phrack 34. Phrack также можно будет найти на различных анонимных FTP-сайтах в Интернете, включая анонимный FTP-сайт EFF.ORG — Unix-машины под управлением Electronic Frontier Foundation, организации, которую мы в Phrack глубоко уважаем. Журнал также доступен на анонимном FTP-сайте CS.WIDENER.EDU.

За пределами Интернета мы надеемся создать несколько систем электронных досок объявлений в качестве архивных сайтов, включая Digital Underground (812)941-9427, которую эксплуатирует The Not. Материалы и письма в Phrack можно присылать туда или через Интернет на адрес "phracksub@STORMKING.COM".

Новый формат будет несколько более профессиональным. Это объясняется тем, что у меня нет желания однажды оказаться в суде, как Knight Lightning. Тем не менее у меня нет намерения превращать Phrack Inc. в какой-то сухой отраслевой журнал. Лёгкость и занимательность — одна из тех вещей, которые привлекли меня в Phrack. Думаю, большинство согласится, что необходимо соблюдать баланс между весельем и делом. Если этот баланс нарушится, вам, читателям, станет скучно — и мне тоже!

Загляните в Phrack World News Special Edition IV за «подробностями» о CyberView '91 — конференции SummerCon, организованной Knight Lightning этим летом в Сент-Луисе, штат Миссури.

Оглавление Phrack XXXIII

Phrack XXXIII Table of Contents
=-=

Shooting Shark

Автор: Crimson Death

В этом выпуске Phrack Profile представлен хакер, знакомый большинству из вас. Его познавательные файлы в Phrack и технических журналах Legion of Doom породили целую волну начинающих Unix-хакеров. Ваш и мой приятель...

~~~~~~~~~~~~~~

Личное

```
               Handle:  Shooting Shark
             Call him:  'Shark'
         Past handles:  None
        Handle origin:  It's the title of the 3rd song on "Revolution By Night,"
                        which many consider to be Blue Oyster Cult's last good
                        album.
        Date of Birth:  11/25/66
  Age at current date:  24
 Approximate Location:  San Francisco Bay Area.
               Height:  5'10"
               Weight:  150 lbs.
            Eye color:  Hazel
           Hair Color:  Dark Brown
            Computers:  First: Apple //e. Presently:  ALR Business V EISA
                                                      386/33.
```

История моей хакерской карьеры

В 1984 году мне посчастливилось учиться на выпускном курсе средней школы, где действовал один из пилотных классов «Advanced Placement Computer Science». Я тогда мало что знал о компьютерах, но интерес был огромный, поэтому я записался. «Advanced Placement Computer Science» подразумевал программирование на Pascal с использованием UCSD P-System на только что вышедшем Apple //e. Pascal меня не особо увлекал — ну кому вообще нравится Pascal? — зато я с удовольствием участвовал в послеурочных сессиях по пиратству программного обеспечения, а нередко — и прямо во время уроков, пока преподаватель рассказывал о циклах DO WHILE или о чём-нибудь столь же захватывающем. Среди любимых игр того времени были ZORK II и то, что я по сей день считаю лучшей игрой для Apple II, — RESCUE RAIDERS. Несколько месяцев спустя после начала учёбы мне каким-то образом удалось уговорить маму купить мне собственный Apple //e с целыми 64K оперативной памяти, монохромным монитором и флоппи-дисководом. Первый дешёвый жёсткий диск для Apple II — Sider — стоил тогда $700 за 10 Мб, так что об этом речи не шло.

Примерно в то же время Coleco активно рекламировала своё дополнение Adam к игровой приставке ColecoVision. Реклама эффективно играла на родительском чувстве вины и звучала примерно так:

> ***УЧИТЕЛЬ:*** *«Я хочу поговорить с вами о Билли. У него не очень хорошо идут дела в школе. Он, похоже, не усваивает новые понятия так же хорошо, как другие дети. Только и делает, что сидит иковыряет в носу.»*
> ***ОБЕСПОКОЕННЫЙ ОТЕЦ:*** *«Ну, господи, не знаю, что и делать. Наверное, всё потому, что его мать так много пила, пока была беременна.»*
> ***УЧИТЕЛЬ:*** *«А вы не думали купить Билли компьютер?»*

И разумеется, в следующей сцене маленький Билли вставлял кассету в новенький Adam и потихоньку карабкался к высоким оценкам.

Со мной, когда я получил СВОЙ компьютер, всё вышло совсем иначе. Я просто приходил домой после школы и играл в Wizardry. Перестал делать домашние задания и завалил 3 из 6 предметов в последнем семестре выпускного класса. К счастью, меня уже приняли в местный государственный университет, так что это было не так критично. Незадолго до выпускного я сдал тест AP Computer Science и набрал минимальный проходной балл. (Я не особо расстроился, когда сэр Фрэнсис Дрейк позже рассказал мне, что провалился. Впрочем, он отвечал на все вопросы на BASIC.)

Хуже того: примерно тогда же вышел «Военные игры». Признаю: мой интерес к хакерству во многом был навеян этим фильмом.

Вскоре после того, как я (едва-едва) окончил школу, я накопил денег и купил — только представьте — Hayes MicroModem //e. Стоил он что-то около $250, и я оказался в раю со скоростью 300 бод. Я начал звонить на местные BBS, где требовалось указывать настоящее имя, а потом перебрался на разные мелкие хакерские BBS. Стоит отметить, что 90% BBS того времени работали на Apple под управлением Networks, GBBS или каких-то их вариантов. Скорость редко превышала 300 бод. На одной из таких Apple Networks BBS я заметил, что пользователи говорят о каких-то загадочных штуках под названием «800 extenders» («экстендеры»). Я простодушно поинтересовался, что это такое, и получил ответ от Elric of Imrryr. Он объяснил: достаточно набрать номер 800, ввести шестизначный код — и можно звонить куда угодно БЕСПЛАТНО! Это было что-то невероятное. Я выбрал себе ник и начал звонить на системы вроде Sherwood Forest II и Sherwood Forest III, OSUNY и PloverNet. В период расцвета на любой из этих систем можно было ежедневно читать десятки новых сообщений с кучей свежих кодов Sprint и экстендеров. Это было здорово! Я продолжал доставать своего наставника — Elric, — и, несмотря на его несомненное раздражение моими тупыми вопросами, мы оставались друзьями. Со временем я понял, что Hayes MicroModem //e уже не то, что нужно, и накопил $400 на Novation Apple Cat 300 — самый крутой модем своего времени. В этом красавце был чип синтеза звука, позволявший генерировать речь, а главное — тоны DTMF и 2600 Гц. По глупости я начал заниматься blue boxing. Ирония в том, что я тогда жил именно в том городе, где десятью годами ранее Стива Возняка и Стива Джобса поймали за бокс.

А потом я поступил в колледж. Я бы, наверное, так и остался второсортным Apple-хакером (вместо того чтобы стать тем, кто я есть сейчас, — второсортным IBM-хакером) по сей день, если бы приятель не сказал мне, что легко взломать новую школьную Pyramid 90x — «супер-мини», работавшую на варианте BSD 4.2. «Профессор, который вёл курс по C, создал кучу аккаунтов с последовательными номерами и одним и тем же паролем по умолчанию,» — рассказал он. — «Просто перебирай их, пока не найдёшь тот, которым ещё не воспользовался студент!» Я урвал аккаунт, которым пользуюсь по сей день — уже семь лет спустя.

Примерно тогда же я позвонил на The Matrix, которую вёл Dr. Strangelove. Это был мой первый опыт с BBS-программой Ken's FORUM-PC. Dr. Strangelove оказался отличным парнем, хотя и смахивает чем-то на лесную мышь (и я говорю это в самом добром смысле). DSL помог мне собрать мой первый XT-клон в общей сложности за $400. Он даже ПОДАРИЛ мне многие нужные компоненты — например, CGA-карту и клавиатуру.

Вскоре после этого The Matrix прекратила работу и была быстро заменена IDI, которой управлял Aiken Drum. Именно здесь я познакомился с сэром Фрэнсисом Дрейком. Вскоре ПОСЛЕ ЭТОГО IDI

тоже закрылась и была быстро заменена Lunatic Labs Unltd, которую вёл мой старый друг The Mad Alchemist. TMA жил в пешей доступности от моего дома, так что я звонил на LunaLabs довольно часто. LunaLabs впоследствии стала базой Phrack на несколько выпусков, когда Knight Lightning и Taran King отошли от дел, поступив на первый курс колледжа.

За это время я по-настоящему погрузился в Unix и начал писать файлы для Phrack. Я написал около шести статей для Phrack, а потом одну для второго технического журнала LOD — с грубым взломщиком паролей перебором. Я понимаю, это звучит архаично, но на дворе был 1984 год, и я был одним из немногих людей в хакерском сообществе, которые действительно много знали о Unix. Несколько человек рассказывали мне, что именно моя статья в LOD TJ приобщила *их* к Unix-хакингу (вот это да). Я также написал оригинальную статью Unix Nasties для Phrack, и дважды, когда позже я активно прыгал по узлам интернета, мне случалось попасть на незатронутую систему в каком-нибудь захолустном колледже — вроде MIT — и найти *свой файл* в чьей-то директории.

В 1987 году я получил письмо из местного офиса ФБР. Оно было адресовано на моё настоящее имя и просило сообщить любую информацию о взломе в Сан-Диего, которой я бы захотел поделиться. Разумеется, я отказался, но они продолжали присылать новые письма. Мне к тому времени исполнилось 18 лет, и я решил прекратить заниматься незаконными вещами. Знаю: «ну и слюнтяй». Так Lunatic Labs, которой тогда управлял The Mad Alchemist, стала моим единственным пристанищем — просто потому, что это была местная доска. Когда Elric и сэр Фрэнсис Дрейк несколько выпусков взяли на себя редактирование Phrack, я писал все их вводные файлы.

Когда мой компьютер сломался, я просто отпустил те времена. Иногда старые знакомые как-то умудрялись меня найти и звонили по голосовой связи — к моему удивлению. Кто-то однажды сказал, что для меня создан аккаунт на BBS под названием «Catch 22» — системе, которая была, видимо, слишком хороша, чтобы долго держаться. Кажется, я позвонил туда дважды, прежде чем она закрылась. Совсем недавно мне позвонил Crimson Death, попросил написать Profile, — и вот мы здесь.

Чем я занимаюсь сейчас

После двух лет на факультете информатики в колледже я сменил специализацию на театральные искусства по трём причинам:

1. Люди с театрального факультета в целом приятнее;
2. Большинство студентов-информатиков были для меня слишком задротистыми (подчёркиваю: большинство); и
3. Я просто никак не мог сдать Математический анализ III!

В прошлом году я получил степень бакалавра по театральным искусствам и, как все свежеиспечённые театральные, начал репетировать реплики вроде «Хотите картошку фри?» и «Могу рассказать про сегодняшнее специальное предложение?». Однако мне фантастически повезло получить работу в топ-менеджменте одного из самых известных на западном побережье производителей IBM-совместимых видеокарт. Должность позволяет мне играться с разными игрушками — например, AutoDesk 3D Studio и 24-битными фрейм-буферами. Созданное мной 24-битное изображение было опубликовано на обложке ноябрьского 1990 года номера журнала Presentation Products. Какое-то время я был системным администратором корпоративной Unix-системы с IP-адресом, netnews и всем прочим. Сейчас я управляю двухлинейной BBS компании — если вы разберётесь, где я работаю, позвоните и оставьте мне сообщение. Я также увлечён MIDI и помог своей маме оборудовать небольшую студию с Tascam Porta One и Roland MT-32. Я снимался в массовке в фильмах «Patty Hearst» (вместе с The $muggler) и «The Doors» (для чего я провёл 22-часовой съёмочный день в театре Warfield в Сан-Франциско на съёмках концертной сцены, КОТОРУЮ ВЫРЕЗАЛИ ИЗ #*%& ФИЛЬМА), и с нетерпением жду новых работ в

кино — в роли, которая не требует от меня носить клёш. Я также играл в местном университетском театре и в следующем году буду ставить полнометражный спектакль в местном муниципальном театре. Я считаю себя разносторонним человеком.

Ах да. В октябре я ещё и женился.

Люди, которых я знал

Elric of Imrryr — Мой настоящий наставник. Он ввёл меня в это дело. Жаль, что перебрался в Лос-Анджелес.

Shadow 2600 — Известный некоторым как David Flory, мир его праху. В начале моей карьеры он упомянул меня и внёс в соавторы статьи для 2600. Это был первый раз, когда я увидел своё имя в печати.

Oryan QUEST — После публикации моей первой статьи в Phrack он начал мне звонить (жил примерно в 20 милях от меня). Звонил просто так и скидывал мне коды, как будто пытался произвести впечатление. Не понимаю, зачем ему была нужна моя валидация. Я был одним из первых, кто раскусил его, и быстро понял, что он патологический лжец. Позже он солгал обо мне на одной BBS и добился моей блокировки, потому что сисоп считал его великим человеком. Вот так.

Sir Francis Drake — Определённо один из самых своеобразных людей, которых я встречал. Он напечатал довольно дрянной двухчастный фантастический рассказ, который я написал, в своём журнале WORM. Вскоре после этого журнал закрылся — думаю, между этими событиями есть связь.

David Lightman — Никогда не встречал его лично, но он раньше пользовался моим Unix-аккаунтом в школе.

The Disk Jockey — Он пробил TRW-отчёт на женщину, на которой я потом женился. Кстати, в одной сцене фильма «Hoosiers» его можно увидеть на заднем плане — играет в баскетбол.

Lex Luthor — Не могу не уважать человека, который сначала опубликовал мою статью в LOD TJ, а потом, год спустя, позвонил мне ни с того ни с сего и дал свой личный код дозвона Tymnet.

Dr. Strangelove — Держит очень крутую BBS под названием JUST SAY YES. Звоните: (415) 922-2008. DSL, пожалуй, несёт единоличную ответственность за то, что я пересел на IBM-клоны, что в свою очередь принесло мне работу (много ли сейчас нанимают Apple //-программистов?).

BBS

Sherwood Forest II and III, OSUNY — Я просто считал их величайшими системами из всех когда-либо существовавших.

Pirate's Bay — Работала под управлением Mr. KRACK-MAN, который считал себя величайшим Apple-пиратом всех времён. По сей день, насколько я знаю, стоит.

The 2600 Magazine BBS — Работала на Apple BBS-программе под названием TBBS. Именно там я познакомился с David Flory.

The Police Station — Помните ЭТУ?

The Matrix, IDI, Lunatic Labs — Три замечательные форум-PC доски в районе Залива.

Catch-22 — 25 пользователей, без очередей!

И, конечно, net.telecom (оригинальный), comp.risks, rec.arts.startrek...

Воспоминания

Помните Alliance Teleconferencing? Кладёшь трубку, идёшь поесть, забываешь о ней, возвращаешься через 24 часа — конференция всё ещё идёт.

Играю в Wizardry и Rescue Raiders на моём Apple //e, пока не теряю чувствительность в пальцах...

Заказываю по карточке 13 спальных мешков Garfield детского размера людям, которые мне в школе особо не нравились...

Звонить операторам канадской DA и воспроизводить им тон 2600 Гц — это всегда было весело.

Трешим все местные центральные офисы вместе с The Mad Alchemist...

Мой момент близости к величию: несколько лет назад я возвращался домой на BART, когда в мой вагон зашёл Стив Возняк с двумя детьми. Вёз их на матч Warriors. Я был единственным человеком в вагоне, который его узнал. Он подписал мне попавшийся под руку экземпляр BYTE, и мы поговорили о его новом проекте — CL-9, универсальном пульте дистанционного управления. (Знаете хоть кого-нибудь, кто действительно КУПИЛ одну из этих штук?)

...И теперь вопрос

«Среди широкого круга фрикеров, с которыми вы встречались, считаете ли вы большинство из них компьютерными фриками-задротами?»

В эпоху пиратства на Apple я встречал немало молодых людей, определённо принадлежавших к Ордену Задрота. Однако настоящих фрикеров/хакеров, с которыми я лично познакомился, я могу пересчитать по пальцам одной руки. Никого из них я бы не назвал задротом, занудой, спазматиком или дорком. Все они — люди, живущие на краю и делающие всё немного иначе. Сколько ЗАКОНОПОСЛУШНЫХ знакомых у вас с кольцом в носу? — но все они вызывали у меня уважение. Впрочем, позвольте взять свои слова обратно. Dr. Strangelove, на мой взгляд, слегка задроватый (моя мама считает его симпатичным, но она же говорила, что сэр Фрэнсис Дрейк «симпатичный» — и когда я ему об этом сказал, его это бесконечно раздражало), однако я считаю его хорошим другом и в целом k-kool d00d. (Уверен, он мне за это сейчас позвонит...) Единственный фрикер, к которому я испытывал искреннюю антипатию, — Oryan QUEST, но лишь потому, что он был патологическим лжецом и занудой. Кто знает, может, сейчас он стал нормальным человеком, так что без обид — особенно если он знает мой домашний адрес.

Ну и в общем...

-> Спасибо за уделённое время, Shooting Shark.

Crimson Death

Руководство хакера по Интернету

Автор: The Gatsby

Версия 2.00 / AXiS / 7 июля 1991 г.

---

1. Оглавление

2. Введение

Первоначально этот информационный файл был опубликован в информационном бюллетене IRG, однако содержал ряд ошибок, которые я хотел исправить. Также я добавил больше технической информации.

Этот файл предназначен для новичков в Интернете и для людей (таких как я), не обучающихся в университете с доступом к Интернету. Он охватывает основные команды, принципы использования Интернета и некоторые советы по хакингу через Интернет. Не существует ВОЛШЕБНОГО способа взломать систему UNIX. Если у вас возникнут вопросы, меня можно найти на нескольких досках.

Пишите мне в Интернете: gats@ryptyde.cts.com
bbs.gatsby@spies.com

— The Gatsby

Особая благодарность Haywire (он же Insanity: SysOp канала Insanity Lane), Doctor Dissector и всем участникам AXiS.

3. Глоссарий, аббревиатуры и сокращения

ACSE — Association Control Service Element (Элемент управления сервисом ассоциаций). Используется совместно с ISO для управления ассоциациями.

ARP — Address Resolution Protocol (Протокол разрешения адресов). Применяется для преобразования IP-адреса в адрес Ethernet.

ARPA — Defense Advanced Research Project Agency (Агентство передовых оборонных исследовательских проектов).

ARPANET — Сеть ARPA. Это экспериментальная PSN, которая по-прежнему является подсетью Интернета.

CCITT — International Telegraph and Telephone Consultative Committee (Международный консультативный комитет по телеграфии и телефонии). Международный комитет, устанавливающий стандарты. Хотелось бы, чтобы они установили стандарт и для написания своего собственного названия!

CERT — Computer Emergency Response Team (Группа реагирования на компьютерные инциденты). Отвечает за координацию мероприятий по реагированию на инциденты безопасности. Публикует весьма полезные отчёты о «дырах» в различных версиях UNIX — настоятельно рекомендую их читать.

CMIP — Common Management Information Protocol (Общий протокол управленческой информации). Новый протокол высокого уровня.

CLNP — Connectionless Network Protocol. OSI-эквивалент интернет-протокола IP.

DARPA — Defence Advanced Research Project Agency. См. ARPANET.

DDN — Defence Data Network (Оборонная информационная сеть).

driver (драйвер) — программа (или программное обеспечение), осуществляющая взаимодействие с самой сетью. Примеры: TELNET, FTP, RLOGON и др.

ftp — File Transfer Protocol (Протокол передачи файлов). Используется для копирования файлов с одного хоста на другой.

FQDN — Fully Qualified Domain Name (Полное доменное имя). Полное имя хоста, отражающее домены, в состав которых он входит.

Gateway (шлюз) — компьютер, осуществляющий связь между сетями.

Host (хост) — компьютер, подключённый к PSN.

Hostname (имя хоста) — имя, официально идентифицирующее каждый компьютер, подключённый к межсети.

Internet (Интернет) — конкретная межсеть на основе IP.

IP — Internet Protocol (Интернет-протокол). Стандарт, позволяющий разнородным хостам устанавливать соединение.

ICMP — Internet Control Message Protocol. Используется для передачи сообщений об ошибках в TCP/IP.

LAN — Local Area Network (Локальная вычислительная сеть).

MAN — Metropolitan Area Network (Городская вычислительная сеть).

MILNET — Несекретная оперативная военная сеть DDN.

NCP — Network Control Protocol (Протокол управления сетью). Официальный сетевой протокол с 1970 по 1982 год.

NIC — DDN Network Information Center (Информационный центр сети DDN).

NUA — Network User Address (Сетевой адрес пользователя).

OSI — Open System Interconnection (Взаимодействие открытых систем). Международная программа стандартизации, облегчающая связь между компьютерами различных марок и моделей.

Protocol (протокол) — правила взаимодействия между хостами, обеспечивающие упорядоченную передачу информации.

PSN — Packet Switched Network (Сеть с пакетной коммутацией).

RFC — Request For Comments (Запрос комментариев). Технические документы о протоколах Интернета; доступны через anonymous ftp на NIC.DDN.MIL.

ROSE — Remote Operations Service Element. Протокол, используемый совместно с приложениями OSI.

TAC — Terminal Access Controller (Контроллер терминального доступа). Компьютер, обеспечивающий прямой доступ к Интернету.

TCP — Transmission Control Protocol (Протокол управления передачей).

TELNET — Протокол для открытия прозрачного соединения с удалённым хостом.

tftp — Trivial File Transfer Protocol (Упрощённый протокол передачи файлов). Один из способов передачи данных между хостами.

UDP — User Datagram Protocol (Протокол пользовательских датаграмм).

Unix — Защищён авторским правом AT&T; я использую это название для обозначения всех Unix-подобных систем, с которыми вам придётся сталкиваться чаще всего.

UUCP — Unix-to-Unix Copy Program (Программа копирования Unix-Unix). Протокол, позволяющий передавать файлы между UNIX-системами. Работает по телефонным линиям, используя собственный протокол, X.25 и TCP/IP. Существует также для VMS и MS-DOS.

uucp (строчными буквами) — команда UNIX uucp. Дополнительную информацию читайте в файлах The Mentor'a из Legion of Doom Technical Journals.

WAN — Wide Area Network (Глобальная вычислительная сеть).

X.25 — Стандартный протокол CCITT, регулирующий соединение двух хостов.

В данном файле я использовал несколько специальных обозначений. Ключ к ним:

`*` — Скопировано непосредственно из UNIX. Располагается у левого края. Обычно это «инструкции по выполнению» или просто «примеры» действий при работе с Интернетом.

`#` — Означает команды или то, что необходимо ввести.

4. Что такое Интернет?

Чтобы понять Интернет, необходимо прежде всего знать, что он собой представляет. Интернет — это совокупность различных сетей. Первой из них стала ARPANET — экспериментальная глобальная сеть (WAN). ARPANET была создана в 1969 году; эта экспериментальная PSN использовала Network Control Protocol (NCP). NCP был официальным протоколом Интернета (известного тогда также как DARPA Internet или ARPA Internet) с 1970 по 1982 год. В начале 80-х DARPA разработало Transmission Control Protocol/Internet Protocol — официальный протокол и по сей день; подробнее об этом — ниже. В результате в 1983 году ARPANet разделилась на две сети: MILNET и ARPANET (обе по-прежнему входят в состав DDN).

Развитие локальных (LAN) и глобальных (WAN) сетей способствовало расширению Интернета — теперь он объединяет более 2000 сетей. В их число входят NSFNET, MILNET, NSN, ESnet и CSNET. Хотя большая часть Интернета сосредоточена в Соединённых Штатах, он также соединяет TCP/IP-сети Европы, Японии, Австралии, Канады и Мексики.

5. Откуда можно получить доступ к Интернету

Интернет чаще всего присутствует в локальных (LAN) и глобальных (WAN) сетях. LAN — это сети, обеспечивающие соединение и взаимодействие группы компьютеров, прежде всего для совместного использования ресурсов: накопителей данных и принтеров. LAN охватывают небольшие расстояния (менее мили) и почти всегда располагаются в пределах одного здания или

комплекса. WAN — это сети, предназначенные для передачи данных на большие расстояния (многие сотни миль). Также получить доступ к Интернету можно через TymNet или Telenet посредством шлюза. Однако NUA придётся искать самостоятельно.

6. TAC

TAC (контроллер терминального доступа) — ещё один способ получить доступ к Интернету. Это просто дозвон до терминального контроллера доступа. Для этого потребуется пароль и учётная запись. TAC обеспечивает прямой доступ к MILNET. Пример телефонного номера TAC: (800)368-2217, однако существует и немало других. Более того, в CERT циркулирует отчёт о людях, пытающихся обнаружить эти номера с помощью социальной инженерии.

Если вы хотите получить руководство по TAC, напишите письмо по адресу:

```
Defense Communications Agency
Attn: Code BIAR
Washington, DC 20305-2000
```

Обязательно укажите, что вам нужен TAC User Guide, 310-p70-74.

Для входа в систему вам потребуется карточка TAC Access Card, которую, вероятно, можно получить в DDN NIC. Вот пример входа в систему:

```
Use Control-Q for help...

*
* PVC-TAC 111: 01               \ TAC использует это для идентификации себя
* @ #o 124.32.5.82               \ Используйте ``O'' для открытия соединения
*                                / с нужным вам интернет-адресом.
*
* TAC Userid: #THE.GATSBY
* Access Code: #10kgb0124
* Login OK
* TCP trying...Open
*
*
```

7. Основные команды

7a. Основные команды TELNET

Ситуация: у вас есть учётная запись на UNIX-системе, которая является хостом в Интернете. Теперь вам открыт весь мир! После входа в UNIX-систему вы увидите командную строку, которая может выглядеть как `$` или `%` (зависит от используемой оболочки и типа Unix-системы). В командной строке доступны все обычные команды UNIX, но находясь на интернет-хосте, вы можете ввести `telnet`, что переведёт вас в командную строку telnet.

```
*
* $ #telnet
* ^   ^
  |   |
  |  команда, которая переводит вас в строку telnet
  |
  обычная командная строка UNIX
```

Вы должны увидеть следующее:

```
*
* telnet>
```

```
*
```

В этой строке вам доступен совершенно другой набор команд (взят из UCSD; может отличаться в зависимости от системы):

```
*
* telnet> #help
*
* close           закрыть текущее соединение
* display         показать рабочие параметры
* open            подключиться к сайту
* quit            выйти из telnet
* send            передать специальный символ
* set             установить рабочие параметры
* status          напечатать информацию о состоянии
* toggle          переключить рабочие параметры
* ?               показать то, что вы сейчас видите
*
```

close — закрыть соединение при многозадачной работе или переключении между системами.

display — управление параметрами отображения:

```
^E    echo (эхо)
^]    escape (экранирование)
^H    erase (стереть символ)
^O    flushoutput (сбросить вывод)
^C    interrupt (прерывание)
^U    kill (уничтожить строку)
^\    quit (выход)
^D    eof (конец файла)
```

open — введите `open [хост]` для подключения к системе:

```
*
* $ #telnet ucsd.edu
*
```

или

```
*
* telnet> #open 125.24.64.32.1
*
```

quit — выйти из telnet и вернуться в UNIX
send — отправить файлы
set — установка параметров
echo — символ для переключения локального эха
escape — символ для возврата в командный режим telnet

Следующие параметры требуют включения `localchars`:

```
erase         -  символ для стирания символа
flushoutput   -  символ для прерывания вывода
interrupt     -  символ для прерывания процесса
kill          -  символ для стирания строки
quit          -  символ для передачи сигнала Break
eof           -  символ для передачи EOF
?             -  показать справочную информацию
```

7b. Анонимный ftp на удалённый сайт

ftp (File Transfer Protocol) используется для копирования файлов с удалённого хоста на тот, на котором вы находитесь. Можно скопировать что угодно. Защита файла passwd ужесточилась, но кое-где он по-прежнему доступен (всегда стоит попробовать).

Это может оказаться полезным, когда вы видите сайт CuD (Computer Underground Digest) в Интернете, принимающий анонимный ftp, и хотите читать CuD, не тратя время на их скачивание с досок. Лучше всего начать с просмотра директории, чтобы понять, что вы получите.

Пример: архивный сайт CuD имеет интернет-адрес 192.55.239.132, а моё имя учётной записи — «gats».

```
*
* $ #ftp
* ^  ^
  |  |
  | команда ftp
  |
 командная строка UNIX

*
* ftp> #open 192.55.239.132
* Connected to 192.55.239.132
* 220 192.55.239.132 FTP Server (sometimes the date, etc)
* Name (192.55.239.132:gats): #anonymous
*            ^         ^        ^
             |         |        |
             |         |       Здесь вводите 'anonymous', если у вас нет
             |         |     учётной записи на 192.55.239.132.
             |         |
             |        Имя моей учётной записи или [откуда]
             |
            Это интернет-адрес или [куда]
*
* Password: #gats
*            ^
             |
            Здесь просто введите своё имя пользователя или всё, что хотите.
            Это не принципиально.

*
* % ftp 192.55.239.132
* Connected to 192.55.239.132
* ftp> #ls
*       ^
        |
       Вы подключены, значит можете просмотреть директорию командой ls.
```

Перемещайтесь, как в обычной UNIX-системе. Большинство команд по-прежнему работают на этом соединении. Вот пример того, как я получаю копию Effector от Electronic Frontier Foundation (выпуск 1.04) с интернет-адреса 192.55.239.132:

```
*
* % #ftp
* ftp> #open 128.135.12.60
* Trying 128.135.12.60...
* 220 chsun1 FTP server (SunOS 4.1) ready.
* Name (128.135.12.60:gatsby): anonymous
* 331 Guest login ok, send ident as password.
* Password: #gatsby
* 230 Guest login ok, access restrictions apply.
* ftp> #ls
* 200 PORT command successful.
* 150 ASCII data connection for /bin/ls (132.239.13.10,4781) * (0 bytes).
* .hushlogin
* bin
* dev
* etc
* pub
* usr
* README
* 226 ASCII Transfer complete.
* 37 bytes received in 0.038 seconds (0.96 Kbytes/s)
* ftp>
```

Здесь можно попробовать выполнить `cd` *в директорию* `etc` *или просто запросить* `/etc/passwd` *командой* `get`*, однако получение файла passwd таким способом — уже умирающее искусство.*

```
* ftp> #cd pub
* 200 PORT command successful.
* ftp> #ls
* ceremony
* cud
* dos
* eff
* incoming
* united
* unix
* vax
* 226 ASCII Transfer complete.
* 62 bytes received in 1.1 seconds (0.054 Kbytes/s)
* ftp> #cd eff
* 250 CWD command successful.
* ftp> #ls
* 200 PORT command successful.
* 150 ASCII data connection for /bin/ls (132.239.13.10,4805) (0 bytes).
* Index
* eff.brief
* eff.info
* eff.paper
* eff1.00
* eff1.01
* eff1.02
* eff1.03
* eff1.04
* eff1.05
* realtime.1
* 226 ASCII Transfer complete.
* 105 bytes received in 1.8 seconds (0.057 Kbytes/s)
* ftp> #get
* (remote-file) #eff1.04
* (local-file) #eff1.04
* 200 PORT command successful.
* 150 Opening ASCII mode data connection for eff1.04 (909 bytes).
* 226 Transfer complete.
* local: eff1.04 remote: eff1.04
* 931 bytes received in 2.2 seconds (0.42 Kbytes/s)
* ftp> #close
* Bye...
* ftp> #quit
* %
*
```

Чтобы прочитать файл, просто получите его командой `get` и выведите в буфер. Если файлы слишком велики, можно передать их через `xmodem` с хоста, на котором вы находитесь. Просто введите `xmodem` — это значительно ускорит получение файлов. Вот настройка (как найдено на ocf.berkeley.edu):

```
Если вы хотите:                                          введите:

отправить текстовый файл с Apple-компьютера на ME          xmodem ra <filename>
отправить текстовый файл с не-Apple домашнего компьютера   xmodem rt <filename>
отправить нетекстовый файл с домашнего компьютера          xmodem rb <filename>
отправить текстовый файл на Apple-компьютер с ME           xmodem sa <filename>
отправить текстовый файл на не-Apple домашний компьютер    xmodem st <filename>
отправить нетекстовый файл на домашний компьютер           xmodem sb <filename>
```

После этого xmodem выведет:

```
*
* XMODEM Version 3.6 -- UNIX-Microcomputer Remote File Transfer Facility
* File filename Ready to (SEND/BATCH RECEIVE) in (binary/text/apple) mode
* Estimated File Size (file size)
* Estimated transmission time (time)
```

```
* Send several Control-X characters to cancel
*
```

Совет: передача файлов — дело непредсказуемое. Один из способов улучшить ситуацию — отключить управление потоком на коммутаторе annex. Перед выполнением rlogin введите в командной строке annex:

```
stty oflow none
stty iflow none
```

Это лучше всего работает при соединении через 2-6092.

Некоторые специальные команды, используемые в ftp-сессии: `cdup` (аналог `cd ..`) и `dir` (выводит подробный список файлов).

tftp (Trivial File Transfer Protocol; команда пишется строчными буквами, поскольку UNIX чувствителен к регистру) — команда для передачи файлов между хостами. Иногда используется аналогично ftp: можно перемещаться по файловой системе с помощью команд UNIX. Я не буду подробно останавливаться на этой части, но расскажу о базовом формате и синтаксисе для получения нужных файлов. Кроме того, я расскажу, как «вытащить» /etc/passwd с удалённых сайтов.

Существует давно известный трюк, позволяющий «вытащить» файл /etc/passwd с различных сайтов, не взламывая систему напрямую. Затем остаётся запустить Brute Hacker (последняя версия) на полученном файле — и вы экономите время и силы. Эта «дыра» (речь не идёт о методе получения прав суперпользователя UNIX) встречается в SunOS 3.X, но исправлена в 4.0. Иногда она присутствует в System V, BSD и ряде других систем.

Единственная проблема с этой «дырой» состоит в том, что системный администратор нередко замечает ваши действия. Проблема возникает при слишком большом числе попыток tftp получить /etc/passwd. При следующем входе в систему вы можете увидеть нечто подобное (скопировано с plague.berkeley.edu — похоже, они поняли, что я делал):

```
*
* DomainOS Release 10.3 (bsd4.3) Apollo DN3500 (host name):
*         This account has been deactivated due to use in system cracking
* activities (specifically attempting to tftp /etc/passwd files from remote
* sites) and for having been used or broken in to from <where the calls are
* from>.  If the legitimate owner of the account wishes it reactivated,
* please mail to the staff for more information.
*
* - Staff
*
```

Команда tftp используется в следующем формате:

```
tftp -<команда> <любое имя> <Интернет-адрес>  /etc/passwd  <netascii>
```

Команда `-g` — получить файл. Файл будет скопирован в вашу домашнюю директорию, где вы сможете делать с ним всё что угодно.

Любое имя — если вы копируете файл в домашнюю директорию, ему нужно дать имя.

Интернет-адрес — адрес, с которого вы хотите получить файл passwd. Таких адресов сотни тысяч.

/etc/passwd — ЭТО ТОТ ФАЙЛ, КОТОРЫЙ ВАМ НУЖЕН. Файл Джона Смита вам ни к чему, хотя его тоже несложно получить.

netascii — формат, в котором файл будет передан.

`&` — добро пожаловать в мир UNIX с его многозадачностью. Этот символ в конце команды позволяет делать другие вещи параллельно (например, одновременно захватить файл passwd с самой UNIX-системы, на которой вы работаете).

Вот пример: мы хотим получить файл passwd с sunshine.ucsd.edu. Файл в домашней директории будет называться `asunshine`.

```
*
* $ #tftp -g asunshine sunshine.ucsd.edu /etc/passwd &
*
```

7d. Основы fingerring'a

Fingering — отличный способ найти учётные записи на удалённых сайтах. Введите `who` или просто `finger` , чтобы получить имена для «прощупывания». Это даст вам массу информации об учётной записи человека. Вот пример:

```
*
* % #who
* joeo                 ttyp0       Jun 10 21:50   (bmdlib.csm.edu)
* gatsby               ttyp1       Jun 10 22:25   (foobar.plague.mil)
* ddc                  crp00       Jun 10 11:57   (aogpat.cs.pitt.edu)
* liliya               display     Jun 10 19:40

                /и выполняем finger по найденным данным

* % #finger bbc
* Login name: ddc                      In real life: David Douglas Cornwall
* Office: David C. Co
* Directory: //aogpat/users_local/bdc     Shell: /bin/csh
* On since Jun 10 11:57:46 on crp00 from aogpat   Phone 555-1212
* 52 minutes Idle Time
* Plan:  I like to eat apples and bananas.
* %
*
```

Теперь можно просто позвонить (или выполнить Telnet) на `aogpat.cs.pit.edu` и попробовать подобрать учётную запись. Попробуйте фамилию в качестве пароля, затем имя, отчество — и все варианты в обратном порядке. Шансы войти весьма высоки, потому что люди беспечны.

Если в данный момент нет онлайн-пользователей для команды `who`, введите `last` — и появится список всех, кто входил в систему. Теперь «прощупайте» их. Единственная проблема с командой `last` — необходимость прервать её выполнение.

Также можно попробовать позвонить отдельным пользователям и представиться системным администратором (то есть применить социальную инженерию). Однако телефонный номер присутствует в файле `.plan` (файл, отображаемый при finger'е пользователя) далеко не всегда.

8. Другие сети

AARNet — Australian Academic and Research Network. Поддерживает исследования различных австралийских университетов. Использует TCP/IP, DECnet и OSI (CLNS).

ARPANET — уже рассматривалась выше.

BITNET — Because It's Time NETwork. Всемирная сеть, соединяющая множество колледжей и университетов. Использует различные протоколы, включая TCP/IP.

CREN CSNET — Corporation for Research and Educational Network (CREN) или Computer + Science research NETwork (CSNET). Связывает учёных по всему миру. CSNET обеспечивает доступ к Интернету, CREN — к BITNET. Сегодня чаще используется название CREN.

CSUNET — California State University Network. Соединяет кампусы Калифорнийского государственного университета и другие университеты Калифорнии. Основана на протоколе CCITT

X.25; также использует TCP/IP, SNA/DSLC, DECnet и другие.

The Cypress Net — Начинала как экспериментальная сеть. Сегодня используется для дешёвого подключения к TCP/IP Интернету.

DRI — Defense Research Internet. WAN, используемая как платформа для работы. Предоставляет различные сервисы: многоадресную рассылку, конференции в реальном времени и прочее. Использует TCP/IP (см. также RFC 907-A).

ESnet — Новая сеть, эксплуатируемая Управлением энергетических исследований Министерства энергетики США (DoE OER). Является основой для всех программ DoE OER. Заменила сеть физики высоких энергий DECnet (HEPnet) и сеть Magnetic Fusion Energy (MFEnet). Поддерживает IP/TCP и DECnet.

JANET — Joint Academic NETwork, базируется в Великобритании, подключена к Интернету. PSN (информация проходит через PAD), использует протокол X.25, хотя поддерживает и TCP/IP. Также соединяется с PSS (Packet Switched Service — PSN, принадлежащая British Telecom).

JUNET — Университетская система обмена сообщениями Японии, использует UUCP, Интернет в качестве основы и X.25 (см. RFC 877). Является частью USENET (сетевые новости).

Los Nettos — Высокоскоростная MAN в районе Лос-Анджелеса. Использует IP/TCP.

MILNET — После разделения ARPANET была создана DDN; MILNET (MILitary NETwork) — её часть. MILNET несекретна, однако существуют ещё три засекреченные сети, входящие в DDN.

NORDUNet — Основа для сетей скандинавских стран: Дании (DENet), Финляндии (FUNET), Исландии (SURIS), Норвегии (UNINETT) и Швеции (SUNET). Поддерживает TCP/IP, DECnet и X.25.

NSN — NASA Science Network. Используется NASA для передачи и ретрансляции информации. Протоколы: TCP/IP. NSN имеет родственную сеть Space Physics Analysis Network (SPAN) для DECnet.

ONet — Ontario Network. TCP/IP-сеть для научных исследований.

NSFNet — National Science Foundation Network. Входит в семейство IP/TCP, однако использует UDP (User Datagram Protocol), а не TCP. Является сетью для американского сообщества научных и инженерных исследований.

Подсети NSFNet:

• **BARRNet** — Bay Area Regional Research Network, расположена в районе Сан-Франциско. TCP/IP.
• **CERFnet** — California Education and Research Federation Network. Исследовательская сеть для университетов Южной Калифорнии. TCP/IP.
• **CICNet** — Committee on Institutional Cooperation. Обслуживает «Большую десятку» и Чикагский университет. TCP/IP.
• **JvNCnet** — John von Neumann National Supercomputer Center. TCP/IP.
• **Merit** — Объединяет академические и исследовательские компьютеры Мичигана. Поддерживает TCP/IP, X.25 и Ethernet для LAN.
• **MIDnet** — Объединяет 18 университетов и исследовательских центров на Среднем Западе США. Протоколы: TELNET, FTP и SMTP.
• **MRNet** — Minnesota Regional Network. Обслуживает Миннесоту. TCP/IP.
• **NEARnet** — New England Academic and Research Network. Связывает различные исследовательские и образовательные учреждения. Дополнительную информацию можно получить, написав на `nearnet-staff@bbn.com`.
• **NCSAnet** — National Center for Supercomputing Applications. Поддерживает всё семейство IP (TCP, UDP, ICMP и др.).

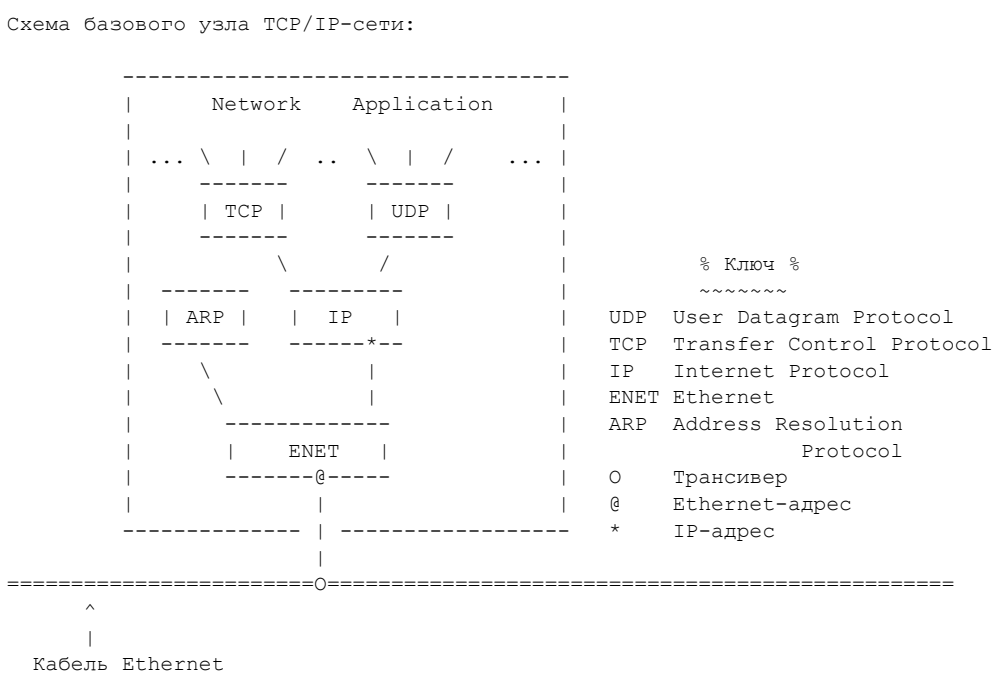
• **NWNet** — North West Network. Обслуживает северо-западные штаты США и Аляску. Поддерживает IP и DECnet.
• **NYSERNet** — New York Service Network. Автономная некоммерческая сеть. TCP/IP.
• **OARnet** — Ohio Academic Resources Network. Предоставляет доступ к Ohio Supercomputer Center. TCP/IP.
• **PREPnet** — Pennsylvania Research and Economic Partnership. Эксплуатируется Bell of Pennsylvania. TCP/IP.
• **PSCNET** — Pittsburgh Supercomputer Center. Обслуживает Пенсильванию, Мэриленд и Огайо. TCP/IP и DECnet.
• **SDSCnet** — San Diego Super Computer Center. Цель — поддержка научных исследований. Интернет-адрес: `y1.ucsc.edu`; также можно позвонить Бобу по телефону (619)534-5060 и попросить учётную запись на его Cray.
• **Sesquinet** — Сеть из Техаса. TCP/IP.
• **SURAnet** — Southeastern Universities Research Association Network. Объединяет учреждения на юго-востоке США.
• **THEnet** — Texas Higher Education Network, управляется Техасским университетом A&M. Соединяется с хостами в Мексике.
• **USAN/NCAR** — University SAtellite Network / National Center for Atmospheric Research. Сеть для обмена информацией.
• **Westnet** — Охватывает западную часть США, за исключением Калифорнии. Поддерживается Университетом штата Колорадо.

USENET — Сетевые новости (база сообщений Интернета). Весьма обширная база с более чем 400 различными темами, охватывающая 17 стран.

9. Протоколы Интернета

TCP/IP — общий термин, обозначающий всё семейство интернет-протоколов. В него входят: IP, TCP, UDP, ICMP, ROSE, ACSE, CMIP, ISO, ARP и Ethernet для LAN. Если хотите узнать больше — обратитесь к RFC.

Протокол TCP/IP — это «многоуровневый» набор протоколов. На следующей диаграмме из RFC 1180 показано, как протокол выстраивается по слоям при установлении соединения.



TCP/IP: Если соединение устанавливается между модулем IP и модулем TCP, пакеты называются TCP-датаграммами. TCP отвечает за то, чтобы команды доходили до адресата. Он отслеживает всё отправленное и повторно передаёт то, что не прошло. IP обеспечивает базовый сервис по доставке TCP-датаграмм из одного места в другое. Может показаться, что всю работу выполняет TCP — это верно для небольших сетей, однако при подключении к удалённому хосту в Интернете (через несколько сетей) задача становится значительно сложнее. Допустим, я подключён с сервера UCSD к LSU (SURAnet): датаграммы должны пройти через основу NSFnet. IP обязан отслеживать все данные при переключении на основе NSFnet с TCP на UDP. Единственная основа NSFnet, соединяющая LSU, находится в Университете Мэриленда, у которого другие наборы каналов. Типы кабелей (магистралей) и каналов — T1 (базовый 24-канальный импульсно-кодовый модулятор 1.544 Мбит/с, принятый в США) и 56 Кбит/с. Но переключение с T1 на 56 Кбит/с и с TCP на UDP — это ещё не всё. Датаграммы на пути к основе NSFnet (в Университете Мэриленда) могут следовать по множеству различных маршрутов с сервера UCSD.

Всё, что делает TCP, — это разбивает данные на датаграммы (управляемые фрагменты) и отслеживает их. Отслеживание ведётся путём добавления заголовка в начало каждой датаграммы. Заголовок содержит 160 (20 октетов) фрагментов информации о датаграмме, в том числе FQDN (полное доменное имя). Датаграммы нумеруются в октетах (группах из восьми двоичных цифр). Например, при 500 октетах данных нумерация датаграмм будет следующей: 0, следующая датаграмма — 500, следующая — 1000, 1500 и т.д.

UDP/IP: UDP — один из двух основных протоколов IP. Иными словами, UDP работает так же, как TCP: добавляет заголовок к отправляемым данным и передаёт их IP для транспортировки по Интернету. Разница в том, что UDP предоставляет сервис для пользовательских сетевых приложений. Он не поддерживает сквозное соединение — просто «выталкивает» датаграммы.

ICMP: ICMP используется для передачи сообщений об ошибках. Например, при попытке подключиться к системе вы можете получить сообщение «Host unreachable» — это и есть ICMP в действии. Данный протокол универсален внутри Интернета по своей природе. Он не использует номера портов в заголовках, поскольку взаимодействует непосредственно с сетевым программным обеспечением.

Ethernet: Большинство сетей используют Ethernet. Ethernet — это, по сути, общая линия. Когда пакеты отправляются в Ethernet, их видит каждый хост в сети. Чтобы пакеты попадали по нужному адресу, разработчики Ethernet позаботились об уникальности каждого адреса. Для этого под адрес Ethernet выделено 48 бит, а встроенный адрес Ethernet хранится в контроллере Ethernet.

Пакеты Ethernet имеют 14-октетный заголовок, включающий адреса «кому» и «от кого». Ethernet не слишком безопасен: существует возможность отправить пакеты сразу в два адреса, что позволяет кому-то наблюдать за вашими действиями. Важно помнить, что Ethernet не связан напрямую с Интернетом. Хост, подключённый одновременно к Ethernet и к Интернету, должен иметь и Ethernet-соединение, и интернет-сервер.

ARP: ARP преобразует IP-адрес в Ethernet-адрес. Для преобразования адресов используется таблица (называемая ARP Table). Поэтому вы никогда не узнаете, что подключены к Ethernet — вы будете подключаться к IP-адресу.

Выше приведено весьма краткое описание нескольких интернет-протоколов. Если вы хотите получить больше информации, её можно найти через anonymous ftp на нескольких хостах. Вот список RFC по теме протоколов:

```
lilac.berkeley.edu
  ^       ^       ^
  |       |       |
  |       |       |____   "edu" указывает, что хост находится под эгидой
  |       |               организации, связанной с образованием. Это домен
  |       |               верхнего уровня.
```

```
|      |
|      |___________  "berkeley" — домен второго уровня. Указывает, что
|                    речь идёт об организации в составе Калифорнийского
|                    университета в Беркли.
|
|___________________  "lilac" — домен третьего уровня. Указывает, что
                      локальное имя хоста — 'lilac'.
```

10. Имена хостов и адреса

Интернет-адреса длинны и трудны для запоминания (например, 128.128.57.83), поэтому мы используем имена хостов. Все хосты, зарегистрированные в Интернете, должны иметь имена, отражающие домены, в которых они зарегистрированы. Такие имена называются Fully Qualified Domain Names (FQDN). Разберём имя по составляющим:

		____ "edu" указывает, что хост находится под эгидой
	организации, связанной с образованием. Это домен	
	верхнего уровня.	
	_____ "berkeley" — домен второго уровня. Указывает, что	
речь идёт об организации в составе Калифорнийского		
университета в Беркли.		
_____ "lilac" — домен третьего уровня. Указывает, что		

Распространённые домены верхнего уровня:

Домен	Значение
COM	Коммерческие предприятия
EDU	Образовательные учреждения
GOV	Невоенные государственные органы
MIL	Военные (несекретные)
NET	Сетевые организации
ORG	Некоммерческие организации

Сетевой адрес — это числовой адрес хоста, шлюза или TAC. Адреса состоят из четырёх десятичных чисел, разделённых точкой.

Существуют три наиболее употребительных класса: Class A, Class B и Class C.

```
Class A  -  от '0'    до  '127'
Class B  -  от '128'  до  '191'
Class C  -  от '192'  до  '223'
```

Class A — предназначен для хостов MILNET. Первая часть адреса содержит номер сети. Вторая — номер физического порта PSN. Третья — номер логического порта; поскольку хост находится в MILNET, это хост MILNET. Четвёртая — номер PSN. Например, `29.34.0.9`: «29» — номер сети, «34» — порт, «9» — номер PSN.

Class B — для интернет-хостов. Первые два «блока» — сетевая часть, следующие два — локальный порт.

```
128.28.82.1
  \_/   \_/
   |     |_____ Локальная часть адреса
   |
   |___________ Часть, определяющая принадлежность к сети.
```

Class C — первые три «блока» — сетевая часть, последний — локальный порт.

```
193.43.91.1
   \_|_/  |_____ Локальный адрес
     |
     |__________ Адрес сети
```

FEDIX — Информационный сервис онлайн

Автор: Сотрудники FEDIX

Что такое FEDIX?

FEDIX — это онлайн-информационный сервис, связывающий сообщество высшего образования с федеральным правительством в целях содействия исследованиям, образованию и предоставлению услуг. Система обеспечивает колледжи, университеты и другие исследовательские организации точными и актуальными сведениями о федеральных ведомствах.

Использование FEDIX не требует НИ РЕГИСТРАЦИОННЫХ ВЗНОСОВ, НИ ПЛАТЫ ЗА ДОСТУП. Единственные расходы — оплата телефонного звонка.

FEDIX ежедневно обновляет информацию по следующим темам:

• Федеральные ПРОГРАММЫ В ОБЛАСТИ ОБРАЗОВАНИЯ И ИССЛЕДОВАНИЙ (включая описания, условия участия, финансирование, сроки подачи заявок).
• СТИПЕНДИИ, ГРАНТЫ И СУБСИДИИ
• Доступное бывшее в употреблении государственное ИССЛЕДОВАТЕЛЬСКОЕ ОБОРУДОВАНИЕ
• Новые источники финансирования для конкретных исследовательских и образовательных программ из COMMERCE BUSINESS DAILY, FEDERAL REGISTER и других источников.
• Исследовательские и образовательные программы ПОМОЩИ МЕНЬШИНСТВАМ
• НОВОСТИ И ТЕКУЩИЕ СОБЫТИЯ в участвующих ведомствах
• ОБЩАЯ ИНФОРМАЦИЯ: история ведомства, бюджет, организационная структура, формулировка миссии и т.д.

Участвующие ведомства

В настоящее время FEDIX предоставляет сведения о 7 федеральных ведомствах, разбитых на 2 общие категории:

1. Исчерпывающая информация о ведомствах в области образования и исследований:
• Министерство энергетики (DOE)
• Управление военно-морских исследований (ONR)
• Национальное управление по аэронавтике и исследованию космического пространства (NASA)
• Федеральное авиационное управление (FAA)

2. Информация о программах помощи меньшинствам:
• Национальный научный фонд (NSF)
• Министерство жилищного строительства и городского развития (HUD)
• Министерство торговли (DOC)

В будущем к FEDIX планируется присоединение дополнительных государственных ведомств.

Требования к аппаратному и программному обеспечению

Доступ к системе возможен с любого микрокомпьютера с коммуникационным программным обеспечением (или простого терминала) и модема, работающего на скорости 1200 или 2400 бод.

Часы работы

Система работает 24 часа в сутки, 7 дней в неделю. Исключения составляют периодическое обновление системы или техническое обслуживание.

Телефонные номера

• Компьютер (линия данных): 301-258-0953 или 1-800-232-4879
• HELPLINE (техническая помощь): 301-975-0103

Линия HELPLINE (для вопросов и комментариев) работает с понедельника по пятницу с 8:30 до 16:30 по восточному летнему времени, кроме федеральных праздников.

Функциональные возможности системы

Несмотря на широкий спектр функций поиска, просмотра и загрузки, система проста в использовании. Следующие возможности обеспечивают быстрый и удобный доступ к базам данных ведомств:

Меню
Информация в системе организована в виде иерархических меню с ветвлением. Выбирая нужные пункты меню (по НОМЕРУ ПУНКТА или двухбуквенному КОДУ МЕНЮ), можно начать с главного меню FEDIX и последовательно переходить через промежуточные меню к нужному подменю. Однако если вы уже знаете код нужного меню, можно пропустить промежуточные шаги и сразу перейти к нему, введя код в приглашении.

Экраны помощи доступны для ключевых меню и вызываются вводом символа '?' в приглашении.

Захват данных
Если вы используете микрокомпьютер с коммуникационным программным обеспечением, ваша система, скорее всего, способна сохранять («захватывать») информацию по мере её отображения на экране. Включив режим захвата, вы сможете просматривать сведения из баз данных и сохранять их в файл на своём компьютере для последующей печати. Это может быть удобно в тех случаях, когда загрузка файлов нежелательна. Инструкции по активации функции захвата смотрите в документации к вашему коммуникационному программному обеспечению.

Загрузка файлов
По всей системе доступны опции поиска, просмотра списков и загрузки файлов с информацией по конкретным темам. Функция загрузки позволяет быстро получать на ваш компьютер текстовые файлы (ASCII) или сжатые самораспаковывающиеся ASCII-файлы для последующего использования в удобное время. Текстовые файлы в формате ASCII с расширением «.MAC» предназначены для загрузки пользователями Macintosh. Сжатые ASCII-файлы с расширением «.EXE» могут загружаться пользователями IBM-совместимых компьютеров. Тем не менее ваша система должна поддерживать передачу файлов (смотрите документацию к коммуникационному программному обеспечению).

Почта

Функция электронной доски объявлений позволяет отправлять и получать сообщения, адресованные ТОЛЬКО СИСТЕМНОМУ ОПЕРАТОРУ. Эта функция НЕ обеспечивает переписку между пользователями. С её помощью можно задавать вопросы о работе системы, получать полезные советы от системного оператора и т.д.

Меню служебных функций

Меню служебных функций, доступное из главного меню FEDIX, позволяет изменять информацию о пользователе, устанавливать приоритетность ведомств для просмотра, выполнять поиск и загрузку информации о ведомствах, задавать меню по умолчанию при входе в систему и устанавливать протокол передачи файлов для загрузки.

Указатель ключевой информации на FEDIX

Ниже приведена ключевая информация по каждому ведомству с указанием кода меню, из которого к ней можно получить доступ. Обратите внимание, что данный список не является исчерпывающим — на FEDIX доступно значительно больше информации, чем здесь перечислено.

ВЕДОМСТВО/БАЗА ДАННЫХ	КОД МЕНЮ
МИНИСТЕРСТВО ЭНЕРГЕТИКИ (DOE)/DOEINFO	
Доступное б/у исследовательское оборудование	:EG:
Информация об исследовательских программах	:IX:
Информация об образовательных программах	:GA:
Поиск/Список/Загрузка информации о программах	:IX:
Информация об исследовательских и учебных реакторах	:RT:
Уведомления о закупках	:MM:
Текущие события	:DN:
НАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ ПО АЭРОНАВТИКЕ И ИССЛЕДОВАНИЮ КОСМОСА/NASINFO	
Информация об исследовательских программах	:RP:
Информация об образовательных программах	:EA:
Поиск/Список/Загрузка информации о программах	:NN:
Описание/Деятельность космических центров	:SC:
Уведомления о закупках	:EV:
Руководство по подготовке предложений и присуждению контрактов	:NA:
УПРАВЛЕНИЕ ВОЕННО-МОРСКИХ ИССЛЕДОВАНИЙ/ONRINFO	
Информация об исследовательских программах	:RY:, :AR:
Специальные программы	:ON:
Поиск/Список/Загрузка информации о программах	:NR:
Описание/Деятельность лабораторий и других объектов ONR	:LB:
Уведомления о закупках (Широкие ведомственные объявления, Запросы предложений и т.д.)	:NE:
Информация о подготовке и администрировании контрактов, грантов, предложений	:AD:
ФЕДЕРАЛЬНОЕ АВИАЦИОННОЕ УПРАВЛЕНИЕ/FAAINFO	
Информация об образовательных программах — доколледжный уровень	:FE:
Программы авиационного образования для меньшинств	:FY:
Поиск/Список/Загрузка информации о программах	:FF:
Ресурсы авиационного образования (бюллетени, фильмы/видео, публикации)	:FR:
Контакты в сфере авиационного образования (правительство, промышленность, академия, ассоциации)	:FO:
Информация об учебных программах авиационной науки для колледжей	:FC:
Уведомление о закупках	:FP:
Запланированные конкурентные и неконкурентные закупки на текущий финансовый год	:F1:
Информация о вакансиях	:FN:
Текущие события	:FV:
МЕНЬШИНСТВА/MININFO	

Министерство торговли США
 Программы помощи меньшинствам в исследованиях/образовании :CP:
 Уведомления о закупках (ВСЕ уведомления по ведомству) :M1:
 Текущие события :M1:
 Контакты по делам меньшинств :M1:

Министерство энергетики
 Программы помощи меньшинствам в исследованиях/образовании :EP:
 Уведомления о закупках (ВСЕ уведомления по ведомству) :M2:
 Текущие события :M2:
 Контакты по делам меньшинств :M2:

Министерство жилищного строительства и городского развития США
 Программы помощи меньшинствам в исследованиях/образовании :HP:
 Уведомления о закупках (ВСЕ уведомления по ведомству) :M3:
 Текущие события :M3:
 Контакты по делам меньшинств :M3:

Национальное управление по аэронавтике и исследованию космоса
 Программы помощи меньшинствам в исследованиях/образовании :NP:
 Уведомления о закупках (ВСЕ уведомления по ведомству) :M4:
 Текущие события :M4:
 Контакты по делам меньшинств :M4:

Национальный научный фонд
 Программы помощи меньшинствам в исследованиях/образовании :SP:
 Уведомления о закупках (ВСЕ уведомления по ведомству) :M5:
 Бюджетная информация :SB:
 Бюллетень NSF :M5:
 Контакты по делам меньшинств :M5:

Справочный список LATA

Автор: Infinite Loop

Официальные идентификационные номера LATA (Local Access and Transport Area — зона местного доступа и транспортировки) телефонных сетей Соединённых Штатов:

[Таблица из 161 записи — опущена]

ШТАТ	НАЗВАНИЕ	НОМЕР
AK	ALASKA	832
AL	BIRMINGHAM	476
AL	HUNTSVILLE	477
AL	MONTGOMERY	478
AL	MOBILE	480
AR	FORT SMITH	526
AR	LITTLE ROCK	528
AR	PINE BLUFF	530
AZ	PHOENIX	666
AZ	TUCSON	668
AZ	NAVAJO RESERVATION	980
CA	SAN FRANCISCO	722
CA	CHICO	724
CA	SACRAMENTO	726
CA	FRESNO	728
CA	LOS ANGELES	730
CA	SAN DIEGO	732
CA	BAKERSFIELD	734
CA	MONTEREY	736
CA	STOCKTON	738
CA	SAN LUIS OBISPO	740

CA	PALM SPRINGS	973
CO	DENVER	656
CO	COLORADO SPRINGS	658
CT	CONNECTICUT <SNET>	920
DC	WASHINGTON	236
FL	PENSACOLA	448
FL	PANAMA CITY	450
FL	JACKSONVILLE	452
FL	GAINESVILLE	454
FL	DAYTONA BEACH	456
FL	ORLANDO	458
FL	SOUTHEAST	460
FL	FORT MYERS	939
FL	GULF COAST	952
FL	TALLAHASSEE	953
GA	ATLANTA	438
GA	SAVANNAH	440
GA	AUGUSTA	442
GA	ALBANY	444
GA	MACON	446
HI	HAWAII	834
IA	SIOUX CITY	630
IA	DES MOINES	632
IA	DAVENPORT	634
IA	CEDAR RAPIDS	635
ID	IDAHO	652
ID	COEUR D'ALENE	960

IL	CHICAGO	358
IL	ROCKFORD	360
IL	CAIRO	362
IL	STERLING	364
IL	FORREST	366
IL	PEORIA	368
IL	CHAMPAIGN	370
IL	SPRINGFIELD	372
IL	QUINCY	374
IL	MATTOON	976
IL	GALESBURG	977
IL	OLNEY	978
IN	EVANSVILLE	330
IN	SOUTH BEND	332
IN	AUBURN/HUNTINGTON	334
IN	INDIANAPOLIS	336
IN	BLOOMINGTON	338
IN	RICHMOND	937
IN	TERRE HAUTE	938
KS	WICHITA	532
KS	TOPEKA	534
KY	LOUISVILLE	462
KY	OWENSBORO	464
KY	WINCHESTER	466
LA	SHREVEPORT	486
LA	LAFAYETTE	488
LA	NEW ORLEANS	490

LA	BATON ROUGE	492
MA	WESTERN MASSACHUSETTS	126
MA	EASTERN MASSACHUSETTS	128
MD	BALTIMORE	238
MD	HAGERSTOWN	240
MD	SALISBURY	242
ME	MAINE	120
MI	DETROIT	340
MI	UPPER PENINSULA	342
MI	SAGINAW	344
MI	LANSING	346
MI	GRAND RAPIDS	348
MN	ROCHESTER	620
MN	DULUTH	624
MN	ST CLOUD	626
MN	MINNEAPOLIS	628
MO	ST LOUIS	520
MO	WESTPHALIA	521
MO	SPRINGFIELD	522
MO	KANSAS CITY	524
MS	JACKSON	482
MS	BILOXI	484
MT	GREAT FALLS	648
MT	BILLINGS	650
MT	KALISPELL	963
NC	ASHEVILLE	420
NC	CHARLOTTE	422

NC	GREENSBORO	424
NC	RALEIGH	426
NC	WILMINGTON	428
NC	FAYETTEVILLE	949
NC	ROCKY MOUNT	951
ND	FARGO	636
ND	BISMARCK	638
NE	OMAHA	644
NE	GRAND ISLAND	646
NE	LINCOLN	958
NH	NEW HAMPSHIRE	122
NJ	ATLANTIC COASTAL	220
NJ	DELAWARE VALLEY	222
NJ	NORTH JERSEY	224
NM	NEW MEXICO	664
NV	RENO	720
NV	PAHRUMP	721
NY	NEW YORK METRO	132
NY	POUGHKEEPSIE	133
NY	ALBANY	134
NY	SYRACUSE	136
NY	BINGHAMTON	138
NY	BUFFALO	140
NY	FISHERS ISLAND	921
NY	ROCHESTER	974
OH	CLEVELAND	320
OH	YOUNGSTOWN	322

OH	COLUMBUS	324
OH	AKRON	325
OH	TOLEDO	326
OH	DAYTON	328
OH	CINCINNATI BELL	922
OH	MANSFIELD	923
OK	OKLAHOMA CITY	536
OK	TULSA	538
OR	EUGENE	670
OR	PORTLAND	672
PA	CAPITAL	226
PA	PHILADELPHIA	228
PA	ALTOONA	230
PA	NORTHEAST	232
PA	PITTSBURGH	234
PA	ERIE	924
PR	PUERTO RICO	820
RI	RHODE ISLAND	130
SC	GREENVILLE	430
SC	FLORENCE	432
SC	COLUMBIA	434
SC	CHARLESTON	436
SD	SOUTH DAKOTA	640
TN	MEMPHIS	468
TN	NASHVILLE	470
TN	CHATTANOOGA	472
TN	KNOXVILLE	474

TN	BRISTOL	956
TX	EL PASO	540
TX	MIDLAND	542
TX	LUBBOCK	544
TX	AMARILLO	546
TX	WICHITA FALLS	548
TX	ABILENE	550
TX	DALLAS	552
TX	LONGVIEW	554
TX	WACO	556
TX	AUSTIN	558
TX	HOUSTON	560
TX	BEAUMONT	562
TX	CORPUS CHRISTI	564
TX	SAN ANTONIO	566
TX	BROWNSVILLE	568
TX	HEARNE	570
TX	SAN ANGELO	961
US	MIDWAY/WAKE	836
UT	UTAH	660
UT	NAVAJO RESERVATION	981
VA	ROANOKE	244
VA	CULPEPER	246
VA	RICHMOND	248
VA	LYNCHBURG	250
VA	NORFOLK	252
VA	HARRISONBURG	927

VA	CHARLOTTESVILLE	928
VA	EDINBURG	929
VI	US VIRGIN ISLANDS	822
VT	VERMONT	124
WA	SEATTLE	674
WA	SPOKANE	676
WI	NORTHEAST	350
WI	NORTHWEST	352
WI	SOUTHWEST	354
WI	SOUTHEAST	356
WV	CHARLESTON	254
WV	CLARKSBURG	256
WV	BLUEFIELD	932
WY	WYOMING	654

ШТАТ	НАЗВАНИЕ	НОМЕР
AK	ALASKA	832
AL	BIRMINGHAM	476
AL	HUNTSVILLE	477
AL	MONTGOMERY	478
AL	MOBILE	480
AR	FORT SMITH	526
AR	LITTLE ROCK	528
AR	PINE BLUFF	530
AZ	PHOENIX	666
AZ	TUCSON	668
AZ	NAVAJO RESERVATION	980
CA	SAN FRANCISCO	722

CA	CHICO	724
CA	SACRAMENTO	726
CA	FRESNO	728
CA	LOS ANGELES	730
CA	SAN DIEGO	732
CA	BAKERSFIELD	734
CA	MONTEREY	736
CA	STOCKTON	738
CA	SAN LUIS OBISPO	740
CA	PALM SPRINGS	973
CO	DENVER	656
CO	COLORADO SPRINGS	658
CT	CONNECTICUT <SNET>	920
DC	WASHINGTON	236
FL	PENSACOLA	448
FL	PANAMA CITY	450
FL	JACKSONVILLE	452
FL	GAINESVILLE	454
FL	DAYTONA BEACH	456
FL	ORLANDO	458
FL	SOUTHEAST	460
FL	FORT MYERS	939
FL	GULF COAST	952
FL	TALLAHASSEE	953
GA	ATLANTA	438
GA	SAVANNAH	440
GA	AUGUSTA	442

GA	ALBANY	444
GA	MACON	446
HI	HAWAII	834
IA	SIOUX CITY	630
IA	DES MOINES	632
IA	DAVENPORT	634
IA	CEDAR RAPIDS	635
ID	IDAHO	652
ID	COEUR D'ALENE	960
IL	CHICAGO	358
IL	ROCKFORD	360
IL	CAIRO	362
IL	STERLING	364
IL	FORREST	366
IL	PEORIA	368
IL	CHAMPAIGN	370
IL	SPRINGFIELD	372
IL	QUINCY	374
IL	MATTOON	976
IL	GALESBURG	977
IL	OLNEY	978
IN	EVANSVILLE	330
IN	SOUTH BEND	332
IN	AUBURN/HUNTINGTON	334
IN	INDIANAPOLIS	336
IN	BLOOMINGTON	338
IN	RICHMOND	937

IN	TERRE HAUTE	938
KS	WICHITA	532
KS	TOPEKA	534
KY	LOUISVILLE	462
KY	OWENSBORO	464
KY	WINCHESTER	466
LA	SHREVEPORT	486
LA	LAFAYETTE	488
LA	NEW ORLEANS	490
LA	BATON ROUGE	492
MA	WESTERN MASSACHUSETTS	126
MA	EASTERN MASSACHUSETTS	128
MD	BALTIMORE	238
MD	HAGERSTOWN	240
MD	SALISBURY	242
ME	MAINE	120
MI	DETROIT	340
MI	UPPER PENINSULA	342
MI	SAGINAW	344
MI	LANSING	346
MI	GRAND RAPIDS	348
MN	ROCHESTER	620
MN	DULUTH	624
MN	ST CLOUD	626
MN	MINNEAPOLIS	628
MO	ST LOUIS	520
MO	WESTPHALIA	521

MO	SPRINGFIELD	522
MO	KANSAS CITY	524
MS	JACKSON	482
MS	BILOXI	484
MT	GREAT FALLS	648
MT	BILLINGS	650
MT	KALISPELL	963
NC	ASHEVILLE	420
NC	CHARLOTTE	422
NC	GREENSBORO	424
NC	RALEIGH	426
NC	WILMINGTON	428
NC	FAYETTEVILLE	949
NC	ROCKY MOUNT	951
ND	FARGO	636
ND	BISMARCK	638
NE	OMAHA	644
NE	GRAND ISLAND	646
NE	LINCOLN	958
NH	NEW HAMPSHIRE	122
NJ	ATLANTIC COASTAL	220
NJ	DELAWARE VALLEY	222
NJ	NORTH JERSEY	224
NM	NEW MEXICO	664
NV	RENO	720
NV	PAHRUMP	721
NY	NEW YORK METRO	132

NY	POUGHKEEPSIE	133
NY	ALBANY	134
NY	SYRACUSE	136
NY	BINGHAMTON	138
NY	BUFFALO	140
NY	FISHERS ISLAND	921
NY	ROCHESTER	974
OH	CLEVELAND	320
OH	YOUNGSTOWN	322
OH	COLUMBUS	324
OH	AKRON	325
OH	TOLEDO	326
OH	DAYTON	328
OH	CINCINNATI BELL	922
OH	MANSFIELD	923
OK	OKLAHOMA CITY	536
OK	TULSA	538
OR	EUGENE	670
OR	PORTLAND	672
PA	CAPITAL	226
PA	PHILADELPHIA	228
PA	ALTOONA	230
PA	NORTHEAST	232
PA	PITTSBURGH	234
PA	ERIE	924
PR	PUERTO RICO	820
RI	RHODE ISLAND	130

SC	GREENVILLE	430
SC	FLORENCE	432
SC	COLUMBIA	434
SC	CHARLESTON	436
SD	SOUTH DAKOTA	640
TN	MEMPHIS	468
TN	NASHVILLE	470
TN	CHATTANOOGA	472
TN	KNOXVILLE	474
TN	BRISTOL	956
TX	EL PASO	540
TX	MIDLAND	542
TX	LUBBOCK	544
TX	AMARILLO	546
TX	WICHITA FALLS	548
TX	ABILENE	550
TX	DALLAS	552
TX	LONGVIEW	554
TX	WACO	556
TX	AUSTIN	558
TX	HOUSTON	560
TX	BEAUMONT	562
TX	CORPUS CHRISTI	564
TX	SAN ANTONIO	566
TX	BROWNSVILLE	568
TX	HEARNE	570
TX	SAN ANGELO	961

US	MIDWAY/WAKE	836
UT	UTAH	660
UT	NAVAJO RESERVATION	981
VA	ROANOKE	244
VA	CULPEPER	246
VA	RICHMOND	248
VA	LYNCHBURG	250
VA	NORFOLK	252
VA	HARRISONBURG	927
VA	CHARLOTTESVILLE	928
VA	EDINBURG	929
VI	US VIRGIN ISLANDS	822
VT	VERMONT	124
WA	SEATTLE	674
WA	SPOKANE	676
WI	NORTHEAST	350
WI	NORTHWEST	352
WI	SOUTHWEST	354
WI	SOUTHEAST	356
WV	CHARLESTON	254
WV	CLARKSBURG	256
WV	BLUEFIELD	932
WY	WYOMING	654

ШТАТ	НАЗВАНИЕ	НОМЕР
AK	ALASKA	832
AL	BIRMINGHAM	476
AL	HUNTSVILLE	477

AL	MONTGOMERY	478
AL	MOBILE	480
AR	FORT SMITH	526
AR	LITTLE ROCK	528
AR	PINE BLUFF	530
AZ	PHOENIX	666
AZ	TUCSON	668
AZ	NAVAJO RESERVATION	980
CA	SAN FRANCISCO	722
CA	CHICO	724
CA	SACRAMENTO	726
CA	FRESNO	728
CA	LOS ANGELES	730
CA	SAN DIEGO	732
CA	BAKERSFIELD	734
CA	MONTEREY	736
CA	STOCKTON	738
CA	SAN LUIS OBISPO	740
CA	PALM SPRINGS	973
CO	DENVER	656
CO	COLORADO SPRINGS	658
CT	CONNECTICUT <SNET>	920
DC	WASHINGTON	236
FL	PENSACOLA	448
FL	PANAMA CITY	450
FL	JACKSONVILLE	452
FL	GAINESVILLE	454

FL	DAYTONA BEACH	456
FL	ORLANDO	458
FL	SOUTHEAST	460
FL	FORT MYERS	939
FL	GULF COAST	952
FL	TALLAHASSEE	953
GA	ATLANTA	438
GA	SAVANNAH	440
GA	AUGUSTA	442
GA	ALBANY	444
GA	MACON	446
HI	HAWAII	834
IA	SIOUX CITY	630
IA	DES MOINES	632
IA	DAVENPORT	634
IA	CEDAR RAPIDS	635
ID	IDAHO	652
ID	COEUR D'ALENE	960
IL	CHICAGO	358
IL	ROCKFORD	360
IL	CAIRO	362
IL	STERLING	364
IL	FORREST	366
IL	PEORIA	368
IL	CHAMPAIGN	370
IL	SPRINGFIELD	372
IL	QUINCY	374

IL	MATTOON	976
IL	GALESBURG	977
IL	OLNEY	978
IN	EVANSVILLE	330
IN	SOUTH BEND	332
IN	AUBURN/HUNTINGTON	334
IN	INDIANAPOLIS	336
IN	BLOOMINGTON	338
IN	RICHMOND	937
IN	TERRE HAUTE	938
KS	WICHITA	532
KS	TOPEKA	534
KY	LOUISVILLE	462
KY	OWENSBORO	464
KY	WINCHESTER	466
LA	SHREVEPORT	486
LA	LAFAYETTE	488
LA	NEW ORLEANS	490
LA	BATON ROUGE	492
MA	WESTERN MASSACHUSETTS	126
MA	EASTERN MASSACHUSETTS	128
MD	BALTIMORE	238
MD	HAGERSTOWN	240
MD	SALISBURY	242
ME	MAINE	120
MI	DETROIT	340
MI	UPPER PENINSULA	342

MI	SAGINAW	344
MI	LANSING	346
MI	GRAND RAPIDS	348
MN	ROCHESTER	620
MN	DULUTH	624
MN	ST CLOUD	626
MN	MINNEAPOLIS	628
MO	ST LOUIS	520
MO	WESTPHALIA	521
MO	SPRINGFIELD	522
MO	KANSAS CITY	524
MS	JACKSON	482
MS	BILOXI	484
MT	GREAT FALLS	648
MT	BILLINGS	650
MT	KALISPELL	963
NC	ASHEVILLE	420
NC	CHARLOTTE	422
NC	GREENSBORO	424
NC	RALEIGH	426
NC	WILMINGTON	428
NC	FAYETTEVILLE	949
NC	ROCKY MOUNT	951
ND	FARGO	636
ND	BISMARCK	638
NE	OMAHA	644
NE	GRAND ISLAND	646

NE	LINCOLN	958
NH	NEW HAMPSHIRE	122
NJ	ATLANTIC COASTAL	220
NJ	DELAWARE VALLEY	222
NJ	NORTH JERSEY	224
NM	NEW MEXICO	664
NV	RENO	720
NV	PAHRUMP	721
NY	NEW YORK METRO	132
NY	POUGHKEEPSIE	133
NY	ALBANY	134
NY	SYRACUSE	136
NY	BINGHAMTON	138
NY	BUFFALO	140
NY	FISHERS ISLAND	921
NY	ROCHESTER	974
OH	CLEVELAND	320
OH	YOUNGSTOWN	322
OH	COLUMBUS	324
OH	AKRON	325
OH	TOLEDO	326
OH	DAYTON	328
OH	CINCINNATI BELL	922
OH	MANSFIELD	923
OK	OKLAHOMA CITY	536
OK	TULSA	538
OR	EUGENE	670

OR	PORTLAND	672
PA	CAPITAL	226
PA	PHILADELPHIA	228
PA	ALTOONA	230
PA	NORTHEAST	232
PA	PITTSBURGH	234
PA	ERIE	924
PR	PUERTO RICO	820
RI	RHODE ISLAND	130
SC	GREENVILLE	430
SC	FLORENCE	432
SC	COLUMBIA	434
SC	CHARLESTON	436
SD	SOUTH DAKOTA	640
TN	MEMPHIS	468
TN	NASHVILLE	470
TN	CHATTANOOGA	472
TN	KNOXVILLE	474
TN	BRISTOL	956
TX	EL PASO	540
TX	MIDLAND	542
TX	LUBBOCK	544
TX	AMARILLO	546
TX	WICHITA FALLS	548
TX	ABILENE	550
TX	DALLAS	552
TX	LONGVIEW	554

TX	WACO	556
TX	AUSTIN	558
TX	HOUSTON	560
TX	BEAUMONT	562
TX	CORPUS CHRISTI	564
TX	SAN ANTONIO	566
TX	BROWNSVILLE	568
TX	HEARNE	570
TX	SAN ANGELO	961
US	MIDWAY/WAKE	836
UT	UTAH	660
UT	NAVAJO RESERVATION	981
VA	ROANOKE	244
VA	CULPEPER	246
VA	RICHMOND	248
VA	LYNCHBURG	250
VA	NORFOLK	252
VA	HARRISONBURG	927
VA	CHARLOTTESVILLE	928
VA	EDINBURG	929
VI	US VIRGIN ISLANDS	822
VT	VERMONT	124
WA	SEATTLE	674
WA	SPOKANE	676
WI	NORTHEAST	350
WI	NORTHWEST	352
WI	SOUTHWEST	354

WI	SOUTHEAST	356
WV	CHARLESTON	254
WV	CLARKSBURG	256
WV	BLUEFIELD	932
WY	WYOMING	654

ШТАТ	НАЗВАНИЕ	НОМЕР
AK	ALASKA	832
AL	BIRMINGHAM	476
AL	HUNTSVILLE	477
AL	MONTGOMERY	478
AL	MOBILE	480
AR	FORT SMITH	526
AR	LITTLE ROCK	528
AR	PINE BLUFF	530
AZ	PHOENIX	666
AZ	TUCSON	668
AZ	NAVAJO RESERVATION	980
CA	SAN FRANCISCO	722
CA	CHICO	724
CA	SACRAMENTO	726
CA	FRESNO	728
CA	LOS ANGELES	730
CA	SAN DIEGO	732
CA	BAKERSFIELD	734
CA	MONTEREY	736
CA	STOCKTON	738
CA	SAN LUIS OBISPO	740

CA	PALM SPRINGS	973
CO	DENVER	656
CO	COLORADO SPRINGS	658
CT	CONNECTICUT <SNET>	920
DC	WASHINGTON	236
FL	PENSACOLA	448
FL	PANAMA CITY	450
FL	JACKSONVILLE	452
FL	GAINESVILLE	454
FL	DAYTONA BEACH	456
FL	ORLANDO	458
FL	SOUTHEAST	460
FL	FORT MYERS	939
FL	GULF COAST	952
FL	TALLAHASSEE	953
GA	ATLANTA	438
GA	SAVANNAH	440
GA	AUGUSTA	442
GA	ALBANY	444
GA	MACON	446
HI	HAWAII	834
IA	SIOUX CITY	630
IA	DES MOINES	632
IA	DAVENPORT	634
IA	CEDAR RAPIDS	635
ID	IDAHO	652
ID	COEUR D'ALENE	960

IL	CHICAGO	358
IL	ROCKFORD	360
IL	CAIRO	362
IL	STERLING	364
IL	FORREST	366
IL	PEORIA	368
IL	CHAMPAIGN	370
IL	SPRINGFIELD	372
IL	QUINCY	374
IL	MATTOON	976
IL	GALESBURG	977
IL	OLNEY	978
IN	EVANSVILLE	330
IN	SOUTH BEND	332
IN	AUBURN/HUNTINGTON	334
IN	INDIANAPOLIS	336
IN	BLOOMINGTON	338
IN	RICHMOND	937
IN	TERRE HAUTE	938
KS	WICHITA	532
KS	TOPEKA	534
KY	LOUISVILLE	462
KY	OWENSBORO	464
KY	WINCHESTER	466
LA	SHREVEPORT	486
LA	LAFAYETTE	488
LA	NEW ORLEANS	490

LA	BATON ROUGE	492
MA	WESTERN MASSACHUSETTS	126
MA	EASTERN MASSACHUSETTS	128
MD	BALTIMORE	238
MD	HAGERSTOWN	240
MD	SALISBURY	242
ME	MAINE	120
MI	DETROIT	340
MI	UPPER PENINSULA	342
MI	SAGINAW	344
MI	LANSING	346
MI	GRAND RAPIDS	348
MN	ROCHESTER	620
MN	DULUTH	624
MN	ST CLOUD	626
MN	MINNEAPOLIS	628
MO	ST LOUIS	520
MO	WESTPHALIA	521
MO	SPRINGFIELD	522
MO	KANSAS CITY	524
MS	JACKSON	482
MS	BILOXI	484
MT	GREAT FALLS	648
MT	BILLINGS	650
MT	KALISPELL	963
NC	ASHEVILLE	420
NC	CHARLOTTE	422

NC	GREENSBORO	424
NC	RALEIGH	426
NC	WILMINGTON	428
NC	FAYETTEVILLE	949
NC	ROCKY MOUNT	951
ND	FARGO	636
ND	BISMARCK	638
NE	OMAHA	644
NE	GRAND ISLAND	646
NE	LINCOLN	958
NH	NEW HAMPSHIRE	122
NJ	ATLANTIC COASTAL	220
NJ	DELAWARE VALLEY	222
NJ	NORTH JERSEY	224
NM	NEW MEXICO	664
NV	RENO	720
NV	PAHRUMP	721
NY	NEW YORK METRO	132
NY	POUGHKEEPSIE	133
NY	ALBANY	134
NY	SYRACUSE	136
NY	BINGHAMTON	138
NY	BUFFALO	140
NY	FISHERS ISLAND	921
NY	ROCHESTER	974
OH	CLEVELAND	320
OH	YOUNGSTOWN	322

OH	COLUMBUS	324
OH	AKRON	325
OH	TOLEDO	326
OH	DAYTON	328
OH	CINCINNATI BELL	922
OH	MANSFIELD	923
OK	OKLAHOMA CITY	536
OK	TULSA	538
OR	EUGENE	670
OR	PORTLAND	672
PA	CAPITAL	226
PA	PHILADELPHIA	228
PA	ALTOONA	230
PA	NORTHEAST	232
PA	PITTSBURGH	234
PA	ERIE	924
PR	PUERTO RICO	820
RI	RHODE ISLAND	130
SC	GREENVILLE	430
SC	FLORENCE	432
SC	COLUMBIA	434
SC	CHARLESTON	436
SD	SOUTH DAKOTA	640
TN	MEMPHIS	468
TN	NASHVILLE	470
TN	CHATTANOOGA	472
TN	KNOXVILLE	474

TN	BRISTOL	956
TX	EL PASO	540
TX	MIDLAND	542
TX	LUBBOCK	544
TX	AMARILLO	546
TX	WICHITA FALLS	548
TX	ABILENE	550
TX	DALLAS	552
TX	LONGVIEW	554
TX	WACO	556
TX	AUSTIN	558
TX	HOUSTON	560
TX	BEAUMONT	562
TX	CORPUS CHRISTI	564
TX	SAN ANTONIO	566
TX	BROWNSVILLE	568
TX	HEARNE	570
TX	SAN ANGELO	961
US	MIDWAY/WAKE	836
UT	UTAH	660
UT	NAVAJO RESERVATION	981
VA	ROANOKE	244
VA	CULPEPER	246
VA	RICHMOND	248
VA	LYNCHBURG	250
VA	NORFOLK	252
VA	HARRISONBURG	927

VA	CHARLOTTESVILLE	928
VA	EDINBURG	929
VI	US VIRGIN ISLANDS	822
VT	VERMONT	124
WA	SEATTLE	674
WA	SPOKANE	676
WI	NORTHEAST	350
WI	NORTHWEST	352
WI	SOUTHWEST	354
WI	SOUTHEAST	356
WV	CHARLESTON	254
WV	CLARKSBURG	256
WV	BLUEFIELD	932
WY	WYOMING	654

Международные бесплатные звонки, звонки по местному тарифу и специальные платные услуги

Автор: The Trunk Terminator

Ниже приведены коды доступа и номера, используемые в различных странах для бесплатных звонков и специальных платных услуг. Показанные коды набора соответствуют тому, как они набираются внутри соответствующей страны. Как правило, прямой доступ к внутренним бесплатным или специальным сетям другой страны невозможен. Там, где международный доступ доступен, он обычно осуществляется через внутренние службы, которые затем переадресуют звонок в страну назначения.

Там, где это возможно, количество цифр обозначено символом `n` (число от 2 до 8) или `x` (любая цифра). Многоточие (`...`) указывает на переменное количество дополнительных цифр или на возможные разногласия в сведениях о количестве используемых цифр.

Бесплатные услуги или услуги с оплатой по местному тарифу

Австралия

```
008 xxx xxx        Именно так Phrack Inc. рекомендует записывать
                   этот номер, чтобы отличить его от кодов зон STD,
                   которые записываются с кодами зон (0x) по
                   (0xxx) и номерами от n xxxx до nxx xxxx.

0014 ttt xxx xxx   Международный бесплатный доступ из Австралии
                   (ttt указывается как "800" или другой код
                   бесплатного доступа; либо ttt может отсутствовать
                   вовсе.

                   (Canada Direct использует 0014 881 150)
```

Бельгия

```
11 xxxx
```

Дания

```
800 xxxxx
8001 xxxx          (оплачивается как местный звонок)
```

Финляндия

```
9800 xxxxx (...)  (PTT в качестве местного оператора)
0800 xxxxx (...)  (частная телефонная компания в качестве местного оператора)
```

Звонок на 9800 стоит столько же, сколько местный (доступен из всех районов Финляндии), тогда как 0800 — действительно бесплатный и доступен из всех зон частных телеоператоров.

Франция

```
05 xxxxxx         Это за пределами кода зоны 1; из Парижа — 16 05.

05 19 xx xx       Эти номера выводят звонок за пределы Франции.

36 63 xx xx       (по местному тарифу)
```

`11` — компьютерный справочник телефонных номеров.
`12` — голосовой справочник (аналог 411 в США).

Германия (Западная)

```
0130 xxxx (...xx) Номер для доступа к AT&T — 0130-0010, для U.S. Sprint — 0130-0013.
```

Для просмотра общего списка бесплатных номеров можно взять экземпляр газеты International Herald и заглянуть в спортивный раздел — там есть реклама AT&T с номерами для звонков в США из различных стран. Нужно просто отбросить номер абонента и использовать только «код зоны».

Ирландия

```
1800 xxxxxx
1850 xxxxxx       (по местному тарифу)
```

Италия

```
167 xxxxx         (количество цифр)
```

Мы не на сто процентов уверены в длине номеров для Италии. Один из способов проверить — взять *международное* издание еженедельного журнала типа TIME: там сплошная реклама и минимум содержания. Но там периодически допускают ошибки, например, указывают парижские номера как (01) xxxxxxxx, хотя правильно — (1) xxxxxxxx.

Мексика

```
91 800 xxxxx....
```

Нидерланды

```
06-0xxx
06-0xxxxxx
06-4xx(x)          06-2229111 — прямой доступ к AT&T USA, Sprint и MCI
                   предоставляют услуги оператора по 06-022xxxx.
```

Раньше можно было позвонить на 06-022xxxx в Данию и затем использовать систему сигнализации CCITT №4 для фрикинга звонков в любую точку мира.

`06-11` — нидерландский аналог 911, звонок бесплатен с таксофонов телефонной компании; в противном случае взимается одна единица, DFL 0,15, около 0,08 доллара США. Обсуждалась возможность сделать такие звонки бесплатными с любого телефона, но я давно не следил за этими обсуждениями. Звонок на бесплатный номер с таксофона требует внесения одной монеты, которая возвращается после звонка.

Общая длина номеров варьируется от 4 до 10 цифр; тире обозначает второй сигнал готовности. Номера с префиксом 06 недоступны для звонков из-за рубежа.

Новая Зеландия

```
0800 xxx xxx
```

Это через государственного оператора — Telecom New Zealand. Clear Communications, недавно появившийся альтернативный оператор дальней связи, пока не предлагает бесплатных услуг. Когда Clear запустит такую услугу, скорее всего, она будет привязана к существующему номеру абонента (например, звоните бесплатно: 050-04-654-3210), поскольку компания не управляет выдачей номеров. На данный момент 0800 — исключительно Telecom.

Северная Америка

```
1 800 nxx xxxx     Доступность бесплатных номеров может варьироваться
                   в зависимости от региона, штата или страны
                   (не все номера 800 доступны во всех регионах).
```

Префикс `nxx` в номере 800 в настоящее время определяет, какой оператор дальней связи или компания по обслуживанию 800-номеров обработает звонок (а в некоторых случаях — и географический регион).

Испания

```
900 xxxxxx         Номер AT&T Direct в Испании: 900-99-00-11.
```

Все таксофоны кнопочные, но генерируют импульсные сигналы. Соединение устанавливается очень долго.

Швеция

```
020 xxxxxx        (без второго сигнала готовности после «020»).
```

Швейцария

```
04605 xxxx        (не бесплатный, но тарифицируется по минимальной ставке)
155 xx xx         («зелёный номер»)
```

В Швейцарии нет ничего точно эквивалентного американским номерам «800». PTT сейчас продвигает «зелёные номера» с префиксом 155. В рекламе прямых продаж по телевизору часто указывают швейцарский номер заказа в виде 155 XX XX. Например, номер доступа к MCI Call USA — 155 02 22. Существуют две проблемы:

1. При звонке с таксофона модели AZ44 (старая модель) все номера, начинающиеся с «1», воспринимаются как «служебные», и после набора 155 таксофон начинает издавать звук «кукушки». Этот звук предназначен для оповещения операторов «служебных номеров» о том, что звонящий пользуется таксофоном (защита от мошенничества). Данный звук весьма мешает при звонках в США через MCI Call USA.

2. Таксофоны нового типа TelcaStar запрограммированы на блокировку клавиатуры после набора 3 цифр «служебного номера». Раньше только номера, начинающиеся с «1», были «служебными», и все «служебные номера» состояли из 3 цифр. PTT знает об этой проблеме и, по имеющимся сведениям, обдумывает, какие инструкции выдать производителю таксофонов.

Номер прямого доступа AT&T USA — 046 05 00 11. Звонок платный, но тарифицируется по минимальной ставке. Данный номер не подвержен проблеме «звука кукушки».

Canada Direct использует 046 05 83 30.

Великобритания

```
0800 xxx xxx      (бесплатно)
0345 xxx xxx      (по местному тарифу)
```

Платные и специальные услуги

Австралия

```
0055 x yxxx       где y=0-4,8 означает, что номер действителен по всей
                          Австралии (и стоит дороже),
                      y=5   означает, что номер действителен только в пределах
                          штата,
                      y=6,7,9 означает, что номер действителен только
                          для столичного города.
```

Финляндия

```
9700 xxxxx        (под управлением PTT)
0700 xxxxx        (под управлением частного оператора)
```

Стоимость варьируется приблизительно от 0,5 до 5 долларов США в минуту.

Франция

```
36 65 xx xx       (5 единиц сообщений за один звонок продолжительностью
                   до 140 секунд)
```

Используется для различных информационных служб, а также чат-линий.

Нидерланды

```
06-9 xx...
06-321 xx...
06-8 xx...        (от 3 до 40 центов в минуту)
```

Другие коды (например, 06-9) предшествуют звонкам по специальному тарифу (аналог номеров 900 в США). Максимальная специальная ставка в настоящее время составляет DFL 0,50 в минуту.

Северная Америка

```
1 900 nxx xxxx    (различные тарифы в зависимости от провайдера)
1 (npa) 976 xxxx  (во многих кодах зон, подключается через регионального
                   оператора; в некоторых районах для звонка требуется
                   код зоны — в зависимости от применяемого внутризонового
                   набора)
```

Другие префиксы обмена в кодах зон (например, 540, 720 или 915) используются для иных платных услуг: групповых чатов, других видов записанных сообщений и т. д. Они варьируются в зависимости от кода зоны в Северной Америке, и не все регионы имеют такие услуги.

Швеция

```
071 x xxxxx
```

Шведский аналог американских номеров «900» — коды 071 — устроен следующим образом.

(Тарифы зависят от следующей цифры)

```
Код          SEK/минута
0712xxxxx       3,65
0713xxxxx       4,90
0714xxxxx       6,90
0715xxxxx       9,90
0716xxxxx      12,50
0717xxxxx      15,30
0719xx         переменный тариф; нельзя набрать напрямую, требуется оператор
```

Номера, начинающиеся с 0713–0717, можно набирать только с телефонов, подключённых к коммутаторам AXE. В настоящее время около половины всех телефонов в Швеции подключены к таким коммутаторам.

Ещё один специальный платный номер — внутренний справочник телефонных номеров: 07975 (6,90 SEK/минута).

Великобритания

```
0836 xxx xxx
0898 xxx xxx
```

Тариф, судя по всему, единый: 34 пенса в минуту в льготное время и 45 пенсов в остальное время.

Фрикинг в Германии

Автор: -=+Ninja Master+=- из -[The Hellfire Club]-

Фрикинг в Германии в данный момент переживает небывалый подъём. Главная причина — объединение Германии. Большая часть, если не всё оборудование в Германии, по-прежнему механическое (особенно на бывшей коммунистической стороне). Поэтому боксинг делается ОЧЕНЬ легко, как и прослушивание линий.

Отслеживание звонков, напротив, по-прежнему затруднено. Это объясняется тем, что при механических коммутаторах требуется много технических специалистов, которые осматривают коммутаторы и отслеживают провода вручную. Обычно они не знают, куда ведёт провод, поэтому им приходится физически следовать по нему.

В настоящий момент в Германии существует два основных способа фрикинга. Первый — боксинг, второй — использование радиотелефонов; оба я опишу ниже.

Боксинг

Боксинг в Германии в целом схож с американским, однако я опишу весь процесс целиком.

Большинство боксинг-сессий в Германии начинается со звонка на бесплатный номер (большинство из которых обеспечивают соединение с американской фирмой AT&T). Чтобы инициировать звонок, вы набираете 0130 - 81 и нужный номер. Бесплатная сеть Германии начинается с 0130. 81 — код соединения с США. Вы ждёте соединения и подаёте сигнал разъединения. Как мы все знаем, в США это 2600 Гц, а в Германии — смесь 2400 и 2600 Гц. После этого вы отправляете одиночную частоту 2400 Гц для удержания линии. Затем вы решаете, хотите ли вы сделать местный звонок внутри США или международный. Не забывайте: вы сейчас подключены к США, поэтому всё, что выходит за их пределы, считается международным, даже если вы звоните из Германии. Звонки внутри США выполняются обычно: KP+0+AC+NNNNNNN. Для международного звонка: KP2+международный_код+0+номер. При этом нужно убрать ноль из набираемого номера. Например, в Германии все номера начинаются с 02366.

Одно существенное различие между боксингом в США и Германии — законодательство. В Германии очень строго следят за информационной безопасностью, однако законы в области фрикинга неоднозначны. Никто не знает, действительно ли фрикер что-то ворует у немецкой телефонной компании, поскольку он использует обычный номер телефона. Нам это может

показаться абсурдным, но именно так там на это смотрят. Поймать фрикера с поличным в Германии — редкий случай, если вообще возможный.

Радиотелефоны

```
  //---------------\\
 || Cordless Phones ||
  \\---------------//
```

Когда я говорю о «радиотелефонах» (cordless phones), я имею в виду не переносные телефоны в системе сотовой связи. Я говорю об обычных домашних радиотелефонах. Они передают сигнал на определённой радиочастоте (около 46 МГц) на «базовый блок», подключённый к настенной розетке.

Суть метода: установите длинную антенну на крыше своего автомобиля и подключите её к трубке. Оптимальная длина антенны — около 1,5 метра. Вам нужна только трубка, поскольку вы собираетесь подключиться к чужой базе, — убедитесь лишь, что аккумуляторы в трубке полностью заряжены. Затем езжайте на машине, пока не услышите свободную линию. После этого просто звоните куда угодно! Как правило, нужно немного поманеврировать и найти позицию, откуда сигнал принимается чисто и откуда хозяин базы вас не видит.

Этот метод работает весьма хорошо ещё и потому, что у большинства радиотелефонов в Германии нет функции выбора кода, столь распространённой здесь (когда можно выставить скремблирующий код на трубке и базе).

Одним из стимулов фрикинговать таким способом является то, что радиотелефоны в Германии незаконны, и их владелец, чьим тоном вы воспользовались, предпочтёт оплатить несколько больших счетов за межгород, нежели ещё более крупные штрафы за использование нелегального радиотелефона.

Радиотелефоны в Германии запрещены, хотя купить их можно практически везде. Незаконным является их физическое подключение к телефонной сети. Телефонная компания там специально ищет владельцев радиотелефонов с помощью оснащённого оборудованием фургона. Как только они обнаружат подключённый радиотелефон, они приезжают с двумя полицейскими и ордером на обыск. Вам могут предъявить обвинения в чём угодно — от незаконного подключения несертифицированного оборудования до подделки документов.

Заключение

```
  //----------\\
 || Conclusion ||
  \\----------//
```

Надеюсь, это немного прояснило, насколько разрозненна телефонная система в Германии, и дало вам несколько полезных советов на тот случай, если вы когда-нибудь окажетесь там.

Если у вас есть комментарии, поправки или дополнения, вы можете связаться со мной через Phrack или через следующие доски:

```
          Lightning  Systems                    9th  Dimension
             414-363-4282                        818-783-5320
```

До следующего раза!

```
             -=+Ninja Master+=-
            -[The Hellfire Club]-
 "Tell Telco We're Phreaking, Phreaking USA!"
```

\\--//

Учебник по TCP/IP: За кулисами интернета

Часть первая из двух

12 сентября 1991 г.

Автор: The Not

Содержание

---

1. Введение

Данный учебник освещает лишь основные, ключевые аспекты TCP/IP и потому представляет собой «скелет» технологии TCP/IP. Здесь опущены история разработки и финансирования, аргументы в пользу её применения, а также её перспективы по сравнению с ISO OSI. Значительный объём технических сведений также не включён. Оставлен минимум информации, которую необходимо понимать специалисту, работающему в среде TCP/IP. К таким специалистам относятся системный администратор, системный программист и сетевой менеджер.

В учебнике используются примеры из UNIX-среды TCP/IP, однако основные положения применимы ко всем реализациям TCP/IP.

Следует отметить, что цель данного материала — объяснение, а не определение. При возникновении любых вопросов о корректной спецификации протокола, пожалуйста, обращайтесь к соответствующему стандартообразующему RFC.

Следующий раздел представляет собой обзор TCP/IP, после которого идут подробные описания отдельных компонентов.

---

2. Обзор TCP/IP

Общий термин «TCP/IP» обычно означает всё, что так или иначе связано с конкретными протоколами TCP и IP. Он может охватывать другие протоколы, приложения и даже сетевую среду. В качестве примеров протоколов можно назвать: UDP, ARP и ICMP. В качестве примеров приложений — TELNET, FTP и rcp. Более точный термин — «интернет-технология». Сеть, использующая интернет-технологию, называется «интернетом».

2.1 Базовая структура

Чтобы понять данную технологию, необходимо прежде всего разобраться со следующей логической структурой:

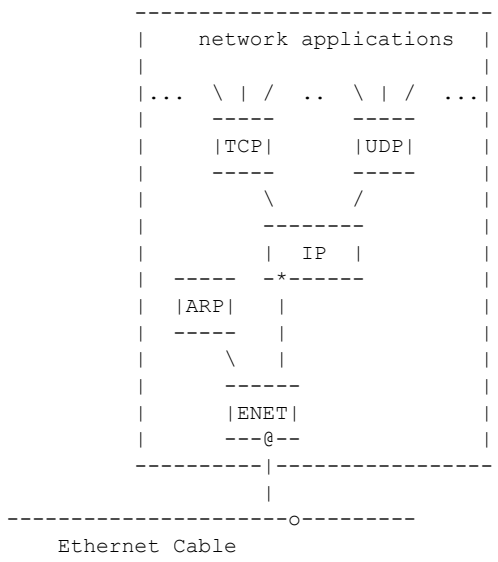


Figure 1. Basic TCP/IP Network Node

Это логическая структура многоуровневых протоколов внутри компьютера, подключённого к интернету. Каждый компьютер, способный взаимодействовать с использованием интернет-технологии, обладает подобной логической структурой. Именно эта логическая структура определяет поведение компьютера в интернете. Прямоугольники обозначают обработку данных по мере их прохождения через компьютер, а линии, соединяющие прямоугольники, показывают путь передачи данных. Горизонтальная линия внизу представляет кабель Ethernet; «o» — это трансивер. «*» — IP-адрес, а «@» — Ethernet-адрес. Понимание данной логической структуры принципиально важно для понимания интернет-технологии; на неё ссылаются на протяжении всего учебника.

2.2 Терминология

Название единицы данных, передаваемой по интернету, зависит от того, на каком уровне стека протоколов она находится. В кратком изложении: если данные находятся в сети Ethernet, они называются кадром Ethernet; если — между драйвером Ethernet и модулем IP, они называются IP-пакетом; если — между модулем IP и модулем UDP, они называются UDP-датаграммой; если — между модулем IP и модулем TCP, они называются TCP-сегментом (в более общем смысле — транспортным сообщением); если же данные находятся в сетевом приложении, они называются сообщением приложения.

Эти определения не являются строгими. Точные определения варьируются в зависимости от источника. Более конкретные определения можно найти в RFC 1122, раздел 1.3.3.

Драйвер — это программное обеспечение, которое напрямую взаимодействует с аппаратным сетевым интерфейсом. Модуль — это программное обеспечение, которое взаимодействует с драйвером, сетевыми приложениями или другим модулем.

Термины «драйвер», «модуль», «кадр Ethernet», «IP-пакет», «UDP-датаграмма», «TCP-сообщение» и «сообщение приложения» используются по мере необходимости на протяжении всего учебника.

2.3 Поток данных

Проследим за данными по мере их прохождения вниз по стеку протоколов, показанному на рисунке 1. Для приложения, использующего TCP (Transmission Control Protocol — протокол управления передачей), данные передаются между приложением и модулем TCP. Для приложений, использующих UDP (User Datagram Protocol — протокол пользовательских датаграмм), данные передаются между приложением и модулем UDP. FTP (File Transfer Protocol — протокол передачи файлов) — типичный пример приложения, использующего TCP. Его стек протоколов в данном примере: FTP/TCP/IP/ENET. SNMP (Simple Network Management Protocol — простой протокол управления сетью) — пример приложения, использующего UDP. Его стек протоколов в данном примере: SNMP/UDP/IP/ENET.

Модуль TCP, модуль UDP и драйвер Ethernet являются мультиплексорами «n к 1». Как мультиплексоры они переключают множество входов на один выход. Они также являются демультиплексорами «1 к n». Как демультиплексоры они переключают один вход на множество выходов в соответствии с полем типа в заголовке протокола.

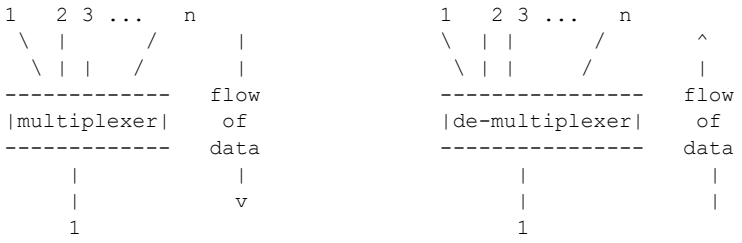


Figure 2. n-to-1 multiplexer and 1-to-n de-multiplexer

Если кадр Ethernet поступает снизу в драйвер Ethernet из сети, пакет может быть передан вверх либо модулю ARP (Address Resolution Protocol — протокол разрешения адресов), либо модулю IP (Internet Protocol — межсетевой протокол). Значение поля типа в кадре Ethernet определяет, в какой модуль — ARP или IP — будет передан кадр.

Если IP-пакет поступает в модуль IP снизу, единица данных передаётся вверх либо в TCP, либо в UDP — в зависимости от значения поля протокола в заголовке IP.

Если UDP-датаграмма поступает в модуль UDP, сообщение приложения передаётся вверх в сетевое приложение на основе значения поля порта в заголовке UDP. Если TCP-сообщение поступает в модуль TCP, сообщение приложения передаётся вверх в сетевое приложение на основе значения поля порта в заголовке TCP.

Мультиплексирование в направлении вниз выполняется просто, поскольку из каждой начальной точки существует только один нисходящий путь; каждый модуль протокола добавляет информацию своего заголовка, чтобы на компьютере-получателе пакет мог быть демультиплексирован.

Данные, исходящие от приложений через TCP или UDP, сходятся в модуле IP и направляются вниз через нижний драйвер сетевого интерфейса.

Хотя интернет-технология поддерживает множество различных сетевых сред, во всех примерах данного учебника используется Ethernet, поскольку именно он является наиболее распространённой физической сетью, применяемой под IP. Компьютер на рисунке 1 имеет одно соединение Ethernet. 6-байтовый Ethernet-адрес уникален для каждого интерфейса в сети Ethernet и расположен на нижнем интерфейсе драйвера Ethernet.

Компьютер также имеет 4-байтовый IP-адрес. Этот адрес расположен на нижнем интерфейсе модуля IP. IP-адрес должен быть уникальным в пределах интернета.

Работающий компьютер всегда знает свой собственный IP-адрес и Ethernet-адрес.

2.4 Два сетевых интерфейса

Если компьютер подключён к двум отдельным сетям Ethernet, его структура выглядит так, как показано на рисунке 3.

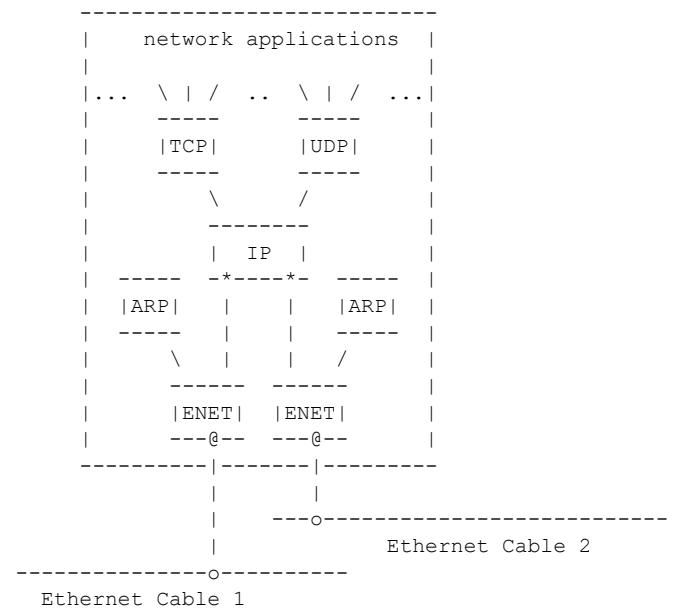


Figure 3. TCP/IP Network Node on 2 Ethernets

Обратите внимание: данный компьютер имеет 2 Ethernet-адреса и 2 IP-адреса.

Из этой структуры видно, что для компьютеров с более чем одним физическим сетевым интерфейсом модуль IP является одновременно мультиплексором «n к m» и демультиплексором «m к n».

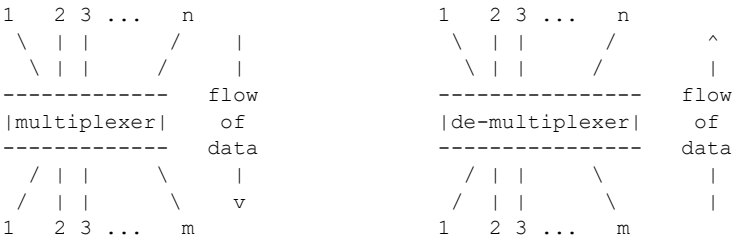


Figure 4. n-to-m multiplexer and m-to-n de-multiplexer

Он выполняет это мультиплексирование в обоих направлениях для обработки входящих и исходящих данных. Модуль IP с более чем одним сетевым интерфейсом сложнее нашего исходного примера тем, что он может передавать данные в следующую сеть. Данные могут поступать через любой сетевой интерфейс и отправляться через любой другой.

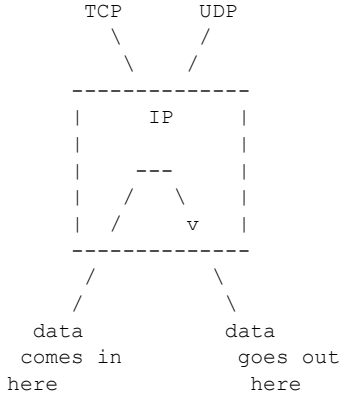


Figure 5. Example of IP Forwarding a IP Packet

Процесс отправки IP-пакета в другую сеть называется «пересылкой» (forwarding) IP-пакета. Компьютер, специально выделенный для задачи пересылки IP-пакетов, называется «IP-маршрутизатором» (IP-router).

Как видно из рисунка, пересылаемый IP-пакет никогда не затрагивает модули TCP и UDP на IP-маршрутизаторе. Некоторые реализации IP-маршрутизатора не имеют модулей TCP или UDP.

2.5 IP создаёт единую логическую сеть

Модуль IP занимает центральное место в успехе интернет-технологии. Каждый модуль или драйвер добавляет свой заголовок к сообщению по мере его прохождения вниз по стеку протоколов. Каждый модуль или драйвер снимает соответствующий заголовок с сообщения по мере того, как оно поднимается по стеку протоколов в направлении приложения. Заголовок IP содержит IP-адрес, который строит единую логическую сеть из множества физических сетей. Это объединение физических сетей и является источником названия: интернет. Совокупность взаимосвязанных физических сетей, ограничивающих область действия IP-пакета, называется «интернетом».

2.6 Независимость от физической сети

IP скрывает лежащее в основе сетевое аппаратное обеспечение от сетевых приложений. Если вы создаёте новую физическую сеть, вы можете ввести её в эксплуатацию, реализовав новый драйвер, который подключается к интернету под IP. Таким образом, сетевые приложения остаются нетронутыми и не подвержены изменениям в аппаратной технологии.

2.7 Совместимость (Interoperability)

Если два компьютера в интернете могут взаимодействовать, говорят, что они «совместимы» (interoperate); если реализация интернет-технологии выполнена качественно, говорят, что она обладает «интероперабельностью» (interoperability). Пользователи компьютеров общего назначения выигрывают от развёртывания интернета благодаря интероперабельности компьютеров, представленных на рынке. Как правило, приобретая компьютер, вы получаете устройство, способное работать в сети. Если компьютер не обладает интероперабельностью и она не может быть добавлена, он занимает редкую и особую нишу на рынке.

2.8 После обзора

Получив необходимые базовые сведения, мы ответим на следующие вопросы:

При отправке IP-пакета — как определяется Ethernet-адрес получателя?

Как IP узнаёт, какой из нескольких нижних сетевых интерфейсов использовать при отправке IP-пакета?

Как клиент на одном компьютере устанавливает связь с сервером на другом?

Почему существуют и TCP, и UDP, а не только один из них?

Какие сетевые приложения доступны?

Ответы на эти вопросы будут даны по порядку — после краткого повторения основ Ethernet.

---

3. Ethernet

Данный раздел представляет собой краткий обзор технологии Ethernet.

Кадр Ethernet содержит адрес получателя, адрес отправителя, поле типа и данные.

Ethernet-адрес занимает 6 байт. Каждое устройство имеет собственный Ethernet-адрес и прослушивает кадры Ethernet с таким адресом получателя. Все устройства также прослушивают кадры Ethernet с групповым адресом получателя «FF-FF-FF-FF-FF-FF» (в шестнадцатеричном формате), называемым «широковещательным» (broadcast) адресом.

В Ethernet используется метод CSMA/CD (Carrier Sense and Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий). CSMA/CD означает, что все устройства взаимодействуют в единой среде, что одновременно может передавать только одно устройство, и что все они могут одновременно принимать данные. Если два устройства пытаются начать передачу в один и тот же момент, коллизия передачи обнаруживается, и оба устройства ждут случайный (но короткий) период перед следующей попыткой передачи.

3.1 Аналогия с людьми

Хорошей аналогией технологии Ethernet служит группа людей, разговаривающих в небольшой, совершенно тёмной комнате. В данной аналогии физической сетевой средой являются звуковые волны в воздухе комнаты вместо электрических сигналов в коаксиальном кабеле.

Каждый человек слышит слова, когда говорит другой (контроль несущей — Carrier Sense). У всех в комнате равные возможности говорить (множественный доступ — Multiple Access), но они не произносят длинных речей, потому что вежливы. Если кто-то ведёт себя невежливо, его просят покинуть комнату (то есть его выбрасывают из сети).

Никто не говорит, пока говорит другой. Но если два человека начинают говорить одновременно, каждый из них это понимает, потому что слышит то, чего сам не говорил (обнаружение коллизий — Collision Detection). Когда эти двое замечают данную ситуацию, они ждут момент, затем один начинает говорить. Другой слышит речь и ждёт, пока первый закончит, прежде чем начать свою.

У каждого человека есть уникальное имя (уникальный Ethernet-адрес), чтобы избежать путаницы. Каждый раз, когда кто-то говорит, он предваряет сообщение именем того, к кому обращается, и своим собственным именем (Ethernet-адресом получателя и отправителя соответственно), то есть: «Привет, Джейн, это Джек, ...бла-бла-бла...». Если отправитель хочет обратиться ко всем, он может сказать «всем» (широковещательный адрес): «Привет всем, это Джек, ...бла-бла-бла...».

---

4. ARP

При отправке IP-пакета — как определяется Ethernet-адрес получателя?

ARP (Address Resolution Protocol — протокол разрешения адресов) используется для преобразования IP-адресов в Ethernet-адреса. Преобразование выполняется только для исходящих IP-пакетов, поскольку именно в этот момент создаются заголовок IP и заголовок Ethernet.

4.1 Таблица ARP для преобразования адресов

Преобразование выполняется путём поиска в таблице. Таблица, называемая таблицей ARP, хранится в памяти и содержит строку для каждого компьютера. В ней есть столбец для IP-адреса и столбец для Ethernet-адреса. При преобразовании IP-адреса в Ethernet-адрес в таблице осуществляется поиск совпадающего IP-адреса. Ниже приведён упрощённый пример таблицы ARP:

```
-----------------------------------
|IP address       Ethernet address |
-----------------------------------
|223.1.2.1        08-00-39-00-2F-C3|
|223.1.2.3        08-00-5A-21-A7-22|
|223.1.2.4        08-00-10-99-AC-54|
-----------------------------------
    TABLE 1.  Example ARP Table
```

Принятое соглашение при записи 4-байтового IP-адреса: каждый байт в десятичном формате, байты разделены точкой. При записи 6-байтового Ethernet-адреса: каждый байт в шестнадцатеричном формате, байты разделены дефисом или двоеточием.

Таблица ARP необходима потому, что IP-адрес и Ethernet-адрес выбираются независимо друг от друга; алгоритм для преобразования IP-адреса в Ethernet-адрес использовать нельзя. IP-адрес выбирается сетевым менеджером исходя из расположения компьютера в интернете. При перемещении компьютера в другую часть интернета его IP-адрес должен быть изменён. Ethernet-адрес выбирается производителем на основе пространства Ethernet-адресов, лицензированного производителем. При замене аппаратной платы интерфейса Ethernet меняется и Ethernet-адрес.

4.2 Типичный сценарий преобразования

В ходе обычной работы сетевое приложение, например TELNET, отправляет сообщение приложения в TCP, затем TCP отправляет соответствующее TCP-сообщение в модуль IP. IP-адрес получателя известен приложению, модулю TCP и модулю IP. На данном этапе IP-пакет сформирован и готов к передаче драйверу Ethernet, однако сначала необходимо определить Ethernet-адрес получателя.

Для поиска Ethernet-адреса получателя используется таблица ARP.

4.3 Пара запрос/ответ ARP

Но как вообще заполняется таблица ARP? Ответ: она заполняется автоматически протоколом ARP по мере необходимости.

Если с помощью таблицы ARP не удаётся выполнить преобразование адреса, происходят два действия:

1. В сеть ко всем компьютерам отправляется ARP-запрос с широковещательным Ethernet-адресом.

2. Исходящий IP-пакет ставится в очередь.

Сетевой интерфейс Ethernet каждого компьютера принимает широковещательный кадр Ethernet. Каждый драйвер Ethernet проверяет поле типа в кадре Ethernet и передаёт ARP-пакет модулю ARP. ARP-запрос говорит следующее: «Если ваш IP-адрес совпадает с данным целевым IP-адресом — пожалуйста, сообщите мне ваш Ethernet-адрес». ARP-запрос выглядит примерно так:

```
---------------------------------------
|Sender IP Address   223.1.2.1        |
|Sender Enet Address 08-00-39-00-2F-C3|
---------------------------------------
```

```
|Target IP Address   223.1.2.2        |
|Target Enet Address <blank>          |
---------------------------------------
     TABLE 2.  Example ARP Request
```

Каждый модуль ARP проверяет IP-адрес, и если целевой IP-адрес совпадает с его собственным IP-адресом, он отправляет ответ непосредственно на исходный Ethernet-адрес. ARP-ответ говорит следующее: «Да, этот целевой IP-адрес принадлежит мне, позвольте сообщить вам мой Ethernet-адрес». В ARP-ответе содержимое полей отправителя и получателя меняется местами по сравнению с запросом. Ответ выглядит примерно так:

```
---------------------------------------
|Sender IP Address   223.1.2.2        |
|Sender Enet Address 08-00-28-00-38-A9|
---------------------------------------
|Target IP Address   223.1.2.1        |
|Target Enet Address 08-00-39-00-2F-C3|
---------------------------------------
     TABLE 3.  Example ARP Response
```

Ответ получает исходный компьютер-отправитель. Драйвер Ethernet проверяет поле типа в кадре Ethernet, затем передаёт ARP-пакет модулю ARP. Модуль ARP анализирует ARP-пакет и добавляет IP-адрес и Ethernet-адрес отправителя в свою таблицу ARP.

Обновлённая таблица теперь выглядит следующим образом:

```
-----------------------------------
|IP address     Ethernet address |
-----------------------------------
|223.1.2.1      08-00-39-00-2F-C3|
|223.1.2.2      08-00-28-00-38-A9|
|223.1.2.3      08-00-5A-21-A7-22|
|223.1.2.4      08-00-10-99-AC-54|
-----------------------------------
TABLE 4.  ARP Table after Response
```

4.4 Продолжение сценария

Новая запись преобразования была автоматически внесена в таблицу буквально через несколько миллисекунд после того, как она понадобилась. Как вы помните из шага 2, исходящий IP-пакет был поставлен в очередь. Далее выполняется преобразование IP-адреса в Ethernet-адрес путём поиска в таблице ARP, после чего кадр Ethernet передаётся в сеть Ethernet. Таким образом, с учётом новых шагов 3, 4 и 5 полный сценарий для компьютера-отправителя выглядит следующим образом:

1. В сеть ко всем компьютерам отправляется ARP-запрос с широковещательным Ethernet-адресом.

2. Исходящий IP-пакет ставится в очередь.

3. Поступает ARP-ответ с данными преобразования IP-адреса в Ethernet-адрес для таблицы ARP.

4. Для IP-пакета, стоящего в очереди, таблица ARP используется для преобразования IP-адреса в Ethernet-адрес.

5. Кадр Ethernet передаётся в сеть Ethernet.

Таким образом, когда запись преобразования отсутствует в таблице ARP, один IP-пакет ставится в очередь. Данные преобразования быстро заполняются посредством пары запрос/ответ ARP, и поставленный в очередь IP-пакет передаётся.

Каждый компьютер имеет отдельную таблицу ARP для каждого из своих интерфейсов Ethernet. Если целевой компьютер не существует, ARP-ответа не последует и запись в таблице ARP не появится. IP будет отбрасывать исходящие IP-пакеты, адресованные на этот адрес. Протоколы верхнего уровня не могут отличить неисправную сеть Ethernet от отсутствия компьютера с целевым

IP-адресом.

Некоторые реализации IP и ARP не ставят IP-пакет в очередь в ожидании ARP-ответа. Вместо этого IP-пакет отбрасывается, а восстановление после его потери возлагается на модуль TCP или сетевое приложение UDP. Восстановление выполняется посредством тайм-аута и повторной передачи. Повторно переданное сообщение успешно отправляется в сеть, поскольку первая копия сообщения уже обеспечила заполнение таблицы ARP.

Настоящая рабочая схема «Красной коробки»

Автор: R.J. "BoB" Dobbs

Что такое «Красная коробка»?

По сути, «Красная коробка» — это устройство, предназначенное для того, чтобы обмануть компьютер телефонной компании, заставив его думать, что монеты опущены в таксофон. Каждый раз, когда вы бросаете монету в таксофон, аппарат сигнализирует о типе монеты одним или несколькими импульсами комбинации частот 1700 Гц и 2200 Гц. Тональные импульсы кодируются следующим образом:

• **5 центов (никель):** один импульс длительностью 60 миллисекунд
• **10 центов (дайм):** два импульса по 60 миллисекунд с паузой 60 миллисекунд
• **25 центов (квотер):** пять импульсов по 35 миллисекунд с паузами по 35 миллисекунд

Как пользоваться

Просто наберите номер для звонка на дальнее расстояние (в некоторых районах сначала придётся опустить настоящий никель), дождитесь, когда компьютер ACTS потребует оплату, и нажмите кнопку «deposit» на красной коробке столько раз, сколько монет нужно симулировать. Тональные сигналы монет передаются из красной коробки в телефон через небольшой динамик, поднесённый к микрофону. Для местных звонков необходимо либо сначала опустить настоящий никель, а потом симулировать остальные монеты, либо воспользоваться оператором по номеру 0+xxx+yyyy. Будьте осторожны, когда на линии оператор — иногда он раскусывает вашу схему с «пищалкой».

Принцип работы схемы

Каждый раз при нажатии кнопки она запускает одну половину IC1, настроенную как моностабильный мультивибратор, который активирует остальную часть схемы на время, определяемое положением переключателя выбора монеты. Это в свою очередь запускает вторую половину IC1, настроенную как астабильный мультивибратор, который генерирует импульсы с регулярными интервалами, задаваемыми потенциометром 100 кОм между выводами 12 и 13. Выход астабильного мультивибратора поочерёдно питает IC2, настроенную как генератор прямоугольных импульсов, обеспечивая необходимые частоты 1700 Гц и 2200 Гц на операционный усилитель, выполняющий роль буфера для управления динамиком.

Настройка и тестирование

При изготовлении устройства ни в коем случае не используйте блок питания 9 В переменного тока! Также не рекомендуется использовать макетную плату. Будьте осторожны с паяльником. И то, и другое создаст вам проблемы.

Для настройки желателен частотомер, однако подойдёт и хороший осциллограф. (Они не являются АБСОЛЮТНО необходимыми, но помогут.) Для определения частоты в Гц с помощью осциллографа можно использовать следующую формулу:

```
          1          S = Измерение волны на дисплее
Hz = -----------
     S*(T*10^-6)     T = Установка селектора времени (миллисекунды)

           1
Hz = ------------------  Hz = 2198
     9.1 * 50ms * 10^-6
```

Аккуратно извлеките IC1 из панельки. Установите временную перемычку от источника +9 В к выводу 14 IC2 и временно отсоедините конденсаторы 0,01 мкФ от выводов 5 и 9 IC2. Включите питание схемы. Измеряя выход с вывода 5 IC2 частотомером или осциллографом, настройте потенциометр 50 кОм между выводами 1 и 6 на частоту 1700 Гц. Затем настройте потенциометр 50 кОм между выводами 8 и 13 на частоту 2200 Гц с вывода 9 IC2. Снимите временную перемычку, повторно подсоедините конденсаторы к выводам 5 и 9 IC2 и вставьте IC1 обратно. (Примечание: при отсутствии частотомера выходы можно настроить на слух, добиваясь нулевых биений между выходным тоном и тоном известной точности, сгенерированным компьютером.)

Далее с помощью мультиметра настройте потенциометр 10 кОм на катоде диода «квотер» на сопротивление около 8 кОм. (Это задаёт разницу между длительностью импульсов квотера и импульсов никеля/дайма — точная настройка этого соотношения может потребоваться на последних этапах калибровки; её можно сделать на слух.)

Теперь временно отсоедините провод между выводами 5 и 10 IC1. Установите переключатель выбора монеты в положение «N» (никель). С помощью осциллографа, измеряя выход с вывода 9 IC1, настройте потенциометр 100 кОм между выводами 12 и 13 IC1 так, чтобы длительность выходных импульсов составляла 60 миллисекунд. Подсоедините провод между выводами 5 и 10 обратно. (Примечание: при отсутствии осциллографа скорость импульсов настраивается на слух с использованием компьютерных тонов для сравнения.)

Оставьте переключатель в положении «N». Настройте потенциометр 50 кОм с надписью «Nickel» так, чтобы при каждом нажатии кнопки «deposit» слышался один звуковой сигнал.

Установите переключатель монеты в положение «Dime». Настройте потенциометр 50 кОм с надписью «Dime» так, чтобы при каждом нажатии кнопки слышался быстрый двойной сигнал.

Наконец, установите переключатель в положение «Quarter». Настройте потенциометр 50 кОм с надписью «Quarter» до тех пор, пока при каждом нажатии кнопки не будет слышаться ровно 5 очень быстрых сигналов. Не беспокойтесь, если сигналы квотера звучат короче и быстрее, чем у никеля и дайма. Так и должно быть.

Заключение

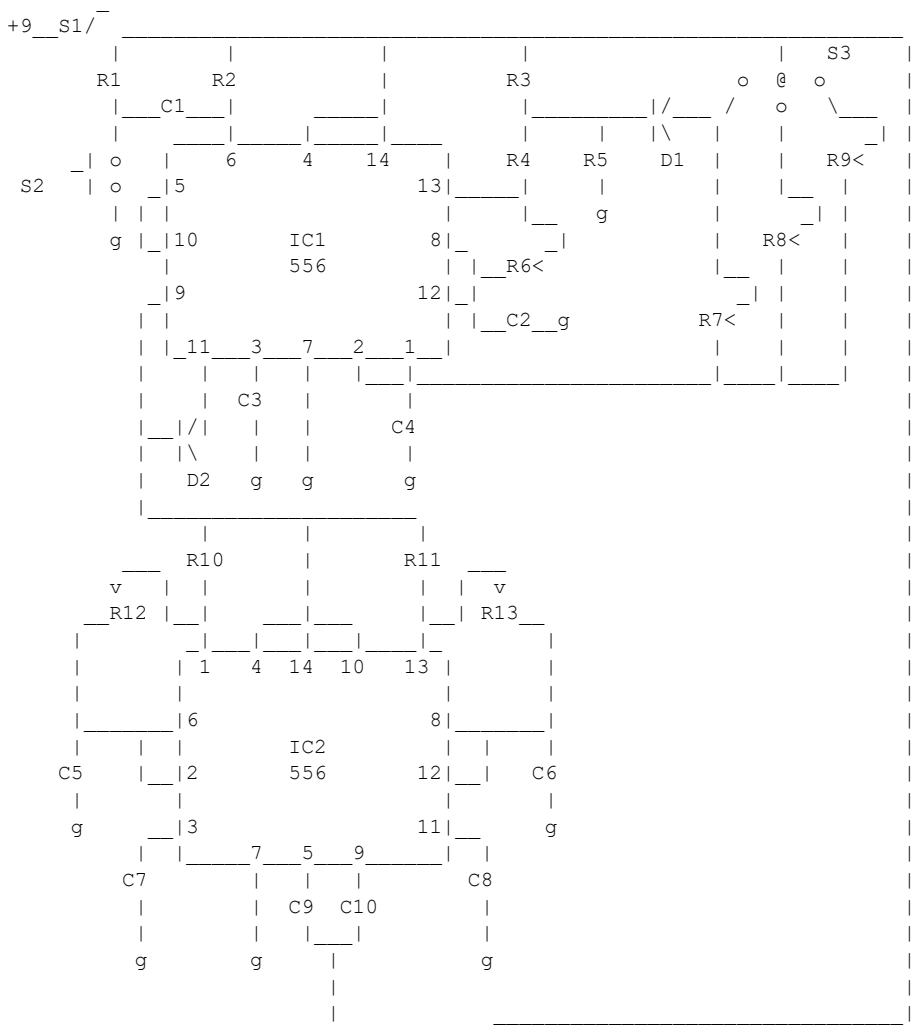
Если всё прошло успешно, ваша красная коробка должна быть полностью откалибрована и готова к работе. Теперь следует провести финальное тестирование с таксофона с использованием тестовой линии DATL (Dial Access Test Line) для проверки монет. Наберите 09591230 и следуйте инструкциям компьютера, используя красную коробку при соответствующих запросах. Компьютер должен правильно идентифицировать все «симулированные» монеты и зафиксировать любые

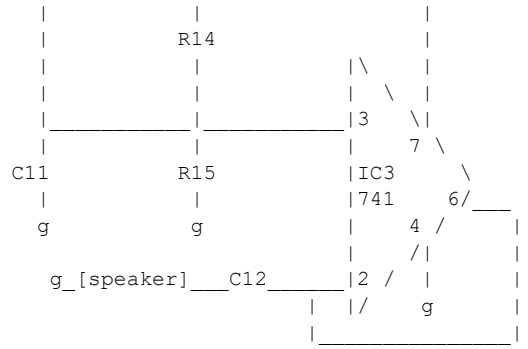
аномалии. При разумной осторожности ваша красная коробка прослужит вам долгие годы. Помните: мелочи не бывает!

Список компонентов «Красной коробки»

2	556 Dual Timer IC	8	конденсатора 0.01мкФ
1	741 Op Amp IC	2	конденсатора 0.1мкФ
2	диода 1N914	1	электролитический конденсатор 1.0мкФ
5	резисторов 10кОм	2	электролитических конденсатора 10мкФ
1	резистор 4.7кОм	1	3-позиционный роторный переключатель
2	резистора 100кОм	1	тумблер SPST
1	подстроечный резистор 100кОм (PC Mount)	1	кнопка без фиксации (нормально разомкнутая)
3	подстроечных резистора 50кОм (PC Mount)	1	зажим для батареи 9В
1	подстроечный резистор 10кОм (PC Mount)	2	панельки DIP 14 pin
2	многооборотных потенциометра 50кОм	1	панелька DIP 8 pin

Принципиальная схема





Кодировка компонентов схемы

R1:10K	R4:10K	R7:50K pot	R10:10K	R13:50K pot
R2:10K	R5:10K	R8:50K pot	R11:10K	R14:100K
R3:4.7K	R6:100K pot	R9:50K pot	R12:50K pot	R15:100K
C1:0.01мкФ	C4:10мкФ	C7:0.01мкФ	C10:0.01мкФ	
C2:1.00мкФ	C5:0.01мкФ	C8:0.01мкФ	C11:0.10мкФ	D1 :1N914
C3:0.01мкФ	C6:0.01мкФ	C9:0.01мкФ	C12:10мкФ	D2 :1N914

S1 - тумблер SPST
S2 - кнопка без фиксации, нормально разомкнутая
S3 - 3-позиционный роторный переключатель g - Земля

Хакеры, пришедшие с холода

```
PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN          P h r a c k   W o r l d   N e w s        PWN
^*^          ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        ^*^
PWN             Special Edition Issue Four            PWN
^*^                                                   ^*^
PWN       "The Hackers Who Came In From The Cold"     PWN
^*^                                                   ^*^
PWN                  June 21-23, 1991                 PWN
^*^                                                   ^*^
PWN              Written by Bruce Sterling            PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
```

Автор: Bruce Sterling : bruces @ well.sf.ca.us

«Миллионеры и вандалы встретились на конвенции компьютерного андерграунда, чтобы обсудить свободу информации. А нашли — свободную любовь.»

Слегка сокращённая версия этой статьи опубликована в журнале Details (октябрь 1991, стр. 94–97, 134). В журнальной версии помещены фотографии Knight Lightning, Erik Bloodaxe, Mitch Kapor и Doc Holiday.

Они назвали это «CyberView '91». На самом деле всё было как обычно — очередной «SummerCon», традиционный летний съезд американского хакерского андерграунда. Организатор мероприятия, 21-летний «Knight Lightning», недавно сумел отбиться от обвинения в компьютерном мошенничестве и злоупотреблениях, которое грозило ему тридцатью годами заключения. Небольшая осторожность казалась вполне уместной.

Мотель по соседству с аэропортом Сент-Луиса — потрёпанный, но достаточно гостеприимный — уже не раз принимал SummerCon. Смена названия была хорошей идеей. Если бы персонал был внимателен и узнал в гостях тех самых ребят, которые бывали здесь раньше, всё могло бы обернуться весьма скверно.

Гостиница SummerCon '88 была заведомо исключена из рассмотрения. Тогда Секретная служба США оборудовала наблюдательный пункт в комнате информатора и через зеркало с односторонней прозрачностью снимала пьяные выходки тогда ещё не столь широко известного «Legion of Doom». Участие в организации SummerCon '88 фигурировало как один из главных пунктов обвинения в уголовном заговоре на федеральном процессе над молодым Knight Lightning в 1990 году.

С той гостиницей были связаны нехорошие воспоминания. Да и без того на тусовках SummerCon все и так изрядно нервничали, играя в «найди федерала». Как правило, на SummerCon присутствовал хотя бы один действующий осведомитель федеральных органов. Хакеры и телефонные фрики любят поговорить. Они говорят о телефонах и компьютерах — и друг о друге.

Мир компьютерного взлома изнутри очень похож на Мексику. Среднего класса нет. Есть миллион мелких пацанов, ковыряющихся со своими модемами, пытающихся стащить коды для дальней связи, умыкнуть пиратский софт, — «kodez kidz» и «warez doodz». Они — пешки, «грызуны». Потом — горстка серьёзных стажёров, начинающих, учеников. Немного. В последние годы — всё меньше.

И наконец — тяжеловесы. Игроки. Legion of Doom — безусловно тяжеловесы. Немецкий Chaos Computer Club — очень тяжелые, и уже вышли на свободу после своих рискованных игр с КГБ.

Masters of Destruction из Нью-Йорка — настоящая головная боль для соперников в андерграунде, но что тут скажешь — тоже тяжеловесы. «Phiber Optik» из MoD почти завершил отбывание общественных работ... «Phoenix» со своей компанией в Австралии когда-то котировались высоко, но о «Nom» и «Electron» с тех пор, как австралийские власти взялись за них, практически ничего не слышно.

Голландцы очень активны, но как-то не тянут на звание «тяжеловесов». Наверное, потому что в Голландии компьютерный взлом легален и за него никого не сажают. Голландцам недостаёт нужного злобного настроя.

Американский ответ на голландскую угрозу прибывал непрерывным потоком аэропортовых автобусов-шаттлов и облезших студенческих развалюх. Один из пиратов программного обеспечения, из числа наиболее зажиточных участников, щеголял чёрным мускл-каром с радар-детектором. В какую-то давнюю доавиационную эпоху этот уголок Сент-Луиса был тихим, плодородным пейзажем в духе Сэмюэля Клеменса. Летние сорняки в человеческий рост по-прежнему буйно росли вдоль четырёхполосного шоссе и объездных дорог у аэропорта.

Угловатая гостиница CyberView была вбита в этот пейзаж будто сброшена с бомбардировщика B-52. В одном углу высилась небольшая офисная башня рядом с многоярусной парковкой. Остальное представляло собой запутанный лабиринт длинных, узких, плохо освещённых коридоров с маленьким бассейном, сувенирным магазином с витриной в пол и унылой столовой. В гостинице было достаточно чисто, и персонал, несмотря на провокации, умело смотрел в другую сторону. Хакеры же, со своей стороны, были к этому месту, кажется, искренне привязаны.

У слова «хакер» — пятнистая история. Настоящие «хакеры», традиционные «хакеры», любят писать программы. Они любят «грызть код», погружаясь в самые плотные его абстракции до тех пор, пока внешний мир за пределами монитора не растворяется. Хакеры, как правило, — полноватые белые технари с густыми лохматыми бородами, говорящие исключительно на жаргоне, часто смотрящие в никуда и изредка смеющиеся без видимой причины. Тусовщики CyberView, хотя и называют себя «хакерами», точнее определяются как компьютерные взломщики. Они не выглядят, не говорят и не ведут себя как хакеры в стиле MIT 1960-х.

Компьютерные взломщики 90-х — это не обитатели программистских берлог с нагрудными карманчиками для ручек. Это молодые белые парни из пригородов, достаточно безобидные на вид, но хитрые. Примерно такого сорта ребята, которых можно застать купающимися голышом в два часа ночи в соседском дворовом бассейне. Из тех, кто застынет под лучом хозяйского фонарика, потом лихорадочно схватит штаны и перемахнёт через забор, оставив за собой полупустую бутылку текилы, футболку Metallica и, весьма вероятно, бумажник.

Можно задаться вопросом: почему во втором десятилетии революции персональных компьютеров большинство взломщиков по-прежнему — белые мальчики-вундеркинды из пригородов? Компьютерный взлом существует достаточно долго, чтобы успело вырасти целое поколение серьёзных матёрых взрослых киберпреступников. Но по большей части этого так и не произошло. Почти все компьютерные взломщики просто бросают это дело после двадцати двух лет. Им, честно говоря, становится скучно. Шнырять по чужим бассейнам надоедает. Они заканчивают учёбу. Женятся. Покупают собственные бассейны. Им надо как-то изображать реальную жизнь.

Legion of Doom — точнее, техасское крыло LoD — прибыл в Сент-Луис с помпой в эти выходные 22 июня. Секретная служба охарактеризовала Legion of Doom как «хай-тек уличную банду», хотя это, пожалуй, один из самых дырявых, нелепых и широко освещённых в прессе преступных заговоров в американской истории.

О основателе Легиона «Lex Luthor» давно почти ничего не слышно. Атлантское крыло Легиона — «Prophet», «Leftist» и «Urvile» — только-только выходят из разных тюрем и разъезжаются по исправительным домам в Джорджии. «Mentor» женился и зарабатывает на жизнь, сочиняя

научно-фантастические игры.

Зато «Erik Bloodaxe», «Doc Holiday» и «Malefactor» присутствовали — лично, и в последних номерах TIME и NEWSWEEK. CyberView предоставил отличный повод техасским думстерам объявить о создании своей новейшей хай-тек, хм, организации — «Comsec Data Security Corporation».

Comsec располагает корпоративным офисом в Хьюстоне, маркетологом и полноценной программой корпоративного компьютерного аудита. Ребята из Легиона теперь — цифровые наёмники. Если у вас есть деньги и вы готовы оплатить суточные и авиабилеты, самые известные компьютерные хакеры Америки явятся прямо к вам и наведут порядок в вашем цифровом хозяйстве — с гарантией.

Bloodaxe — стройный, поразительно красивый молодой техасец с волосами до плеч, в зеркальных очках, при галстуке и с незаурядным даром красноречия — взял слово. Перед тремя десятками бывших коллег, собравшихся наверху со стаканчиками кофе в пенопластовых стаканах и банками колы в номере «Марк Твен», Bloodaxe с видом знатока изложил несколько горьких истин о современной компьютерной безопасности.

Большинство так называемых «экспертов по компьютерной безопасности» — конкуренты Comsec — это дорогостоящие шарлатаны! Они берут с доверчивых корпораций тысячи долларов в день, чтобы посоветовать руководству запирать двери на ночь и пользоваться шредерами. Comsec Corp, напротив — при случайном участии консультантов «Pain Hertz» и «Prime Suspect» — располагает, пожалуй, самым внушительным в Америке реальным опытом непосредственного взлома компьютеров.

Comsec, продолжал Bloodaxe ровным голосом, не занимается доносительством на бывших хакерских товарищей. На случай, если кто-то здесь вдруг, ну, беспокоится... С другой стороны, любой безрассудный дурак, рискнувший атаковать систему, защищённую Comsec, должен быть готов к серьёзной хакерской разборке.

— Почему какая-нибудь компания должна вам доверять? — лениво поинтересовался кто-то.

Malefactor — крепкий молодой техасец с короткой стрижкой и фигурой футбольного лайнбекера — пояснил: после найма Comsec получает доступ к компьютерной системе работодателя на законных основаниях и не имеет никакого смысла «взламывать» её. К тому же сотрудники Comsec будут лицензированы и застрахованы.

Bloodaxe горячо уверял, что LoD покончил с хакингом раз и навсегда. В этом просто нет будущего. Для LoD настало время двигаться дальше, а корпоративный консалтинг — их новый рубеж. (Карьерные перспективы закоренелых компьютерных взломщиков, если уж говорить честно, крайне скудны.) «Мы не хотим жарить гамбургеры или продавать страховку, когда нам стукнет тридцать», — протянул Bloodaxe. «И гадать, когда Тим Фоули выломает дверь!» (Специальный агент Тимоти М. Фоули из Секретной службы США вполне заслуженно считается самым грозным антихакерским копом в Америке.)

Bloodaxe вздохнул с тоской. «Оглядываясь на свою жизнь... я понимаю, что в сущности одиннадцать лет учился в школе, где сам себя готовил стать консультантом по компьютерной безопасности».

После ещё нескольких неудобных вопросов Bloodaxe наконец добрался до главного. Кто-нибудь теперь ненавидит их? — спросил он почти робко. Считают ли люди, что Легион предал идеалы? Никто не высказал такого мнения. Хакеры качали головами, смотрели себе на кеды, тянули колу из банок. Они как будто не видели в этом особой разницы, если честно. Уже не при таких обстоятельствах.

Больше половины участников CyberView публично заявляли, что завязали с хакингом. По меньшей мере один хакер — явившийся на конвент по одному ему ведомой причине в белокуром парике и

дешёвой тиаре и теперь ловивший брошенные Cheetos в пенопластовый стаканчик — уже зарабатывал на жизнь «консультированием» частных детективов.

Практически у каждого участника CyberView за плечами были: арест, изъятие компьютера или как минимум допрос — а когда федеральная полиция берёт за горло подростка-хакера, тот, как правило, выкладывает всё.

К 1987 году, через какой-то год после того, как они всерьёз взялись за борьбу с хакерами, Секретная служба уже имела рабочие досье на всех, кто реально имел значение. К 1989-му у них были дела практически на каждую душу в американском цифровом андерграунде. Для правоохранительных органов проблема никогда не состояла в том, чтобы выяснить, кто такие хакеры. Проблема — понять, чем же они на самом деле занимаются, и ещё труднее — убедить общественность, что это действительно важно и опасно для общественной безопасности.

С точки зрения хакеров, копы в последнее время вели себя странно. Копы и их покровители из телефонных компаний просто не понимают современного мира компьютеров и боятся. «Они думают, что нас нанимают некие злые гении, руководящие шпионскими сетями», — рассказал мне один хакер. «Они не понимают, что мы делаем это не ради денег, а ради власти и знания». Сотрудников телефонной безопасности, выходящих на контакт с андерграундом, обвиняют в двойной лояльности и увольняют запаниковавшие работодатели. Молодой житель Миссури хладнокровно резюмировал противоречие: «Они слишком зависят от вещей, которые не понимают. Они отдали свои жизни компьютерам».

«Власть и знание» — мотивы, которые кажутся странными. «Деньги» — куда понятнее. Растут армии профессиональных воров, крадущих телефонные услуги ради наживы. Хакеры же занимаются этим, ну, ради власти и знания. Это сделало их более уязвимыми для поимки, чем уличных мошенников, ворующих коды доступа в аэропортах. Зато и куда более пугающими.

Возьмём всё более острые проблемы, создаваемые «системами электронных досок объявлений» (Bulletin Board Systems). «Доски» — это домашние компьютеры, подключённые к домашним телефонным линиям, способные хранить и передавать данные по телефону: тексты, программы, игры, электронную почту. Доски появились в конце 70-х, и, хотя подавляющее большинство из них абсолютно безвредны, некоторые пиратские борды быстро превратились в позвоночный столб цифрового андерграунда 80-х. Больше половины участников CyberView держали собственные борды. «Knight Lightning» вёл электронный журнал «Phrack», выходивший на многих подпольных бордах по всей Америке.

Борды — это тайна. Борды — это заговор. Бордам приписывают укрывательство: сатанистов, анархистов, воров, детских порнографов, арийских нацистов, религиозных сектантов, наркоторговцев — и, конечно, пиратов программного обеспечения, телефонных фриков и хакеров. Подпольные хакерские борды были не очень-то успокоительны — они нередко щеголяли ужасающими именами в стиле тяжёлого металла: «Speed Demon Elite», «Demon Roach Underground», «Black Ice». (Современные хакерские борды предпочитают вызывающие названия вроде «Uncensored BBS», «Free Speech», «Fifth Amendment».)

Подпольные борды несут контент, такой же отвратительный и пугающий, как, скажем, подпольные газеты 60-х — тех времён, когда йиппи ворвались в Чикаго и ROLLING STONE рассылал подписчикам трубочки для косяков. «Файлы анархии» — популярный контент на нелегальных бордах: как собрать трубчатую бомбу, как сделать коктейль Молотова, как синтезировать метедрин и ЛСД, как проникнуть в здание, как взорвать мост, самые эффективные способы убить человека одним ударом тупым предметом — и всё это сильно нервирует законопослушных граждан. Неважно, что все эти данные в открытом доступе в публичных библиотеках, где защищены Первой поправкой. Есть что-то в том, что они находятся на компьютере — где любой подросток с модемом и клавиатурой может это прочитать, распечатать и распространить, бесплатно, как воздух — в этом есть что-то жуткое.

«Brad» — нью-эйджевский язычник из Сент-Луиса, ведущий сервис «WEIRDBASE» в международной сети бордов FidoNet. Брэд погряз в бесконечном скандале: его читатели стихийно организовали подпольную железную дорогу, чтобы помочь нью-эйджевскому чернокнижнику вывезти из Техаса свою дочь-подростка — подальше от фундаменталистских христианских родственников по жене, убеждённых, что он убил жену и намеревается принести дочь в жертву Сатане! Скандал попал на местное телевидение Сент-Луиса. Копы заявились и допросили Брэда. Запах пачули Алистера Кроули тяжело висел в воздухе. Конца-края хлопотам не было видно.

Если ты занимаешься чем-то чудным и сомнительным и держишь борду об этом — жди настоящих неприятностей. В 1990 году была изъята борда издателя научно-фантастических игр Стива Джексона. Некая крионическая компания в Калифорнии, заморозившая женщину для посмертной консервации прежде, чем та была официально, э-э, «мёртвой», лишилась своих компьютеров. Торговцы оборудованием для выращивания наркотических растений лишились своих компьютеров. В 1990 году по всей Америке закрылись борды: Illuminati, CLLI Code, Phoenix Project, Dr. Ripco. Компьютеры изымаются как «улики», но поскольку полиция может держать их у себя неограниченное время для изучения, это вплотную приближается к конфискации и наказанию без суда. Это одна из весомых причин, по которой Митчелл Капор появился на CyberView.

Митч Капор — соизобретатель мегахита делового программного обеспечения LOTUS 1-2-3 и основатель□□гиганта Lotus Development Corporation. В настоящее время он является президентом недавно созданной группы по защите гражданских свобод в электронной сфере — Electronic Frontier Foundation. Капор, которому сейчас сорок лет, обычно носит гавайские рубашки и представляет собой типичного постхиппи-киберпространственного мультимиллионера. Он и главный юридический советник EFF «Johnny Mnemonic» прилетели на мероприятие на частном самолёте Капора.

Капор был вовлечён в хаос цифрового андерграунда поневоле — когда получил по почте незапрошенную дискету от нелегальной группировки «NuPrometheus League». Эти жулики (до сих пор не пойманные) похитили конфиденциальное фирменное программное обеспечение Apple Computer, Inc. и распространяли его повсюду, чтобы выдать коммерческие тайны Apple и унизить компанию. Капор решил, что дискета — розыгрыш, или, скорее всего, хитроумная попытка заразить его машины компьютерным вирусом.

Но когда по наводке Apple явилось ФБР, Капор был поражён масштабом их наивности. Вот они — хорошо одетые федеральные чиновники, вежливо обращающиеся к нему «мистер Капор» и готовые вести войну до последнего против злобных хакеров-мародёров. Они, судя по всему, не понимали, что именно «хакеры» создали всю индустрию персональных компьютеров. Джобс был хакером, Возняк тоже, даже Билл Гейтс, самый молодой миллиардер в истории Америки, — все «хакеры». Новый застёгнутый на все пуговицы режим в Apple вышел из себя, а федералы были готовы, но не имели ни малейшего понятия. Ладно, проявим снисходительность — федералы были «испытывающими трудности с ориентацией в ситуации». «Страдающими дефицитом клюшки». «По-иному информированными»...

В 70-е годы (рассказывал Капор притихшим и почтительно внимавшим молодым хакерам) он сам занимался «пиратством программного обеспечения» — как назвали бы это сегодня. Конечно, тогда «компьютерное программное обеспечение» ещё не было крупной индустрией. Но сегодня «хакеров» преследует полиция за то, что сами пионеры отрасли делали в порядке вещей. Капора это возмущало. Его собственная история, образ жизни его пионерской юности, высокомерно вычёркивался из исторической летописи нынешними корпоративными андроидами. Нынче люди даже морщились, когда Капор открыто заявлял, что в 60-е принимал ЛСД.

Немало молодых хакеров встревожилось этим признанием Капора и уставилось на него с изумлением, будто ожидая взрыва.

«Закон располагает только кувалдами, тогда как нам нужны штрафные квитанции за неправильную парковку и превышение скорости», — сказал Капор. В 1990 году страну охватила антихакерская истерия. Были предприняты колоссальные правоохранительные усилия против призрачных угроз. В Вашингтоне, в тот самый день, когда было объявлено об основании Electronic Frontier Foundation, в одном из комитетов Конгресса официально представили сюжет голливудского боевика «Крепкий орешек 2», в котором хакеры-террористы захватывают компьютерную систему аэропорта, — как если бы эта голливудская фантазия представляла реальную и непосредственную угрозу для Американской республики. Схожий хакерский триллер «Военные игры» был представлен Конгрессу в середине 80-х. Истерика никому не служила, порождая лавину глупых и неисполнимых законов, способных принести больше вреда, чем пользы.

Капор не хотел «замазывать разногласия» между своим Фондом и сообществом андерграунда. По твёрдому убеждению EFF, тайное проникновение в чужие компьютеры морально неприемлемо. Как и кража телефонных услуг, оно заслуживает наказания. Но не жестокого беспощадного преследования. Не уничтожения всей жизни молодого человека.

После живого и весьма серьёзного обсуждения вопросов цифровой свободы слова вся компания отправилась ужинать в итальянский ресторан в местном торговом центре — за счёт щедрого Капора. Высказавшись и внимательно выслушав других, Капор начал поглядывать на часы. В Бостоне его ждал шестилетний сын — с новой компьютерной игрой на Macintosh. Короткий телефонный звонок — и самолёт разогрет, Капор и его адвокат покидают город.

После того как силы благопристойности — такие как они были — удалились с поля, Legion of Doom с энтузиазмом взялся за «Мексиканские флаги». «Мексиканский флаг» — смертоносный многослойный коктейль из красного гренадина, белой текилы и зелёного мятного ликёра. Сверху наливается тонкий слой рома крепостью 75 градусов, поджигается, и всё это всасывается через соломинки.

Торжественный ритуал с огнём и соломинками вскоре был забыт по мере нарастания общего хаоса. Бродя из комнаты в комнату, толпа становилась всё более шумной и буйной, хотя и без особых инцидентов — тусовщики CyberView благоразумно захватили целое крыло гостиницы.

«Crimson Death», жизнерадостный молодой специалист по железу с детским лицом, проколотым носом и тремя серьгами, попытался взломать гостиничную телефонную АТС, но лишь обрезал телефонную связь в собственном номере.

Кто-то объявил, что в соседнем крыле дежурит полицейский. Последовала лёгкая паника. Пьяные хакеры столпились у окна.

В дверь соседнего крыла тихо скользнул джентльмен в коротком махровом халате и блестящих шёлковых боксёрах.

Соседнее крыло гостиницы захватили свингеры, проводившие там приватную оргию выходного дня. Это был сент-луисский клуб любителей свободных отношений. Выяснилось, что дежуривший при входе коп — это свингер при исполнении в нерабочее время. Он яростно угрожал разобраться с Doc Holiday. Ещё один свингер чуть не съездил по физиономии «Bill from RNOC», чья похотливая хакерская любознательность, разумеется, не знала предела.

Конкуренция была неравной. По мере того как выходные шли вперёд и алкоголь лился рекой, хакеры медленно, но верно инфильтрировали незадачливых свингеров, оказавшихся на удивление открытыми и терпимыми. В какой-то момент те даже пригласили группу хакеров присоединиться к веселью, хотя «им нужно было привести своих женщин».

Несмотря на сокрушительный эффект многочисленных «Мексиканских флагов», Comsec Data Security, судя по всему, не испытывала особых затруднений в этом отношении. Они отправились в центр города с цветной фотографией в TIME в кармане и вернулись с впечатляющей глубинной пробой сент-луисской женской половины человечества. Одна из новых знакомых, улучив

свободную минуту, влезла в номер Doc Holiday, опустошила его бумажник и стащила его диктофон Sony и все рубашки.

Жизнь замерла ради финального эпизода сезона STAR TREK: THE NEXT GENERATION. Серию смотрели затаив дыхание — а потом снова вернулись к изнурению свингеров. Bill from RNOC хитро выждал охрану и прокрался в здание, украсив все закрытые двери пятнами горчицы из дозатора.

В мутном свете похмельного воскресного утра один хакер с гордостью показал мне большой плакат с надписью от руки PRIVATE — STOP, похищенный им у незадачливых свингеров на выходе из их крыла. Каким-то образом ему удалось проникнуть в здание и непринуждённо влиться в компанию в одной из спален, где он вступил в долгую и весьма познавательную беседу с агентом по продаже авиабилетов из числа свингеров о безопасности аэропортовых компьютерных терминалов. Жена этого агента в тот момент лежала на кровати в объятиях третьего джентльмена. Выяснилось, что сама она много работает с LOTUS 1-2-3. Она была в восторге, узнав, что изобретатель программы Митч Капор был в этой самой гостинице в этот самый уикенд.

Митч Капор. Вот здесь? В Сент-Луисе? Ничего себе.

Жизнь странная штука.

Список гостей CyberView '91

```
                          CyberView '91 Guest List
                          ~~~~~~~~~~~~~~~~~~~~~~~~
Those known best by handles:                                  Those not:

Bill From RNOC / Circuit / The Conflict / Dead Lord           Dorothy Denning
Dispater / Doc Holiday / Dr. Williams / Cheap Shades          Michael Godwin
Crimson Death / Erik Bloodaxe / Forest Ranger / Gomez         Brad Hicks
Jester Sluggo / J.R. "Bob" Dobbs / Knight Lightning           Mitch Kapor
Malefactor / Mr. Fido / Ninja Master / Pain Hertz             Bruce Sterling
Phantom Phreaker / Predat0r / Psychotic Surfer of C&P
Racer X / Rambone / The Renegade / Seth 2600 / Taran King
Tuc <Tuc gets his own line just because he is cool!>
```

Phrack World News

Выпуск XXXIII / Часть первая

Автор: Compiled by Crimson Death

Обыск у Sir Hackalot силами полиции штата Джорджия

> *«Они были довольно злы, потому что ничего на меня не нашли.»*

Так прокомментировал ситуацию Sir Hackalot в разговоре с Crimson Death вскоре после столкновения с властями. Полиция штата Джорджия провела обыск у Sir Hackalot в рамках расследования компьютерного мошенничества. Странность заключается в том, что Sir Hackalot не проявлял никакой активности более года, и никаких реальных улик против него предъявлено не было. Силовики просто явились и изъяли его оборудование. Несмотря на то что Sir Hackalot не был арестован, его допросили о трёх других местных пользователях BBS, к которым в тот же день также наведались с визитом. В настоящее время Sir Hackalot ожидает возврата своего оборудования.

Не связан ли этот недавний обыск с печально известным изъятием публичного Unix-сервера Jolnet из Локпорта, штат Иллинойс, в рамках дела Phrack E911? Sir Hackalot был пользователем той системы, а в нынешних реалиях правоохранительного мышления одного этого факта вполне достаточно, чтобы оправдать очередное вторжение в гражданские права SH.

Справедливая сделка для кабельных пиратов

Автор: David Hartshorn

National Programming Service подписала соглашение с 12 программистами, представляющими 18 каналов, о льготном пакете конвертации для потребителей с незаконно модифицированными модулями VideoCipher II. Сделка будет предложена исключительно тем клиентам, которые переведут свои модифицированные модули VideoCipher II на модули VC II Plus в рамках Программы защиты потребительской безопасности (CSPP). Программа станет альтернативой нынешнему требованию NPS о минимальной покупке пяти услуг для клиентов, проходящих конвертацию.

Участвующие программисты согласились предоставить бесплатное программирование до конца 1991 года для клиентов, осуществляющих конвертацию. Для участия клиент должен купить годовую подписку, которая начнётся 1 января 1992 года и продлится до 31 декабря 1992 года. Любые дополнительные услуги, которые клиент захочет приобрести, начнут действовать с момента конвертации и будут действительны в течение 12 последовательных месяцев.

Президент NPS Майк Шрёдер заявил, что цель программы — перевести в разряд законопослушных плательщиков тех, кто сейчас не платит за контент. Если клиент сохранит модифицированный модуль, в конце 1992 года ему придётся потратить не менее 600 долларов на новый модуль плюс оплату программирования — ведь к тому времени он будет вынужден перейти на новую систему из-за потери звука в модифицированном устройстве. Если же клиент перейдёт сейчас на VC II Plus с MOM (Videopal), то чистые эффективные затраты составят всего 289,55 доллара (с учётом кредита на программирование от Videopal в размере 105 долларов и приблизительно 90 долларов

бесплатного программирования).

В пакет включены: ABC, A&E, Bravo, CBS, Discovery Channel, Family Channel, NBC, Lifetime, Prime Network, PrimeTime 24, TNN, USA Network, WPIX, WSBK и WWOR. Розничная цена пакета — 179,99 доллара.

Подробности: (800)444-3474

Clark Development Systems переходит к жёстким мерам

Автор: Crimson Death (сисоп Free Speech BBS)

Большинство из вас слышали о BBS-программном обеспечении PC-Board, однако, возможно, вы не знаете, что Clark Development Systems намерена делать с людьми, использующими нелегальные копии этой программы. Следующие сообщения появились на Salt Air BBS — основной BBS поддержки для зарегистрированных владельцев PC-Board.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Date: 08-19-91 (11:21)              Number: 88016 of 88042
  To: ALL                           Refer#: NONE
>From: FRED CLARK                      Read: HAS REPLIES
Subj: WARNING                       Status: PUBLIC MESSAGE
Conf: SUPPORT (1)                Read Type: GENERAL (A) (+)

********************************  WARNING  ********************************

Due to the extent and nature of a number of pirate PCBoard systems which have
been identified around the US and Canada, we are now working closely with
several other software manufacturers through the SPA (Software Publisher's
Association) in order to prosecute these people.  Rather than attempting to
prosecute them solely through our office and attorney here in Salt Lake, we
will now be taking advantage of the extensive legal resources of the SPA to
investigate and shut down these systems.  Since a single copyright violation
will be prosecuted to the full extent of $50,000 per infringement, a number of
these pirates are in for a big surprise when the FBI comes knocking on their
door.  Please note that the SPA works closely with the FBI in the prosecution
of these individuals since their crimes are involved with trafficking over
state lines.

The SPA is now working closely with us and the information we have concerning
the illegal distribution of our and other software publisher's wares.  Please
do not allow yourself to become involved with these people as you may also be
brought into any suits and judgements won against them.

We are providing this information as reference only and are not pointing a
finger at any one specific person or persons who are accessing this system.
This message may be freely distributed.

Fred Clark
President
Clark Development Company, Inc.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Date: 08-19-91 (08:28)              Number: 47213 of 47308
To: AL LAWRENCE                   Refer#: NONE
>From: DAVID TERRY                     Read: NO
Subj: BETA CODE IS NOW OFFLINE      Status: RECEIVER ONLY


PLEASE NOTE!      (This message is addressed to ALL!)

The beta code is now offline and may be offline for a couple of days. After
```

```
finding a program which cracks PCBoard's registration code I have taken the
beta code offline so that I can finish up work on the other routines I've been
working on which will not be cracked so easily.  I'm sorry if the removal
inconveniences anyone.  However, it's quite obvious that SOMEONE HERE leaked
the beta code to a hacker otherwise the hacker could not have worked on
breaking the registration code.

I'm sorry that the few inconsiderates have to make life difficult for the rest
of you (and us).  If that's the way the game is played, so be it.

P.S. -- We've found a couple of large pirate boards (who we have not notified)
        who should expect to see the FBI show up on their doorstep in the not
        too distant future.  Pass the word along.  If people want to play rough
        then we'll up the ante a bit ... getting out of jail won't be cheap!
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
```

Мне кажется, они пытаются всех запугать. Я думаю, у ФБР есть занятия поважнее, чем гоняться за сисопами, которые не купили PC-Board. По крайней мере, надеюсь на это. Сначала они ввели ключ, необходимый для запуска бета-версии PCB: его можно было получить только введя REGISTER на Salt Air, после чего система шифровала ваше имя и выдавала ключ для регистрации беты. В бета-код версии 14.5a также была встроена дата истечения срока, но уже в первый день выхода релиза на Salt Air пираты создали программу, позволявшую генерировать собственный ключ с любым именем. Судя по всему, и эта «новая» техника Clark Systems тоже не удалась — уже взломана. Может, им стоит сосредоточиться на том, как PC-Board функционирует в качестве BBS, а не на защите от взлома. Тем более что большинство пиратских систем в любом случае не работают на PC-Board!

Новый код города в Джорджии

Использование телефонной связи в Джорджии возросло настолько стремительно — вследствие роста населения и распространения таких сервисов, как факс и мобильная связь — что телефонных номеров начинает не хватать.

Southern \ Bell введёт новый код города — 706 — в Джорджии в мае 1992 года. Территория, ныне обозначаемая кодом 404, будет разделена.

Клиенты в зоне местных звонков Атланты продолжат использовать код 404. Клиенты за пределами зоны бесплатных местных звонков Атланты будут использовать код 706. Код 912 (Южная Джорджия) это изменение не затронет.

С 3 мая 1992 года по 2 августа 1992 года можно будет набирать КАК 706, ТАК И 404 для звонков в новую зону. После 2 августа 1992 года использование кода 706 станет обязательным.

О введении нового кода объявлено заблаговременно, чтобы клиенты могли подготовиться к изменениям.

Отключение 20 июля 1991 года

Из AT&T Newsbriefs (и дополнительных источников: San Francisco Chronicle (7/20/91, A5) и Dallas Times Herald (7/20/91, A20))

Некий хулиган, перехвативший и перенаправивший конфиденциальные телефонные сообщения из систем голосовой почты мэрии \, вынудил официальных лиц отключить телефонную систему. Город

приобрёл эту высокотехнологичную телефонную систему в 1986 году за 28 миллионов долларов. Однако чиновники забыли обязать каждого сотрудника использовать пароль, позволяющий только ему самому получать или переадресовывать голосовые сообщения из его «телефонного ящика», пояснил представитель AT&T Вёрджил Уайлди. В результате, по его словам, любой человек, понимающий принцип работы системы, может перенаправлять сообщения куда угодно, создавая полный хаос.

Арест, связанный с Red October

Авторы: Stickman, Luis Cipher, Orion, Haywire, Sledge и Kafka Kierkegaard

7 августа 1991 года в 8:00 утра в Уолнат-Крике, Калифорния, адвокаты Novell в сопровождении пяти федеральных маршалов провели обыск в доме Стивена Меренко, известного под псевдонимом Captain Ramius. Всё его компьютерное оборудование было конфисковано адвокатами Novell: диски, ленточные резервные копии и всё аппаратное обеспечение.

Официальные лица Novell подали аффидевит в Окружной суд США по Северному округу Калифорнии. Меренко обвиняется в незаконном распространении файлов Novell NetWare.

Следователь Novell заходил на BBS Меренко в качестве обычного пользователя 11 раз на протяжении нескольких месяцев. Он загрузил коммерческое программное обеспечение другой компании — с её разрешения — чтобы заработать доверие и в итоге скачать файл, являющийся частью Novell NetWare 386 версии 3.11, полная установка которого обходится более чем в 10 000 долларов.

Novell подала гражданский иск против BBS Red October. Поэтому, даже если Меренко будет признан виновным в том, что позволял другим пользователям скачивать защищённое авторским правом или коммерческое программное обеспечение, в тюрьму он не попадёт. Максимальное наказание по данному гражданскому делу составляет 100 000 долларов за каждое нарушенное произведение.

BBS Red October являлась площадкой групп THG/TSAN/NapE, имела четыре узла, 4 гигабайта жёсткого диска в онлайн-доступе и проработала четыре года.

Антипиратский натиск Novell

Обыск Novell на BBS Red October 7 августа 1991 года стал последним эпизодом продолжающейся два года антипиратской кампании. На той же неделе, когда произошёл обыск у Red October, была совершена облава и на оригинальный Wishlist BBS в Редондо-Бич, Калифорния. В апреле того же года (1991) Novell подала иск против семи реселлеров в пяти штатах, обвинённых в незаконной продаже NetWare. Осенью прошлого года было конфисковано оборудование двух жителей Теннесси, обвинённых в перепродаже NetWare через BBS. По словам Дэвида Брэдфорда, старшего вице-президента и главного юрисконсульта Novell, а также председателя Фонда защиты авторских прав Ассоциации издателей программного обеспечения, борьба с пиратством принесла свои плоды.

Лотерея может использовать Nintendo как альтернативный способ участия 1 сентября 1991 года

Взято из Minneapolis Star Tribune (раздел B)

> *«Ещё предстоит устранить ряд шероховатостей.»*

Вскоре жители Миннесоты смогут выигрывать джекпоты уже с 1993 года, не выходя из собственной гостиной. Следующим летом штат приступит к тестированию новой системы, которая позволит игрокам выбирать числа и покупать билеты дома с помощью игровой приставки Nintendo. Система, которую предстоит создать штату совместно с Control Data Corporation, будет в чём-то напоминать банковские операции через банкомат. Игроки будут использовать приставку Nintendo и государственный лотерейный картридж. Картридж подключится по телефону к компьютерной системе лотереи, позволяя участникам выбирать числа для Lotto America, Daily 3 и Gopher 5, а также играть в моментальные розыгрыши. Доступ к системе будет осуществляться через персональные коды безопасности или пароли. Неверные пароли будут отклоняться. Участие разрешено только взрослым.

Необходимо решить ряд вопросов: организация системы предоплаты для игроков, компьютерная безопасность и регистрация совершеннолетних. Nintendo-приставки имеются в 32% домохозяйств Миннесоты. Примерно половина пользователей приставок старше 18 лет. Участники летнего эксперимента получат приставку Nintendo, телефонный модем и лотерейный картридж.

---

15 000 писем по следам «Кукушкиного яйца» 8 сентября 1991 года

Перепечатано из RISKS Digest
Автор: Cliff Stoll

В 1989 году я написал «Яйцо кукушки» — правдивую историю о том, как мы выследили компьютерного взломщика. Полагая, что некоторые читатели захотят со мной связаться, я указал свой электронный адрес в предисловии к книге.

К моему изумлению, книга стала бестселлером, и я получил настоящий шквал электронной почты. За 2 года по четырём сетям (Internet, Genie, Compuserve и AOL) пришло около 15 000 писем. Это говорит о том, что от 1 до 3 процентов читателей отправляют письма по электронной почте.

Меня поразило разнообразие вопросов и комментариев: от замечаний по поводу моего употребления слова «хакер» до усовершенствованных рецептов печенья с шоколадной крошкой. Удивительно, но гневных и оскорбительных писем пришло совсем мало — несколько десятков.

Я старался отвечать на каждое письмо отдельно; в последнее время я создал несколько шаблонов для ответов на наиболее распространённые вопросы. Примерно 5% моих ответов не доходят до адресатов — интересно, скольким людям так и не удаётся достучаться до меня.

Я рад слышать от людей; приятно осознавать, как далеко разошлась книга (письма из Москвы, с Южного полюса, из Финляндии, Японии и даже из Беркли); но отныне я намерен больше времени уделять астрономии и меньше — ответам на почту.

С уважением, Cliff Stoll
cliff@cfa.harvard.edu
stoll@ocf.berkeley.edu

Мировые новости Phrack

Автор: Составлено Dispater

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN               Phrack World News             PWN
PWN                                             PWN
PWN            Issue XXXIII / Part Two          PWN
PWN                                             PWN
PWN             Compiled by Dispater            PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Legion of Doom открывает компанию

Ниже приводится подборка нескольких статей Майкла Александра из журнала ComputerWorld о компании Comsec Data Security, Inc.

Comsec Data Security, Inc.

Chris Goggans a/k/a Erik Bloodaxe 60 Braeswood Square
Scott Chasin a/k/a Doc Holiday Houston, Texas 77096
Kenyon Shulman a/k/a Malefactor (713)721-6500
Robert Cupps — не бывший хакер (713)721-6579 FAX

Хакеры улучшают имидж (стр. 124, 24 июня 1991 г.)

ХЬЮСТОН. Трое самопровозглашённых членов Legion of Doom — одной из самых печально известных хакерских группировок в США — заявили, что теперь хотят получать деньги за свои навыки. Вместе с бывшим биржевым трейдером они основали компанию по компьютерной безопасности Comsec Data Security, которая будет помогать корпорациям защищаться от хакеров.

«Мы занимаемся компьютерной безопасностью последние 11 лет — просто с другой стороны баррикад», — сказал Скотт Часин, который, по его словам, использовал ник Doc Holiday в качестве члена Legion of Doom. Группа прекратила существование в конце прошлого года, добавил Часин.

Новая компания планирует предлагать услуги тестирования на проникновение, аудита и обучения, а также продукты в области безопасности. «У нас есть информация, которую не купишь в книжных магазинах: мы знаем, почему хакеры взламывают, что ими движет, почему они любопытны», — сказал Часин.

Стартап уже встретил серьёзный скептицизм.

«Нанял бы я взломщика сейфов охранником в свой банк?» — задался вопросом Джон Блэкли, администратор информационной безопасности Capitol Holding Corporation в Луисвилле, штат Кентукки. «Если бы они вели себя прилично 5–10 лет, я бы, может, и пересмотрел своё мнение, но 12–18 месяцев назад они были хакерами, и теперь им ещё нужно себя доказать.»

«Не нанимаешь же ты прохиндеев, чтобы они смотрели на твою систему», — сказал Том Пелетье, специалист по информационной безопасности General Motors Corporation. «Legion of Doom —

известная антисистемная группировка, и хотя приятно видеть, что у них появилась капиталистическая жилка, GM не стала бы нанимать этих людей.»

У Comsec уже есть три контракта с компаниями из списка Fortune 500, сообщил Часин.

«Мне нравится их подход, и я предполагаю, что они легитимны», — сказал Норман Саттон, консультант по безопасности Leemah Datacom Corporation в Хейворде, Калифорния. Его фирма близка к подписанию дистрибьюторского соглашения с Comsec, добавил Саттон.

Федеральные правоохранители описывали Legion of Doom в обвинительных заключениях, ордерах на обыск и других документах как сплочённую группу примерно из 15 хакеров, члены которой перенаправляли звонки, похищали и изменяли данные, нарушали телефонную связь путём взлома телефонных коммутаторов и прочими способами.

Группа была основана в 1984 году, через её ряды прошли десятки членов. Около 12 бывших участников были арестованы за преступления, связанные с компьютерным взломом; трое бывших членов в настоящее время отбывают тюремное заключение; ещё как минимум трое находятся под следствием. Ни одному из основателей Comsec обвинения, связанные с компьютерными преступлениями, предъявлены не были.

(Статья сопровождается цветной фотографией всех четырёх основателей Comsec)

Предложение, от которого трудно отказаться? (стр. 82, 1 июля 1991 г.)

Том Пелетье, специалист по информационной безопасности General Motors в Детройте, говорит, что никогда не наймёт Comsec Data Security — консалтинговую компанию в области безопасности, основанную тремя бывшими членами Legion of Doom. «Не берёшь же ты неизвестно кого и не вручаешь им ключи от королевства», — сказал Пелетье. Крис Гоггинс, один из основателей Comsec, парировал: «У нас нет ключей от их королевства, но я навскидку знаю как минимум четырёх человек, у которых они есть.» Comsec предложила провести бесплатное тестирование на проникновение систем GM, чтобы доказать серьёзность намерений компании, сообщил Гоггинс. «Им нужно лишь подписать форму о том, что они не будут нас преследовать.»

Группа обманула экспертов по безопасности (стр. 16, 29 июля 1991 г.)

«Хьюстонская Comsec одурачила консультантов, чтобы собрать информацию о безопасности»

ХЬЮСТОН. Консультанты по компьютерной безопасности должны были быть начеку, однако как минимум шесть экспертов на прошлой неделе признали, что попались на удочку. По словам консультантов, они стали жертвами социальной инженерии со стороны Comsec Data Security, Inc. — недавно созданной консалтинговой компании в области безопасности.

Comsec выдавала себя за потенциального клиента, используя название Landmark Graphics Corporation — крупного хьюстонского издателя программного обеспечения, — чтобы собрать информацию о том, как составлять деловые предложения, проводить аудиты безопасности и прочие работы в сфере безопасности, сообщили консультанты.

Трое из четырёх основателей Comsec — самопровозглашённые бывшие члены Legion of Doom, одной из самых известных в стране хакерских группировок, по данным правоохранителей.

«В своём пресс-релизе они говорят: "Наша фирма выбрала уникальный подход к стратегии продаж"», — сказал один из консультантов, попросивший об анонимности по причине профессионального конфуза. «Что ж, социальная инженерия — это, безусловно, уникальная стратегия продаж.»

Социальная инженерия — это метод, широко используемый хакерами для получения информации от готовых помочь, но ничего не подозревающих сотрудников, которая затем может быть использована для взлома компьютерной системы.

«Это молодые ребята, которые понятия не имеют о ведении бизнеса, и они пытаются выудить эти знания у всех вокруг», — сказал Рэнди Марч, директор по консалтингу Computer Security Consultants, Inc. в Риджфилде, штат Коннектикут.

По словам консультантов, сбор информации под видом потенциального клиента — распространённый приём, однако Comsec нарушила принятую деловую этику, выдав себя за реально существующую компанию.

«Это довольно серьёзное нарушение деловой этики — прибегать к таким подлогам», — сказал Харди Морган, финансовый директор Landmark Graphics. «Они, может, и перестали взламывать, но методы работы у них не изменились.»

Морган сообщил, что его компания получила семь или восемь звонков от консультантов по безопасности, которые follow up'ились по информации, отправленной ими «Карлу Стивенсу» — якобы вице-президенту компании.

Всё та же история

Все консультанты рассказали Моргану одно и то же: их связался «Стивенс», который заявил, что готовится провести аудит безопасности и ему нужна информация, чтобы продать эту идею высшему руководству. «Стивенс» попросил консультантов подготовить подробное предложение с описанием этапов аудита безопасности, ценами и прочей информацией.

Затем консультантам было предписано отправить материалы экспресс-почтой на хьюстонский адрес, который впоследствии оказался домом двух основателей Comsec. В ряде случаев звонивший оставлял номер телефона, который при наборе оказывался постоянно занятым тестовым номером телефонной компании.

Морган сообщил, что «Стивенс» обнаружил детальные знания о компьютерных системах компании, известные лишь немногим сотрудникам. Хотя доказательств того, что системы компании были взломаны извне, нет, Landmark «укрепляет бастионы безопасности», сказал Морган.

Выдавать себя за потенциального клиента — не такой уж редкий способ сбора конкурентной информации, сказал Крис Гоггинс, один из основателей Comsec, некогда использовавший ник Erik Bloodaxe.

«Если бы мы не были теми, кто мы есть, это было бы вещью, не имеющей никакого значения», — сказал Гоггинс.

«Они определённо подтверждают, что звонили некоторым своим конкурентам», — сказал Майкл Кэш, адвокат, представляющий Comsec. «То, что они использовали Landmark Graphics, — это их ошибка, но это было первое название, которое пришло им в голову. Они никак не проникали в Landmark Graphics.»

Теперь и вы можете стать обладателем официальной футболки Legion of Doom. Это та самая рубашка, которая мгновенно разошлась на хакерской конференции «Cyberview» в Сент-Луисе. Присоединяйтесь к числу гордых владельцев, в числе которых лауреат премий писатель Брюс Стерлинг, добавив этот коллекционный предмет в свой гардероб. Эта профессионально изготовленная, стопроцентно хлопковая рубашка напечатана с обеих сторон. На лицевой стороне изображена надпись «Legion of Doom Internet World Tour», а также меч и телефон, пронзающие земной шар в стиле «череп и скрещённые кости». На обороте — слова «Hacking for Jesus», а также внушительный список «остановок тура» (интернет-сайтов) и цитата Алистера Кроули. Эта футболка продаётся исключительно как сувенирный товар и ни в коей мере не пытается прославить компьютерные преступления.

Стоимость рубашек — всего $15.00, включая доставку! Для зарубежных заказов доплата $5.00. Отправляйте чек или денежный перевод (никаких наложенных платежей, наличных или кредитных карт — даже если это действительно ваша карта :-) на имя Chris Goggans по адресу:

```
Chris Goggans
5300 N. Braeswood #4
Suite 181
Houston, TX 77096
```

Steve Jackson Games против Соединённых Штатов Америки

Статьи перепечатаны из Effector Online 1.04 и 1.08
1 мая 1991 г. / 24 августа 1991 г.

«Распространение Конституции на американское киберпространство»

С целью установления конституционной защиты электронных СМИ и получения возмещения ущерба за незаконный обыск, изъятие и предварительное ограничение публикации Steve Jackson Games и Electronic Frontier Foundation подали гражданский иск против Секретной службы США и других лиц.

1 марта 1990 года Секретная служба США едва не уничтожила Steve Jackson Games (SJG) — отмеченное наградами издательское предприятие в Остине, штат Техас.

Ранним утром агенты Секретной службы провели обыск в офисе SJG на основании незаконного и неконституционного ордера. Покидая офис, они забрали рукопись, готовившуюся к публикации, частную электронную почту и несколько компьютеров, включая аппаратное и программное обеспечение компьютерной BBS-системы SJG. При этом ни Джексон, ни его компания не были не только виновны в каком-либо преступлении, но даже и не являлись подозреваемыми. Обыск был проведён на основании «беспочвенного подозрения», что где-то в офисе Джексона «может находиться» документ, компрометирующий систему безопасности телефонной службы 911.

В последующие месяцы Джексон наблюдал, как бизнес, который он строил долгие годы, оказался на грани банкротства. SJG была успешным и авторитетным издателем книг и других материалов для приключенческих ролевых игр. Джексон также управлял компьютерной BBS для общения с клиентами и авторами, получения отзывов и предложений по новым игровым идеям. На доске объявлений также хранилась частная электронная почта ряда пользователей. Эта личная переписка была изъята в ходе обыска. Несмотря на неоднократные требования вернуть рукописи и оборудование, Секретная служба отказалась выполнить их в полной мере.

Более чем через год после обыска Electronic Frontier Foundation совместно с владельцем SJG Стивом Джексоном подала прецедентный гражданский иск против Секретной службы США, агентов Секретной службы Тимоти Фоли и Барбары Голден, помощника прокурора США Уильяма Кука и

Генри Клюпфеля.

«Это самое важное дело, возбуждённое на сегодняшний день, — сказал главный юрисконсульт EFF Майк Годвин, — для отстаивания конституционных прав пользователей компьютерных коммуникационных технологий. Оно установит конституционное измерение электронного самовыражения. Это также будет одним из первых дел, в котором Закон о конфиденциальности электронных коммуникаций применяется как щит, а не как меч, — закон, гарантирующий пользователям этого цифрового носителя ту же защиту частной жизни, которой пользуются те, кто пользуется телефоном и почтой США.»

Комментируя общую роль Electronic Frontier Foundation в этом деле и других вопросах, президент EFF Митч Капор заявил: «Мы действовали как организация, заинтересованная в защите несправедливо обвинённых. Но Electronic Frontier Foundation также намерена активно участвовать в установлении более широких принципов. Мы начинаем с этого дела, где вопросы ясны. Но за этим конкретным действием EFF также убеждена, что крайне важно привлекать к ответственности правительство, частных лиц и организации, нарушившие конституционные права граждан. Мы также надеемся, что это дело поможет развенчать мир компьютерных пользователей в глазах широкой общественности и расскажет людям о потенциале компьютерных сообществ.»

Интересы Стива Джексона и Electronic Frontier Foundation в этом деле представляют Харви А. Сильвергейт и Шэрон Л. Бекман из Silverglate & Good (Бостон); Эрик Либерман и Ник Позер из Rabinowitz, Boudin, Standard, Krinsky & Lieberman (Нью-Йорк); а также Джеймс Джордж-младший из Graves, Dougherty, Hearon & Moody (Остин, Техас).

Копии жалобы, незаконного ордера на обыск, заявлений Стива Джексона и Electronic Frontier Foundation, юридический информационный листок и другие соответствующие материалы можно получить по запросу в EFF.

Пресс-представителям и представителям электронных СМИ по запросу также были предоставлены следующее заявление Митчелла Капора и юридический информационный листок, подготовленный Шэрон Бекман и Харви Сильвергейтом из Silverglate & Good — юридической фирмы, занявшей центральное место в подаче данного иска.

«Почему Electronic Frontier Foundation подаёт иск в защиту Стива Джексона»

С этим делом Electronic Frontier Foundation начинает новый этап активных правовых действий. Мы намерены бороться за широкую конституционную защиту операторов и пользователей компьютерных электронных досок объявлений.

Крайне важно установить принцип, согласно которому компьютерные BBS и системы компьютерных конференций имеют право на те же права, гарантированные Первой поправкой, что и другие средства массовой информации. Не менее важно установить, что операторы досок объявлений — будь то частные лица или компании — не подлежат неконституционным, чрезмерно широким обыскам и изъятию какого-либо содержимого их систем, включая электронную почту.

Electronic Frontier Foundation также убеждена, что крайне важно привлекать к ответственности правительство, частных лиц и организации, нарушившие конституционные права других людей.

Mitchell Kapor,
Президент, The Electronic Frontier Foundation

«Юридический информационный листок: Steve Jackson Games против Секретной службы США и других»

Данный иск направлен на отстаивание прав небольшого успешного предпринимателя/издателя на ведение исключительно законной деятельности без неоправданного вмешательства государства. Также целью данного судебного разбирательства является твёрдое установление принципа, согласно которому законная деятельность, осуществляемая с помощью компьютерных технологий, включая компьютерные коммуникации и публикации, имеет право на те же конституционные гарантии, которые давно предоставлены печатным СМИ. Компьютеры и модемы — не менее, чем печатные станки, пишущие машинки, почта и телефоны, будучи средствами, которые американцы выбирают для общения друг с другом, — защищены нашими конституционными правами.

Фактические обстоятельства и стороны:

Стив Джексон из Остина, штат Техас, — успешный представитель малого бизнеса. Его компания Steve Jackson Games — отмеченный наградами издатель приключенческих игр и соответствующих книг и журналов. Помимо книг и журналов, SJG управляет электронной BBS (Illuminati BBS) для своих клиентов и всех, кто интересуется приключенческими играми и смежными литературными жанрами.

В числе истцов также указаны различные пользователи Illuminati BBS. Профессиональные интересы этих пользователей охватывают область от литературного творчества до компьютерных технологий.

Хотя ни Джексон, ни его компания не находились под подозрением в какой-либо преступной деятельности, компании был нанесён почти смертельный удар 1 марта 1990 года, когда агенты Секретной службы США при содействии других сотрудников правоохранительных органов провели обыск в её офисе, изъяв компьютерное оборудование, необходимое для работы издательского бизнеса. Правительство изъяло Illuminati BBS и все хранившиеся на ней коммуникации, включая личную электронную почту, заблокировав работу BBS более чем на месяц. Секретная служба также конфисковала публикации, защищённые Первой поправкой, в том числе черновики готовившейся к выходу книги ролевой игры GURPS Cyberpunk. Публикация книги была существенно отложена, пока сотрудники SJG переписывали её по более ранним черновикам. Эта фэнтезийная игровая книга, которую один из агентов нелепо назвал «руководством по компьютерным преступлениям», с тех пор разошлась тиражом более 16 000 экземпляров и была номинирована на престижную отраслевую премию. Никаких свидетельств преступной деятельности найдено не было.

Заявление на получение ордера, которое по требованию правительства находилось под seal в течение семи месяцев, свидетельствует о том, что агенты расследовали деятельность сотрудника компании, которого, по их мнению, вне работы занимался подозрительной деятельностью. Из заявления на ордер также следует, что Секретная служба не только не имела оснований полагать, что в SJG будут обнаружены какие-либо улики преступной деятельности, но и что правительство не сообщило магистрату, выдавшему ордер, что SJG является издателем и что планируемый обыск повлечёт предварительное ограничение конституционно защищённых свободы слова, печати и объединения.

Ответчиками по данному делу являются Секретная служба США и лица, которые, планируя и осуществляя этот грубо незаконный обыск и изъятие, злоупотребили полномочиями, предоставленными им федеральным правительством. В их числе — помощник прокурора США Уильям Дж. Кук, агенты Секретной службы Тимоти М. Фоли и Барбара Голден, а также Генри М. Клюпфель из Bellcore, принимавший активное участие в незаконной деятельности в качестве агента федерального правительства.

Эти ответчики — те же самые лица и организации, несущие ответственность за уголовное преследование в прошлом году электронного издателя Крейга Нейдорфа. Правительство в том деле предъявило обвинение в том, что публикация Нейдорфом материалов о системе улучшенной

экстренной связи 911 представляла собой межштатную перевозку похищенного имущества. Преследование завершилось в пользу Нейдорфа в июле 1990 года, когда Нейдорф доказал, что опубликованные им материалы были общедоступны.

Правовое значение:

Данное дело касается конституционных и законодательных прав издателей, ведущих свою деятельность в электронных СМИ, а не в традиционных печатных СМИ, а также прав физических лиц и компаний, использующих компьютерные технологии для общения и ведения личных и деловых дел.

Совершенно неоправданный обыск SJG со стороны правительства и изъятие его книг, журналов и BBS нарушили чётко установленные законодательные и конституционные нормы, в том числе:

• **Закон о защите конфиденциальности 1980 года**, который в целом запрещает правительству обыскивать офисы издателей в поисках материалов, являющихся продуктом их труда, и иных документов, в том числе хранящихся в электронном виде;

• **Первую поправку к Конституции США**, гарантирующую свободу слова, печати и объединения и запрещающую правительству подвергать цензуре публикации — как в печатных, так и в электронных СМИ;

• **Четвёртую поправку**, запрещающую неразумные правительственные обыски и изъятия, включая как общие обыски, так и обыски, проводимые без достаточных оснований полагать, что по указанному адресу будут обнаружены конкретные улики преступной деятельности;

• **Закон о конфиденциальности электронных коммуникаций и Федеральный закон о прослушивании**, которые вместе запрещают правительству изымать электронные коммуникации без обоснования и надлежащего разрешения.

ОБНОВЛЕНИЕ ПО ДЕЛУ STEVE JACKSON GAMES: ПРАВИТЕЛЬСТВО ПОДАЁТ ОТВЕТ

После нескольких задержек EFF наконец получила ответ правительства на иск Steve Jackson Games. Наши адвокаты тщательно изучают эти документы, и вскоре мы сможем дать более подробный комментарий.

Шэрон Бекман из Silverglate and Good, один из ведущих адвокатов по данному делу, заявила:

«В целом этот ответ не содержит для нас ничего неожиданного. Напротив, он подтверждает, что события по данному делу разворачивались именно так, как мы и предполагали. Наша позиция по-прежнему очень сильна. Кроме того, по мере продвижения вперёд становится всё очевиднее, что дело Steve Jackson Games станет переломным судебным процессом в части распространения конституционных гарантий на данный носитель.»

Федералы арестовывают «установщика логической бомбы» (1 июля 1991 г.)

by Michael Alexander (ComputerWorld) (стр. 10)

САН-ДИЕГО. Федеральные агенты на прошлой неделе арестовали обиженного программиста по обвинению в предполагаемой закладке логической бомбы, предназначенной для уничтожения программ и данных, связанных с программой правительства США по ракете Atlas стоимостью в

миллиард долларов. По данным правоохранителей, программист надеялся быть заново нанятым корпорацией General Dynamics — его бывшим работодателем и производителем ракеты — в качестве высокооплачиваемого консультанта для устранения нанесённого ущерба.

Майкл Дж. Лауффенбургер, 31 год, которому предъявлено обвинение в закладке бомбы, был арестован после того, как 10 апреля 1991 года его коллега случайно обнаружил разрушительную программу, обезвредил её и уведомил властей. По имеющимся данным, Лауффенбургер запрограммировал логическую бомбу на срабатывание в 18:00 24 мая 1991 года в период праздничных выходных Memorial Day с последующим самоуничтожением.

Лауффенбургеру предъявлены обвинения в несанкционированном доступе к компьютеру федерального значения и покушении на компьютерное мошенничество. В случае осуждения ему грозит до 10 лет лишения свободы и штраф в размере 500 000 долларов. Лауффенбургер заявил о своей невиновности и был освобождён под залог в 10 000 долларов.

В обвинительном заключении говорится, что в период работы в отделении General Dynamics Space Systems Division в Сан-Диего Лауффенбургер являлся главным архитектором программы базы данных, известной как SAS.DB и PTP, использовавшейся для отслеживания наличия и стоимости деталей, применяемых при строительстве ракеты Atlas.

20 марта он создал программу под названием Cleanup, которая при запуске удалила бы программу PTP, удалила бы другой набор программ, использовавшихся для ответа на запросы правительства об информации, а затем самоуничтожилась бы без следа, — об этом рассказал Митчелл Дембин, помощник прокурора США, ведущий данное дело.

Пентагон открыт для хакеров!

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                         PWN
PWN              Phrack World News          PWN
PWN                                         PWN
PWN          Issue XXXIII / Part Three      PWN
PWN                                         PWN
PWN            Compiled by Dispater         PWN
PWN                                         PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Составил Dispater

---

9 сентября 1991 года
Источник: USA Today

ФБР расследует заявление израильского подростка о том, что во время войны в Персидском заливе он взломал компьютер Пентагона. Израильская газета в воскресенье назвала хакера — им оказался 18-летний Дери Шрайбман. В пятницу он был задержан в Иерусалиме, однако отпущен без предъявления обвинений. По сообщению «Едиот Ахронот», Шрайбман читал секретные сведения о ракете «Пэтриот» — применённой в этой войне впервые для уничтожения иракских «Скадов» в полёте.

«Нигде не было написано "Вход воспрещён"», — приводит слова Шрайбмана, сказанные полиции, цитата из газеты. — «Там просто написано: "Добро пожаловать"». Официальный ответ Пентагона: ведомство относится к «компьютерной безопасности очень серьёзно», заявил в воскресенье пресс-секретарь, капитан ВВС Сэм Гриззл. Аналитики говорят, что это не первый случай проникновения в военные компьютеры. «Не существует... системы защиты, которая была бы на 100% надёжной», — говорит Алан Сабровски, профессор Родс-колледжа в Мемфисе.

Telesphere подана в суд кредиторами; компания вынуждена объявить о банкротстве

Источник: Telecom Digest (comp.dcom.telecom)

В понедельник, 19 августа, компания Telesphere Communications, Inc. была подана в суд группой из десяти кредиторов, утверждающих, что компания, наиболее известная своими услугами 900-х номеров, не оплачивает свои счета. Группа кредиторов — все они являются информационными провайдерами, пользующимися номерами 900 через Telesphere, — заявляет, что компания задолжала им в общей сложности два миллиона долларов за услуги, оказанные через телефонные развлекательные линии, спортивные прогнозы, гороскопы, линии откровенных разговоров и прочие сервисы. По их словам, Telesphere на протяжении нескольких месяцев не выплачивает им причитающиеся комиссионные. Группа кредиторов обратилась в суд по делам о банкротстве США в штате Мэриленд с требованием инициировать в отношении Telesphere принудительное банкротство по главе 7 (то есть ликвидацию компании и распределение всех активов между кредиторами).

Компания заявила, что намерена противостоять попыткам кредиторов вынудить её объявить о банкротстве. Представитель компании также сообщил, что более чем с 50 процентами информационных провайдеров, которым причитаются выплаты, уже достигнуто соглашение.

Telesphere признала серьёзные проблемы с денежным потоком, однако объяснила их большим количеством безнадёжных долгов, которые местные телефонные компании выставляют ей к возмещению. Когда конечные пользователи 900-х сервисов не платят местному оператору, тот в свою очередь не платит 900-оператору — в данном случае Telesphere, — а расходы списываются с резервного депозита, обязательного для каждого информационного провайдера.

Однако информационные провайдеры оспаривают размер выставляемых им безнадёжных долгов. Они утверждают, что Telesphere никогда должным образом не документировала ежемесячно предъявляемые им претензии. По меньшей мере в одном случае информационный провайдер подал в суд на конечного пользователя за неоплату и выяснил в ходе допроса, что пользователь местному оператору заплатил, а местный оператор, в свою очередь, произвёл выплату Telesphere. В своём иске против компании информационные провайдеры утверждают, что Telesphere фактически получила оплату по многим позициям, которые были выставлены им как безнадёжные долги, «и, по всей видимости, использует эти деньги для финансирования иных аспектов своей деятельности за счёт одной из категорий кредиторов — а именно информационных провайдеров...». Telesphere отвергла эти обвинения.

Прежде базировавшаяся в Чикагском регионе (г. Оук-Брук, штат Иллинойс), Telesphere ныне расположена в Роквилле, штат Мэриленд.

Хищение телефонных услуг у корпораций стремительно растёт

28 августа 1991 года
Автор: Эдмунд Л. Эндрюс (New York Times)

«Это, безусловно, крупнейший сегмент мошенничества в сфере связи», — говорит Рами Абухамдех, независимый консультант и до недавнего времени исполнительный директор Ассоциации по борьбе с мошенничеством в области связи в Маклине, штат Вирджиния. «Всё это оборудование просто ждёт ваших звонков, и управляется людьми, для которых защита телекоммуникаций не является профессией».

Mitsubishi International Corp. сообщила о потерях в размере 430 000 долларов прошлым летом — преимущественно из-за звонков в Египет и Пакистан. Procter & Gamble Co. потеряла 300 000 долларов в 1988 году. Нью-йоркская администрация по людским ресурсам лишилась 529 000 долларов в 1987 году. Секретная служба, расследующая подобные телефонные преступления, сообщает, что сейчас еженедельно получает от трёх до четырёх официальных жалоб и набирает дополнительных специалистов по телефонным коммуникациям.

В своём единственном на сегодняшний день решении по данному вопросу Федеральная комиссия по связи постановила в мае, что оператор дальней связи вправе взыскать оплату за незаконные звонки с пострадавшей компании. В ходе резонансного дела Mitsubishi, поданного в июне, компания предъявила AT&T иск на 10 миллионов долларов в окружном суде США в Манхэттене, утверждая, что AT&T не только произвела оборудование, через которое посторонние лица получили доступ к телефонной сети Mitsubishi, но и получала плату за его обслуживание.

Для небольших компаний, располагающих меньшими ресурсами, чем Mitsubishi, подобные проблемы могут быть финансово сокрушительными. Так, компания WRL Group, небольшой разработчик программного обеспечения из Арлингтона, штат Вирджиния, обнаружила у себя счета за 5 470 звонков, которых она не совершала, — этой весной, после того как установила бесплатный номер 800 и автоответчик с голосовой почтой для приёма входящих вызовов. Менее чем за три недели злоумышленники набрали счёт на 106 776 долларов у US Sprint, подразделения United Telecommunications.

Прежде большую часть расходов несли операторы дальней связи, поскольку кражи объяснялись уязвимостями их сетей. Однако теперь телефонные компании настаивают на том, что за оплату звонков должны отвечать клиенты, так как те не приняли надлежащих мер по обеспечению безопасности своего оборудования.

Компания Consumertronics, торгующая по каталогу из Аламогордо, штат Нью-Мексико, продаёт брошюры за 29 долларов, описывающие общие принципы взлома голосовой почты и конкретные уязвимости различных моделей. В брошюру включён список номеров 800 с указанием типов подключённых к ним систем голосовой почты. «Это в образовательных целях», — заявил владелец компании Джон Уильямс, добавив, что принимает Mastercard и Visa. Аналогичные сведения можно почерпнуть из журнала «2600 Magazine» — ежеквартального издания, посвящённого телефонному хакингу и выпускаемого в Мидл-Айленде, штат Нью-Йорк.

Procter & Gamble

22 августа 1991 года
Источник: Telecom Digest

12 августа 1991 года The Wall Street Journal опубликовал материал на первой полосе о расследовании, которое полиция Цинциннати провела в отношении телефонных записей по запросу компании Procter & Gamble Co. — с целью установить, кто мог передать внутреннюю информацию в редакцию Wall Street Journal. Речь шла о публикациях предположительно за период с 1 марта по 10 июня 1991 года, что побудило P&G обратиться за защитой по закону штата Огайо о коммерческой тайне. В связи с возможным нарушением этого закона Большое жюри выдало повестку о предоставлении записей определённых телефонных звонков, совершённых в питтсбургский офис Wall Street Journal из района Цинциннати, а также на домашний номер журналиста этого издания. Для понимания контекста: питтсбургский офис Wall Street Journal представлял интерес предположительно в силу того, что именно журналист Алеша Суэзи была ответственна за освещение деятельности Procter & Gamble и работала из питтсбургского офиса.

13 августа 1991 года подписчик CompuServe Рик Бёрд Лент пересказал материал журнала другим участникам SIG TELECOM.ISSUES на CompuServe и задал следующий вопрос:

> *«Очевидно, что записи фиксируют лишь факт соединения двух номеров, содержание разговоров для проверки недоступно. Но что если у CB была голосовая почта? И если телефонные расследования ведут к шлюзам онлайн-сервисов (MCI Mail, CIS) — распространяется ли на них также действие судебной повестки?»*

На момент публикации поста г-на Лента было известно, что Wall Street Journal сообщал о большом количестве телефонных записей, переданных Cincinnati Bell местной полиции. Точные цифры в комментарии Лента не фигурировали. Поэтому я не могу утверждать, публиковались ли в журнале какие-либо конкретные данные 12 августа 1991 года — пока не ознакомлюсь с самой статьёй.

14 августа 1991 года журнал опубликовал дополнительные подробности о расследовании полиции в связи с возможным нарушением закона Огайо о коммерческой тайне. Wall Street Journal сообщил, что на основании повестки Большого жюри полиция Цинциннати обязала Cincinnati Bell предоставить телефонные записи за 15-недельный период — в общей сложности 40 миллионов звонков из префиксов 655 и 257 в зоне 513. По данным Wall Street Journal, повестка была выдана всего через четыре рабочих дня после выхода 10 июня 1991 года статьи о проблемах в подразделениях P&G по производству продуктов питания и напитков.

В среду [14 августа 1991 года] Associated Press сообщило, что P&G не ожидает предъявления обвинений по результатам полицейского расследования возможных нарушений закона Огайо о коммерческой тайне. Пресс-секретарь P&G Терри Лофтус был процитирован следующим образом: «Расследование не дало результатов и фактически сворачивается». Лофтус пояснил, что компания «провела внутреннее расследование, которое ничего не выявило. Это был наш первый шаг. Завершив внутреннее расследование, мы решили передать дело в полицейское управление Цинциннати».

Попытки Associated Press связаться с Гэри Армстронгом, главным следователем по делу P&G, предпринятые до 14 августа 1991 года, успехом не увенчались. Никто другой из полицейского управления Цинциннати комментировать ситуацию AP не стал.

15 августа 1991 года Associated Press подготовило краткое изложение материала Wall Street Journal от 14 августа 1991 года о расследовании в отношении P&G. Помимо этого, AP процитировало ещё одного представителя P&G — Сидни МакХью. Г-жа МакХью в целом повторила заявление Лофтуса от 13 августа, добавив: «Мы уведомили местное полицейское управление Цинциннати о случившемся, поскольку посчитали, что, возможно, было совершено преступление, нарушающее законодательство Огайо. Полиция приняла решение о проведении самостоятельного расследования».

После выхода материала в журнале от 14 августа AP вновь безуспешно попыталось связаться с офицером Гэри Армстронгом. У прокурора Артура М. Нея оказался неопубликованный домашний номер телефона, и поэтому, по сведениям AP, в среду вечером [14 августа 1991 года] он был недоступен для комментариев.

За последние несколько недель в прессе появилось немало материалов об обвинениях в том, что P&G, местное большое жюри и/или полиция Цинциннати нашли «нестандартный» способ обойти Первую поправку к Конституции США. В своём обзоре материала Wall Street Journal от 14 августа, опубликованном 15 августа, AP процитировало цинциннатского адвоката Роберта Ньюмана, специализирующегося на вопросах Первой поправки: «Нет никаких оснований делать повестку такой широкой. Это вызывает тревогу». Ньюман также выразил мнение: «P&G не нужно вторгаться в жизнь сотрудников P&G, не говоря уже об остальных».

В том же материале AP цитируются слова регионального координатора Американского союза гражданских свобод Цинциннати Джима Роджерса: «Повестка затрагивает каждого, кто находится в зоне 513. Если я позвонил в The Wall Street Journal, какое дело до этого P&G?»

В более позднем репортаже AP от 18 августа 1991 года клевлендский адвокат Дэвид Марбургер был процитирован с замечанием: «Меня беспокоит вопрос: если бы аналогичная проблема возникла у небольшой компании в Цинциннати, стали бы правоохранительные органы вмешиваться и помогать ей?» Марбургер также добавил, что произошедшее стало для него «неожиданностью», имея в виду характер полицейского расследования.

В ответ командир отдела уголовных расследований полиции Хейдон Томпсон сказал Cincinnati Business Courier: «Procter & Gamble — это новостной повод, но не по этой причине мы проводим данное расследование». Представитель P&G Терри Лофтус отверг мнение о том, что компания отреагировала чрезмерно, пояснив: «Мы делаем то, что должны, — защищаем интересы акционеров. А когда мы считаем, что совершено преступление, — передаём эту информацию в полицию».

Тем временем Cincinnati Post опубликовал редакционный комментарий за минувшие выходные, назвав просьбу P&G о полицейском расследовании «примерно тем же, что и когда самый здоровый игрок в уличный баскетбол кричит о фоле, стоит кому-то его едва задеть». Наконец, AP в материале от 18 августа 1991 года обратило внимание на «тесные отношения» между городом Цинциннати и P&G. В подтверждение этой близости мэр Цинциннати Дэвид Манн был

процитирован следующим образом: «Традиция здесь такова: в любом гражданском или благотворительном начинании нужно заполучить P&G на борт — и все остальные выстроятся в очередь». Как человек, проживший вблизи Цинциннати восемь лет, я могу подтвердить: отношения Procter & Gamble с городом действительно были весьма тесными.

Хакер обвиняется в Австралии

13 августа 1991 года

По сообщению Associated Press из Мельбурна, 20-летний студент специальности «информатика» Нахшон Эвен-Хаим обвиняется в магистратском суде Мельбурна в несанкционированном доступе к одному из компьютеров CSIRO (государственного исследовательского института Австралии), а также по 47 эпизодам незаконного использования телефонной сети Telecom Australia для несанкционированного доступа к компьютерам различных американских организаций — в том числе университетов, NASA, Лаборатории Лоуренса Ливермора и компании Execucom Systems Corp. из Остина, штат Техас, где он, по имеющимся данным, уничтожил важные файлы, включая единственную опись активов компании. По словам обвинения, полиция записала телефонные разговоры, в которых Эвен-Хаим описывал некоторые из своих действий. В рамках продолжающегося досудебного разбирательства обвиняемый пока не заявил о признании или непризнании вины.

«Позвони Папе» завоёвывает популярность в США

17 августа 1991 года
Источник: Toronto Star

Ватикан тянется к миру, однако Канада, похоже, не торопится откликнуться. В США, набрав номер 900, можно ежедневно получать духовное напутствие от Папы Иоанна Павла II. Многоязычный сервис, официально авторизованный Ватиканом и ласково прозванный «Позвони Папе», носит официальное название «Christian Messaging From the Vatican». Представитель Bell Canada сообщил, что подобного номера в Канаде не существует. Тем не менее Дес Бёрдж, директор по коммуникациям Архиепархии Торонто, считает этот платный для американских абонентов сервис хорошим способом помочь людям ощутить свою связь с Папой. (Toronto Star)

PWN: Краткие заметки

1. Agent Steal сидит в тюрьме в Техасе в ожидании суда по различным обвинениям, включая мошенничество с кредитными картами и угон автомобилей.

---

2. Blue Adept находится под следствием по подозрению во взломе нескольких компьютерных систем, в том числе в Технологическом институте Джорджии и NASA.

---

3. Control C был вызван повесткой Федерального большого жюри для снятия отпечатков пальцев, фотографирования и предоставления образца почерка — после того как сотрудники Michigan Bell и осуждённые члены Legion of Doom (в частности, The Leftist и Urvile) дали показания.

Control C ранее работал в службе безопасности Michigan Bell вплоть до января 1990 года, когда был уволен приблизительно в то же время, что и обыски у Knight Lightning, Phiber Optic и ряда других лиц. Control C в преступлении не обвинён, однако статус дела остаётся неопределённым.

---

4. Гейл Тэкерей, специальный помощник прокурора округа Марикопа, штат Аризона, назначена вице-президентом компании Gatekeeper Telecommunications Systems, Inc. — стартапа в Далласе. Тэкерей была одним из следователей, участвовавших в операции «Сан-Девил» — широко освещавшейся в прессе совместной операции штата и федеральных властей по борьбе с компьютерными преступлениями. Gatekeeper разработала устройство, которое, по заявлению компании, является надёжной защитой от компьютерных хакеров. Тэкерей заявила, что её уход мало скажется на расследовании, однако один из следователей, пожелавший остаться анонимным, сказал, что это верный признак того, что расследование идёт на спад. (ComputerWorld, 24 июня 1991, стр. 126)

---

5. «Байки из электронного леса» — Ларри Уэлз, известный подпольный карикатурист 1960-х годов, ударился в киберпанк. Недавно он посвятил целый выпуск своего нового комикса «Cherry» приключениям хакера, которую засасывает в компьютер и которая вынуждена взламывать путь сквозь Страну Воза. (ComputerWorld, 1 июля 1991, стр. 82)

---

6. Фонд свободного программного обеспечения (FSF), созданный на основе философии свободного ПО и свободного доступа к компьютерам, отключил часть своих машин от Интернета после того, как злонамеренные хакеры неоднократно удаляли файлы организации. FSF также закрыл открытые аккаунты в системе, чтобы перекрыть доступ хакерам, использовавшим её как плацдарм для атак на другие компьютеры по всему Интернету — после многочисленных жалоб от других пользователей сети. Ричард Столлман, директор FSF и известный хакер старой закалки, отказался поддерживать решение своих сотрудников — хотя и не стал его отменять — и, лишённый доступа по паролю, был вынужден перейти на автономную машину без телекоммуникационных связей с внешним миром. (ComputerWorld, 15 июля 1991, стр. 82)

---

7. Руководители ряда пользовательских групп Apple Macintosh получили письмо от ФБР с просьбой об содействии в деле о похищении ребёнка. ФБР запрашивает руководителей групп, чтобы выяснить, нет ли среди их членов женщины, подходящей под описание участницы спора об опеке над ребёнком. Почему ФБР считает беглянку пользователем Macintosh — неясно. (ComputerWorld, 29 июля 1991, стр. 90)

---

8. Компьютерные вирусы, атакующие IBM PC и совместимые с ними компьютеры, приближаются к своеобразному рубежу. По словам известного немецкого эксперта по компьютерным вирусам Клауса Брунштайна, в ближайшие несколько месяцев их список перешагнёт отметку в 1 000. Он опубликовал перечень известных вредоносных программ для систем MS-DOS, включающий 979 вирусов и 19 троянских программ. Итого — 998 единиц «вредоносного ПО» (malware), как называет их Брунштайн. (ComputerWorld, 29 июля 1991, стр. 90)

---

9. «Высокий полдень на электронном фронтире» — осенью этого года Верховный суд США может вынести решение по апелляции на приговор по делу «США против Роберта Таппана Морриса». Напомним: Моррис — бывший студент Корнеллского университета, случайно парализовавший Интернет с помощью программы-червя. Моррис также упоминается в книге «Киберпанк» Кэти Хафнер и Джона Маркоффа.

---

10. «Компьютеризированные уголовные досье ФБР» — в системах уголовных записей ФБР и штатов по-прежнему имеются «значительные пробелы в автоматизации и полноте данных», — сообщает Бюро по оценке технологий Конгресса в исследовании «Автоматизированная проверка данных о покупателях огнестрельного оружия: проблемы и варианты решений». По оценке OTA, создание системы полной и точной «мгновенной» проверки по имени данных государственных и федеральных уголовных баз при покупке оружия займёт несколько лет и обойдётся в 200–300 миллионов долларов. ФБР до сих пор получает сведения о решениях суда (обвинительный приговор, прекращение дела, оправдание и т. д.) лишь по половине из 17 000 записей об арестах, ежедневно вносимых в систему. Таким образом, «примерно половина арестов в базе уголовных дел ФБР ("Межштатный идентификационный индекс", он же "Triple I") не имеет информации о судебных решениях. ФБР с трудом удаётся получать эти данные». OTA отметило, что наиболее близкая к системе мгновенной проверки практика для покупателей оружия действует в Вирджинии: из каждых 100 покупателей 94 получают одобрение в течение 90 секунд, однако из шести отказов четыре-пять впоследствии оказываются основаны на ошибочных данных (совпадение имён, арест за тяжкое преступление, не повлёкший обвинительного приговора, или судимость за проступок, не лишающая права на владение оружием). (62 стр., 3 долл. — OTA, Washington, D.C. 20510-8025, 202/224-9241; или U.S. Government Printing Office, Stock No. 052-003-01247-2, Washington, D.C. 20402-9325, 202/783-3238). (Privacy Journal, август 1991, стр. 3)

• -

Основанный в 1974 году, Privacy Journal — независимое ежемесячное издание, посвящённое вопросам конфиденциальности в эпоху компьютеров. Освещает законодательство, правовые тенденции, новые технологии и общественные настроения, влияющие на конфиденциальность информации и право личности на неприкосновенность частной жизни.

Подписка — 98 долларов в год (125 долларов для зарубежных подписчиков); предусмотрены специальные льготные тарифы для студентов и других категорий читателей. Принимаются телефонные и почтовые заказы, оплата кредитными картами.

Privacy Journal
P.O. Box 28577
Providence, Rhode Island 02908
(401)274-7861