Phrack RU issue 037

Русская версия Phrack, выпуск 037. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; Unix/Linux, BSD, Windows NT и администрирование систем; социальная инженерия, carding, физический доступ и практические схемы; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: КАК ПОДПИСАТЬСЯ НА ЖУРНАЛ PHRACK; Phrack Loopback; Pirates' Cove («Пиратская бухта»); Исследование Information America; Как уйти от штрафа за радар (Часть 1 из 2): «Ваш день в суде»; Card-O-Rama: Технология магнитных полос и не только; Руководство пользователя VAX/VMS. Часть II из III; Основные команды системы VOS; Дело CompuServe: шаг вперёд в защите онлайн-сервисов по Первой поправке; WeenieFest '92: Встреча с Джоном Маркоффом; Phrack World News; Phrack World News; Phrack World News; Phrack World News.

Больше крутых материалов в моём телеграм канале @grogrigs

КАК ПОДПИСАТЬСЯ НА ЖУРНАЛ PHRACK

Автор: Dispater

```
                              ==Phrack Inc.==

                  Volume Four, Issue Thirty-Seven, File 1 of 14

                                Issue XXXVII Index
                                _________________

                                 P H R A C K   3 7

                                   March 1, 1992
                                   _____________

    ~Promoting The Free Exchange Of Information In The New World Disorder~
```

«Я слишком крут для своего Phrack... Только представьте!»

Оглядываясь на Том III, отметим несколько исторических дат, связанных с Phrack:

• **24.02.89** — Выпущен Phrack 24.
• **18.01.90** — Агенты Секретной службы США провели обыск у Knight Lightning как редактора Phrack.
• **23.01.90** — Агенты Секретной службы США провели обыски у Phiber Optik и Acid Phreak.
• **06.02.90** — Knight Lightning и The Prophet преданы суду федерального округа в Чикаго, штат Иллинойс. The Prophet, The Leftist и The Ur-Vile преданы суду федерального округа в Атланте, штат Джорджия.
• **15.02.90** — Knight Lightning заявил о признании себя НЕВИНОВНЫМ.
• **01.03.90** — Агенты Секретной службы США провели обыски у Erik Bloodaxe, The Mentor и в компании Steve Jackson Games.

Phrack вернулся! Добро пожаловать в первый выпуск Phrack Тома Четвёртого! В этом номере представлена статья «Exploring Info-America» («Исследование Инфо-Америки») авторства The Omega и White Knight. Среди прочих примечательных материалов — ДВЕ статьи от Count Zero, очередная часть серии Black Kat о VAX/VMS, а также информация о системе VOS от Dr. No-Good! Кроме того, начиная с этого выпуска, мы вводим новую постоянную рубрику Pirate's Cove («Пиратская бухта») от Rambone — о пиратском сообществе. И наконец, особая благодарность новейшему члену редакции Phrack — Spirit Walker — за помощь в подготовке этого выпуска.

В Phrack Loopback вас ждёт небольшой сюрприз. Наш старый приятель THE DICTATOR переписывается с Knight Lightning и со мной по сети. Да, всё верно! Dale Drew, сыгравший ключевую роль в разоблачениях в ходе OPERATION SUN-DEVIL («Операция Солнечный Дьявол») и следивший за нашими друзьями на SummerCon '88, — вернулся. И, верите или нет... он хочет Phrack! Говоря об «Операции Солнечный Дьявол»: федеральное правительство вынесло обвинительный приговор первому подсудимому — подробности в Phrack World News (Часть 2).

Phrack World News (Часть 3) содержит всё, что вам нужно знать о том, как региональные телефонные компании (Regional Bell Operating Companies) относятся к нашим частным хобби-BBS; а в следующем выпуске мы расскажем, что ВЫ можете с этим сделать! Также в следующем номере ждите предварительных подробностей о SummerCon '92!!! Появится ли там снова ESP?

Прежде чем слухи разойдутся снова, поясню, что происходит с руководством Phrack. Crimson Death решил уйти из Phrack и заняться своей новой BBS на базе UNIX — CyberWaste! Если вы хотите оставаться на связи с Crimson Death, пишите пока на cdeath@GNU.AI.MIT.EDU. Однако следите за

именем хоста CyberWaste: @DEMONSEED.COM!

Вот, пожалуй, и всё на сей раз. Если вы собираетесь на Вторую конференцию по компьютерам, свободе и приватности (a/k/a CFP-2) в Вашингтоне, О.К. (18–20 марта 1992 года) — Knight Lightning и я будем там и рады вас увидеть!

С уважением,
Dispater
phracksub@stormking.com

Распространение Phrack теперь осуществляется с помощью программного обеспечения Listserv. Все адреса из списка рассылки Phrack, существовавшего до того, как вы получили это письмо, были удалены из списка.

Если вы хотите вновь подписаться на Phrack Inc., следуйте этим инструкциям:

1. Отправьте электронное письмо на адрес `LISTSERV@STORMKING.COM`. Письмо должно быть отправлено с того аккаунта, на который вы хотите получать Phrack.

2. Оставьте поле «Subject:» пустым.

3. Первая строка вашего письма должна содержать:
`SUBSCRIBE PHRACK`

4. НЕ оставляйте свой адрес в поле имени! (Это поле предназначено исключительно для использования сотрудниками PHRACK, поэтому, пожалуйста, указывайте полное имя.)

После получения подтверждения вы будете добавлены в список рассылки Phrack. Если вы не получите это сообщение в течение 48 часов, отправьте ещё одно. Если вы ВСЁ ЕЩЁ не получите ответа, свяжитесь с `SERVER@STORMKING.COM`.

Будущие выпуски вы будете получать от `PHRACK@STORMKING.COM`.

При возникновении любых проблем с этой процедурой обратитесь на `SERVER@STORMKING.COM` с подробным описанием.

Вам должно прийти подтверждение подписки.

FTP-САЙТЫ PHRACK

Ниже приведён краткий список надёжных сайтов. Более полный список появится в следующем выпуске.

Организация	Адрес / IP	Путь
Washington University in St. Louis	WUARCHIVE.WUSTL.EDU / 128.252.135.4	/doc/policy/pub/cud/Phrack
Electronic Frontier Foundation	EFF.ORG / 192.88.144.3	/pub/cud/Phrack
University of Chicago	CHSUN1.SPC.UCHICAGO.EDU / 128.135.46.7	/pub/cud/phrack

---

СОДЕРЖАНИЕ

Electronic Frontier Foundation	EFF.ORG / 192.88.144.3	/pub/cud/Phrack
University of Chicago	CHSUN1.SPC.UCHICAGO.EDU / 128.135.46.7	/pub/cud/phrack

---

И напоследок... Ninja Master, это для тебя!

> *«Но ты понимаешь — ты никто. Ты — никто.*
> *И ты сам выбрал это по собственной воле.*
> *Юридически — официально — тебя просто не существует!»*
> *Из книги «Наездник на ударной волне» (The Shockwave Rider)*

Phrack Loopback

Автор: Phrack Staff

Phrack Loopback — это форум для вас, читателей, где можно задавать вопросы, высказывать проблемы и обсуждать любые интересующие темы. Здесь также редакция Phrack делится рекомендациями, рецензируя различные примечательные материалы: журналы, программное обеспечение, каталоги, оборудование и прочее.

Обзор журнала 2600, осень 1991

```
PO Box 752                              Тарифы для частных подписчиков:
Middle Island, NY 11953                 США : 4 номера (1 год) $21.00
InterNet: 2600@well.sf.ca.us            Заруб.: 4 номера (1 год) $30.00
Phone: 516-751-2600                     Корпоративные / деловые тарифы:
Fax: 516-751-2608                           : 4 номера (1 год) $50.00
```

Автор: Dispater

Журнал 2600 издаётся с 1984 года Эммануэлем Голдстайном. «The Hacker Quarterly» насчитывает чуть менее 50 страниц и выходит с глянцевыми обложками в формате 5,5"×8,25". В 2600 вы найдёте привычные статьи о хакинге и фрикинге, а также несколько приятных сюрпризов. Журнал нередко затрагивает темы, напрямую не связанные с хакингом или фрикингом, но весьма полезные. Есть и рубрика «письма редактору», и даже раздел купли-продажи.

В данном номере, в частности, есть статья о замках Simplex и о том, насколько легко их открыть. Приложены фотографии вскрытых почтовых ящиков Federal Express, оснащённых замками Simplex. Следующим по интересности оказался материал о тех странных маленьких полосках на деловых письмах. «Postal Hacking» не расскажет вам, как отправлять письма бесплатно, зато объяснит, как ускорить доставку без каких-либо затрат. Кроме того, там была статья «Protecting Your Social Security Number», недавно опубликованная в Phrack Inc. Issue 35.

Также имеется статья о видеозаписи с голландскими хакерами, взламывавшими военные системы. 2600 даже предлагает приобрести видеокассету, частично показанную в скандальном шоу Джеральдо [придурок]. Хороша и статья о психологии в хакерском мире. Несколько фрейдистский анализ сотрудницы службы безопасности, боящейся «монтирования» (своего жёсткого диска), «проникновения» (в её систему), «заражения» (вирусами) и «головной боли» (из-за хакеров) — весьма проницателен и очень смешон. Помимо всего перечисленного, по страницам 2600 рассыпаны разрозненные крупицы полезной информации (списки COCOT, NUA, ANI, небольшие полезные программы, интересные деловые и правительственные формы от читателей и т. д.).

Наконец, о том, на что все жалуются, — о цене. Но у 2600 есть отличное предложение для бедных студентов-хакеров: если вы присылаете материал в 2600 Magazine и он публикуется, вы получаете бесплатную подписку. По-моему, звучит честно! Может, нам стоит попробовать то же самое с Phrack?

В целом 2600 Magazine — ОТЛИЧНОЕ издание, которое настоятельно рекомендуется к прочтению.

Что у вас на уме?

Некоторые люди так и не понимают намёков

Недавно Phrack Inc. получил запрос на подписку от некоего человека, сыгравшего ключевую роль в операции Sun-Devil. Возможно, вы знаете его по BBS, где он нередко использовал псевдонимы «The Dictator» или «Blind Faith». Мы знаем его как Дейла Дрю. Кто бы мог подумать, что он осмелится попросить у нас подписку? Лично я не мог в это поверить.

На случай, если вы забыли или последние два года провели в норе: Дейл Дрю был платным осведомителем Секретной службы США, который тайно позволил правительственным агентам снять на видео SummerCon '88 в Сент-Луисе, штат Миссури.

Ниже приведён пример сообщения Дейла Дрю / The Dictator / Blind Faith на BBS. Он утверждает, что является со-сисопом на Lutzifer, и несёт прочий вздор.

```
ZDDDDD Packet Switching Networks/PSNs DDDD September 27, 1991 at 8:52 pm DDDDD?
3 Left by  Blind Faith (Level 40)Title: Telenet (No Replies)3
3 > <-702-> CoSys on Lutz (Tymnet) <To: Anyone3
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDY

Пара моментов:

Есть ли среди вас, помимо меня, кто-нибудь, знакомый с отладчиками Tymnet и/или
Telenet? (Xray, TDT2, Isis и т. д.)...  TDT2 на Telenet — отличная вещь, потому
что в частных сетях у них вшитый пароль... всегда пускает. Раньше было и в
публичной сети, но примерно два года назад они это исправили.
(может, не везде, но я больше не могу найти те, что до сих пор работают)

sprint — это NUI Tymnet, ведущий в Telenet

Telenet меняет формат своих хостов. Они добавляют лишнюю цифру (слишком много
хостов, видимо). Так что следите за этим. Я не знаю точно когда, но представитель
службы поддержки клиентов оказался ОЧЕНЬ полезным..

--BF
"What, me worry?"
[Message menu] Command (?/Help):
```

Дейл Дрю в настоящее время работает в службе безопасности Tymnet. Для получения дополнительной информации о деятельности Дейла Дрю настоятельно рекомендуется прочитать Computer Underground Digest (CUD), выпуск 3.02.

Зная, что Knight Lightning с удовольствием (усмешка) услышит от своего старого приятеля, я переслал письмо на электронный адрес Knight Lightning'а.

```
From: ddrew@btnagns.Tymnet.COM (Dale Drew)
To: phrack@stormking.com

Я хотел бы, чтобы моё имя было добавлено в список рассылки Phrack. Раньше я
получал Phrack из Чикагского университета, но было бы удобнее получать номера
непосредственно по почте.

Кроме того, я был крайне разочарован тем, что Phrack решил снизить стандарты
качества информации, опубликовав содержимое Phrack issue #36.

Dale Drew
Sr. Information Security Specialist

From: Knight Lightning
To: Dale Drew

Дейл (DicKtator / Blind Faith) — должен признать, что у тебя есть смелость
написать моим друзьям в Phrack и попросить подписку.

Ты — платный осведомитель Секретной службы. Ты подставляешь людей под арест.
Ты берёшь чужое доверие и предаёшь его. Ты лжец и мошенник. Знаешь, Дейл, я
даже не мог себе такого представить — пока примерно за пару недель до суда у меня
```

не появилась возможность посмотреть те видеозаписи SummerCon '88. Ты и твои фашистские дружки из Секретной службы точно провели нас (даже если на тех плёнках нет ничего противозаконного... Отличный способ потратить деньги налогоплательщиков).

Так что когда ты писал в Phrack на днях, ты и правда думал, что тебя не узнают? Ты рассчитывал на тёплый приём?

Когда я был редактором Phrack, у меня была политика приглашать сотрудников правоохранительных органов и специалистов по безопасности в список рассылки Phrack. Я больше не руковожу Phrack, но моя рекомендация нынешним редакторам очень проста. Они не должны отправлять Phrack тебе... не потому что ты связан с правоохранительными органами... потому что ты — НИЗШАЯ ФОРМА ЖИЗНИ и заслуживаешь только нашего глубокого презрения.

Короче говоря — я говорю от имени модемного сообщества в целом: "ПОШЁЛ ТЫ, ПРИДУРОК!" Ползи обратно под свой камень, откуда вылез, и катись прямо в ад!

Knight Lightning

From: Dale Drew
To: Knight Lightning

Крейг,

Похоже, ты не так зрел, как мне давали понять. Отсутствие в списке рассылки Phrack меня не волнует — это было бы лишь удобством. Phrack, как ты, несомненно, знаешь, доступен по всей сети, и я просто продолжу получать копии оттуда.

Я понятия не имел, что ты и новоиспечённые редакторы Phrack решили стать настолько инфантильными. Но, видимо, ничего не изменится, и мне грустно это видеть.

--Dale

Вещественные доказательства

From: John Higdon
To: Dispater

> Dispater пишет:
>
> Думаю, в юмористическом выпуске Phrack (36) будет топ-10 самых глупых вещей,
> которые любит изымать Секретная служба.

Я консультирую защиту по предстоящему делу и имел возможность ознакомиться с «доказательствами», изъятыми у обвиняемого дома. Примечательные предметы: модель ракетной пусковой установки, местные карты улиц, около дюжины телефонов типа 2500, пишущая машинка, предварительно записанные аудиокассеты. При этом один интересный предмет оставили: консоль TSPS.

Задумываешься, что (если вообще что-то) проносится в голове у офицеров, исполняющих ордер.

John

Защити свою BBS от федералов — как бы не так!

Уверен, многие из вас видели текстовые файлы о том, как сделать вашу BBS более защищённой. Один такой файл, гуляющий по сети, принадлежит Babbs Boy из Midnight Society. Один из членов нашей редакции Phrack показал этот документ Майку Годвину из EFF — адвокату. Вот его

комментарии:

```
From: Mike Godwin
To: Phrack Inc.

(По поводу некоторых файлов о том, как «защитить» свою BBS от федералов:)

>  Начнём с экрана входа: если ФЕДЕРАЛЫ хотят что-то от вашей доски,
>  они обязаны предоставить 100% точную информацию.

Это неверно. Спросите законодателей, осуждённых в ходе операций «подставы».
На самом деле, насколько я могу судить по беглому просмотру этого документа,
абсолютно ни одна часть так называемых «юридических» советов не соответствует
истине.

Сотрудники правоохранительных органов, скрывающие свою личность (например,
«агенты под прикрытием»), постоянно получают допустимые доказательства.

--Mike
```

Diet Phrack полезен для здоровья

```
From: Gordon Meyer
To: Dispater
Subject: Phrack #36

Спасибо, что прислал Diet Phrack! Похоже, кое-что из прежней энергии наконец
возродилось. Мне особенно понравилось вступление — в нём чувствуется
интенсивность, гордость и юмор. Очень напоминает некоторые «старые» выпуски
PHRACK. Здорово!

До встречи,
Gordon R. Meyer
```

Анонимная почта

```
From: Creeping Death

>        Привет, ребята. Хотел спросить, не могли бы вы рассказать, как
> отправлять анонимную почту. Я слышал, что это возможно, но здесь в
> университете, похоже, никто понятия не имеет. Пожалуйста, помогите.
>
```

Есть много способов это сделать. Один из них описан ниже. Однако помните, что существуют и другие варианты.

Dispater

Анонимная почта через SMTP с помощью простого shell-скрипта

Автор: The Artful Dodger

Этот файл предназначен для тех, кто хочет или любит отправлять анонимную почту через сеть, но не хочет возиться с сырыми командами SMTP. Поэтому я написал простой shell-скрипт, который берёт всё на себя. Программа весьма проста, но я всё равно дам краткое объяснение.

Запустить программу можно двумя способами: просто набрав имя, под которым вы её сохранили, или это же имя плюс адрес получателя. В любом случае вы в итоге окажетесь у приглашения «From:». Если просто нажать Enter, программа подставит ваш userid@hostname. В противном случае можно ввести всё, что вздумается.

Далее появится запрос о том, какой хост использовать для SMTP. Если вы используете свой текущий хост, просто нажмите Enter — он выбирается по умолчанию. Иначе введите любой хост, который допускает telnet на порт 25. Затем нужно выбрать редактор для составления письма. По умолчанию — vi, но можно использовать любой другой. В общем-то, это и всё из интерактивных действий. После ввода этих данных программа создаёт файл tmpamail1 и дописывает в него четыре строки. Первая — «helo amail», поскольку SMTP-порт некоторых хостов не принимает команды, пока не представишься. Вторая — «mail from: » и имя отправителя (реальное или вымышленное). Третья — «rcpt to: » и адрес получателя. Последняя — просто слово «data».

Конечно, все эти команды можно ввести вручную, но зачем, если есть программа? Затем программа запускает редактор и создаёт файл tmpamail2. После того как вы закончите составлять сообщение и выйдете из редактора, программа спросит, хотите ли вы отправить это сообщение — что, думаю, не требует пояснений. Затем программа дописывает «.» и «quit» в tmpamail2, после чего присоединяет tmpamail2 к tmpamail1 — и у вас получается один файл со всей необходимой информацией заголовка для отправки сообщения через SMTP и выхода из него. Затем программа посылает всё это на порт 25 указанного хоста. И если всё пройдёт хорошо, адресата будет ждать письмо. И последнее: программа удаляет оба временных файла по завершении. Надеюсь, вам всем понравится этот небольшой скрипт — он немного упрощает отправку анонимной почты.

The Artful Dodger

```
#! /bin/csh -fB
### This is a simple shell script for easy use of anonymous mail.  To run the
### program just save it and delete everything up until the #! /bin/csh -fB
### line.  Then just type the name you save it as or the name and whoever
### you will be mailing.  e.g.  amail bill@some.university.edu or just amail.
###
###   The Artful Dodger

if ($1 != "") then
   set mto=$1
else
   echo 'To: '
   set mto=$<
endif

echo -n 'From: '
set mfrom=$<

echo -n 'Use which host for smtp (return for '`hostname`') ? '
set usehost=$<

echo -n 'Use which editor (return for vi)? '
set editor=$<
if($editor =="") then
   set editor=vi
endif

if ($mfrom == "") then
   set mfrom=`whoami`'@'`hostname`
endif

echo 'helo amail' >> tmpamail1
echo 'mail from: '$mfrom >> tmpamail1
echo 'rcpt to: '$mto >> tmpamail1
echo 'data' >> tmpamail1

$editor tmpamail2
clear
```

```
echo -n 'Are you sure you want to send this? '
set yorn=$<
if($yorn == 'y') then
   echo . >> tmpamail2
   echo quit >> tmpamail2
   cat tmpamail2 >> tmpamail1
   telnet $usehost  25 < tmpamail1 > /dev/null
   echo 'Mail has been sent to: '$mto
   echo '                  From: '$mfrom
endif
rm tmpamail1 tmpamail2
```

Pirates' Cove («Пиратская бухта»)

Новая постоянная колонка журнала Phrack Magazine

Автор: Rambone

---

1) Введение

Для начала позвольте представиться. Я известен под хэндлом Rambone, веду борд в районе Среднего Запада. Уверен, что подобная колонка станет неожиданностью для многих читателей — однако после разговоров с Dispater'ом, множеством читателей и людьми из хакерского и пиратского мира мы пришли к следующему выводу: пиратство и *Warez Dudez* прошли долгий путь за последние пять лет и являются неотъемлемой частью андеграунда. Читаете ли вы журнал ради информации о хакинге, фрикинге или даже ради тех отличных историй о взломах — я думаю, эта колонка станет добрым дополнением к Phrack Magazine.

---

2) Вирусы

Какой-нибудь доверчивый простак скачивает программу, распаковывает её и, вместо того чтобы проверить на вирусы, сразу запускает. Решив, что игрушка унылая, удаляет её и выключает компьютер — ложится спать без малейших тревог. На следующий день пытается включить машину, а та выдаёт: «Bad or missing COMMAND.COM» — или что-нибудь в этом роде.

Это лишь один из примеров того, что случается с бесчисленным множеством людей в пиратском мире — они не ожидают, что впереди их ждут часы мучительного восстановления жёсткого диска. Несмотря на то что вирусы являются распространённой проблемой уже много лет, по-настоящему заметный след в пиратском мире они начали оставлять лишь в последнее время.

Будь то склоки между группировками или просто одинокий тип, которому нечем заняться, кроме как выпустить трейнер с грёбаным вирусом внутри, — это в любом случае недопустимо. Те, кто несёт ответственность за распространение подобного программного обеспечения, по моему мнению, являются главными виновниками: они прекрасно понимают, что собираются сделать, и не испытывают никаких угрызений совести, рассылая заражённое ПО. Сам факт того, что единственный способ, который они видят для сведения счётов с другой группой — это распространение программы с вирусом или трояном, говорит об их полном кретинизме.

Я не призываю группировки прекращать или, напротив, продолжать свои внутренние разборки. Они были, есть и будут. Я говорю о другом: у групп есть ответственность — вести себя достойно и прекратить распространение программ с вирусами и троянами. С другой стороны, большинство сисопов не рассылают заражённые программы намеренно. Их загружают на BBS, а когда обнаруживают — уже поздно: файлы успели разойтись по всей стране.

Моя главная забота — о рядовых пользователях. Если бы всё ограничивалось одними лишь проблемами между группировками, это было бы ещё полбеды. Но безответственно выпускать программу с вирусом — это одна из самых низких форм мести в пиратском мире, и с этим нужно

покончить, чтобы вернуть пиратству тот уровень, который был до начала эпидемии «бомб».

Примечание пользователю

Большинство вирусов встречаются в трейнерах и кряках — будьте внимательны с каждым из них. Лучший способ проверки — `PKUNZIP -T` в сочетании со сканером McAfee's Virus Scanner; я нахожу его наиболее надёжным. Если кто-то испытывает трудности с временной распаковкой `.ZIP`, `.ARJ` и подобных архивов, у меня есть отличный `.BAT`-файл для этого — опишу его в одном из следующих выпусков. НЕ запускайте программу, не просканировав хотя бы директорию, куда вы её распаковали, — хотя сканирование самого ZIP-архива значительно надёжнее.

---

3) Сети (Nets)

В некоторых выпусках мы будем обсуждать новые и уже устоявшиеся сети. Сначала объясню, что такое сеть (net): это группа сообщений, рассылаемых по сетям через модем. Они принимаются BBS и направляются в соответствующие конференции для чтения сисопом и пользователями. Одна из новых и перспективных сетей, которая могла бы заинтересовать широкий круг сисопов, называется «CyberCrime». Она ищет борды, совместимые с Fido, а именно: LSD, Telegard, WildCat, Tag, Remote Access, Omega, QBBS, Paragon, Infinity, Revelation, Cypher и др. Эта сеть активно занимается темами P/H/C/A (фрикинг/хакинг/кардинг/анархия), а также пиратскими дискуссиями. Кроме того, она подключена к общим обсуждениям TSAN и ведёт работу по установлению связей сисопов с другими сетями. Если вас интересует вступление в эту сеть — подайте заявку на Infinite DarkNess, (305)LOOK4-IT; логин: Cybercrime, пароль: Death — и следуйте инструкциям. Заполните заявку на CyberCrime node. MidNight Sorrow позвонит на ваш борд (система должна работать в полноценном режиме), войдёт в систему и загрузит CYBER.ARJ — официальный стартовый комплект CyberCrime. После этого вы в деле.

---

4) BBS-доски

В связи с арестами NSHB/USA/TGR я решил воздержаться от каких-либо обзоров BBS. Надеюсь, паника вокруг этих дел утихнет, и мы сможем вернуться к этой теме.

---

5) Новости

Как всем уже известно, The NotSoHumble Babe и The Grim Reaper, сисоп BBS The Void, были арестованы за кардинг. Об этом уже написали и рассказали во всех возможных изданиях, поэтому скажу лишь одно: это вызвало волну паранойи в пиратском сообществе, и несколько хороших бордов в результате закрылись. Поскольку я не говорил с Эми и Майком лично, в детали вдаваться не буду. Эми (NSHB) являлась членом USA (United Software Association), Майк (TGR) вёл BBS под названием The Void и был дистро-сайтом INC. Но пока я не получу ответа от одного человека из USA, я не стану пересказывать чужие слухи — продолжение следует в следующем выпуске.

---

6) Новые варезы

Игра месяца:

```
                    Star Trek:  25th Anniversary

  Графика       [CGA/EGA/VGA]
  Звук          [ADL/SNB/PCSPK]
  Управление    [Мышь/Джойстик/Клавиатура]
  Взломана      [EMC/USA/Razor?]
  Поставщик     [?]
  Взломана      [отдельный кряк]
  Защита        [Dox Check]
```

Три крекинговые группы заявили, что выпустили её первыми. Поскольку я видел релиз от EMC раньше остальных — пусть даже на несколько часов — именно им я отдаю пальму первенства. Эта игра из тех, что понравится вам вне зависимости от того, являетесь ли вы поклонником «Звёздного пути» или нет. На открывающем экране «Энтерпрайз» стремительно мчится по вашему монитору, а музыка из оригинального саундтрека гремит из динамиков (если у вас есть звуковая карта). Затем вас бросают в учебный бой с другим кораблём, и приключение начинается. Звёздный флот направляет вас на первую миссию — спасти планету. Графика великолепна и напоминает новые игры в стиле Sierra с нарисованными задними планами. Игра сочетает приключенческую составляющую с несколькими сценариями космических сражений; для комфортного управления в боевых сценах рекомендуется мышь. Головоломки очень сложные, однако на местных BBS уже есть и прохождение, и чит. Так что если застрянете — помощь найдётся, нужно только поискать.

Примечание

Вот и всё на сегодня. Мне пришлось убрать около 60% этого материала, потому что многие сейчас предпочитают держаться в тени ещё пару месяцев. Ждите более подробных материалов в следующих выпусках: интервью, обзоры BBS, профили и советы по взлому защит.

Исследование Information America

Автор: The Omega (Restricted Data Transmissions / RDT) и White Knight (Cult of the Dead Cow / -cDc-)

```
:===:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:===:
:==                                                                        ==:
:==                    Exploring Information-America                       ==:
:==                   :=============================:                      ==:
:==                                 by                                     ==:
:==              The Omega                         White Knight            ==:
:==  Restricted Data Transmissions (RDT)      Cult of the Dead Cow (-cDc-)  ==:
:==                                                                        ==:
:==                                                                        ==:
:==                 "Truth Is Cheap, But Information Costs!"               ==:
:==                                                                        ==:
:==                       ------------------------                         ==:
:==                                                                        ==:
:==        "Textfiles:  We're in it for the girlies and the money."        ==:
:==                                                                        ==:
:==  Monkey-Boyz!                                                1/24/92  ==:
:===:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:===:
```

Введение

Эпоха информации вступила в зрелость лишь совсем недавно: мощные технологии баз данных стали значительно доступнее в реализации (достаточно вспомнить, как MCI смогла поддерживать базу данных людей, которым вы звоните чаще всего, в рамках программы Friends & Family), и параллельно с этим сбор информации стал всё более масштабным и пристальным. После производства оружия и наркоторговли «сбор информации», пожалуй, является одним из наиболее прибыльных предприятий в Америке.

На протяжении последних двух десятилетий кредитные бюро, телефонные компании и прямые маркетологи в совокупности накопили полные потребительские профили более чем на 150 миллионов американцев. Но по большей части эта информация использовалась лишь для прогнозирования будущих покупательских привычек потребителей или, что ещё хуже, для их формирования. В целях выставления счетов и маркетинга актуальные адреса, номера телефонов и сведения о домохозяйстве сохранялись как сопутствующие данные.

Однако до недавнего времени вся эта информация НЕ БЫЛА КОММЕРЧЕСКИ ДОСТУПНА В ЕДИНОЙ БАЗЕ ДАННЫХ, специально ориентированной на нужды правоохранительных органов, частных сыщиков, охотников за беглецами и юристов. По нашим сведениям, Information America является первым доступным сервисом, использующим ранее собранные данные с явной целью предоставлять актуальные сведения о местонахождении, личные профили и информацию о правовых затруднениях (банкротство, судебные иски и т. д.) как можно большего числа американцев.

Information America

> *«Проводите ли вы проверку биографии, разыскиваете ли свидетеля, занимаетесь ли поиском пропавших должников или собираете материалы для суда — [Info America] предоставляет вам быстрый и удобный способ получить информацию о людях по всей стране... нажатием одной клавиши.»*

Information America (IA) предоставляет единый сервис, чьи базы данных перекрёстно индексируют Национальный файл смены адреса Почтовой службы (NCOA), клиентские данные крупных издательских и прямых маркетинговых компаний, записи актов о рождении, данные водительских удостоверений, телефонные справочники, списки избирателей, различные государственные документы и многое другое. IA заявляет, что в системе хранятся в режиме онлайн (и поддерживаются в возможно актуальном состоянии) более 111 миллионов имён, 80 миллионов домохозяйств и 61 миллион телефонных номеров.

Вместе с доступом IA к дополнительным базам данных — таким как Dun & Bradstreet, данные секретаря штата и материалы из до 49 государственных ведомств — вы можете:

• Найти пропавшего ответчика или свидетеля и получить список соседей для дальнейшего расследования.
• Найти руководителей корпораций, акционеров или пропавших наследников.
• Найти человека в целях взыскания задолженности.
• Найти родителя-беглеца, похитившего ребёнка у другого родителя в ходе споров об опеке.
• Установить корпоративные аффилиации физического лица.
• Изучить записи о банкротствах, судебных исках, обременениях и судебных решениях в отношении физических и юридических лиц.
• Изучить документы, поданные в Комиссию по ценным бумагам и биржам (SEC), и деловые новости из крупных информационных агентств.
• Собрать информацию о руководителях, структуре собственности, финансовом положении и отношениях материнской и дочерних компаний.
• Определить, имеет ли иностранная корпорация зарегистрированного агента для местного судопроизводства (например, для вручения судебного иска).

Вход в систему IA

Доступ к Information America осуществляется через местный дозвон Tymnet (7-E-1); используйте идентификатор терминала `a` и введите `infoam` в приглашении «please log in:». IA отобразит знакомые запросы VAX — `USERNAME` и `PASSWORD`. Имена пользователей вида `BIDAxxxx` (где x — цифра) распознаются VAX как учётные записи IA и, при верном пароле, запускают скрипт интерактивной среды базы данных. Учётные записи, обходящие интерактивную среду и предоставляющие обычный доступ к командной оболочке VAX, должны существовать, однако ни White Knight, ни я этот путь не исследовали.

После входа вас встречает примерно следующее:

```
----------------------------[ Title Screen ]----------------------------

     Welcome to VAX/VMS version V5.4-2 on node ALAMO
 Last interactive login on Thursday, 17-SEP-1991 12:47


                COMPUTER EQUIPMENT SELECTION MENU


 What type of computer equipment or software are you using?


      1.  PERSONAL COMPUTER (or 100% IBM compatible)
      2.  PERSONAL COMPUTER with WESTMATE SOFTWARE
      3.  WESTLAW TERMINAL
      4.  OTHER EQUIPMENT
      5.  NETWORK SYSTEM (TTY)

     99.  EXIT OFF SYSTEM
 Please call Information America's Client Support at 1-(800) 235-4008
```

```
 if you would like assistance.


Please specify number: 1

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
*                                                                       *
*                W E L C O M E    T O   T H E                         *
*                                                                       *
*      I N F O R M A T I O N   A M E R I C A   N E T W O R K            *
*                                                                       *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

     For details select menu option 75 on the beginning IA Menu

 * Information America Expands California Lawsuits!
 * Global Real Property Asset Locator Now Online!
 * Cover All the Bases...Using the NEW, IMPROVED CORPORATE GLOBAL Service!


Enter your name (last name first): public, john

---------------------------[ Title Screen ]---------------------------
```

В большинстве случаев клиенты IA подключаются с IBM-совместимых компьютеров. Однако вариант 1 (PERSONAL COMPUTER (or 100% IBM compatible)) вполне подходит любому пользователю, способному эмулировать VT-100.

Запрос «Enter your name (last name first)» служит исключительно для внутренних целей выставления счетов: законный владелец учётной записи может отслеживать, кто из сотрудников корпорации пользовался системой. Гипотетически, если бы кто-то захотел получить доступ к системе без собственной действующей учётной записи, наиболее логичным способом избежать подозрений было бы использование имени сотрудника организации — владельца учётной записи, например самого владельца.

В какой-то момент IA предложит ввести Client Billing Code. Это также сугубо внутренняя информация для целей выставления счетов. IA — дорогостоящий сервис: помимо ежемесячной платы в 95 долларов, существуют почасовые тарифы, поштучные сборы и ряд скрытых расходов. Уже по этой причине клиенты IA крайне дотошно сверяют детализированные счета. По возможности вводите Client Billing Code, совместимый со схемой кодирования организации — владельца учётной записи.

Главное меню Information America

В IA доступны 19 основных опций поиска, разбитых на три категории:

- Корпоративные, UCC и смежные записи
- Общенациональные сервисы
- Записи округов и судов

```
-----------------------------[ Main Menu ]-----------------------------

INFORMATION AMERICA NETWORK                                  1

     I N F O R M A T I O N   A M E R I C A   B E G I N N I N G   M E N U
                (Copyright 1991, Information America, Inc.)

                CORPORATE, UCC, & RELATED RECORDS
                 1. Corporate Global (CGL)
                 2. Corporate & Limited Partnership Records (COR)
                 3. State & County UCCs, Liens & Judgments (ULJ)
                 4. State UCC & Lien Filings (UCC)
5. Sleuth (SL)                          6. Litigation Prep (LP)
```

```
NATIONWIDE SERVICES                    COUNTY & COURT RECORDS
 7. People Finder (PF)                  15. County Records (COU)
 8. Executive Affiliation (EA)          16. Bankruptcy Records (BNK)
 9. Business Finder (BF)                17. Lawsuits (LS)
10. Business News (BN)                  18. Real Property Asset Locator (RP)
11. SEC Filings (SEC)                   19. Real Prop, Liens & Judgments (RLJ)
12. Duns Business Records Plus (DB)
13. Name Availability/Reservation (NAR) 75. Help Line (HL)
14. Document Ordering eXpress (DOX)     99. Exit the System (OFF)

Enter the menu number or abbreviation of your choice:

-----------------------------[ Main Menu ]-----------------------------
```

Из трёх категорий наибольший интерес представляют опции раздела NATIONWIDE SERVICES. Information America проста в использовании, полностью управляется через меню и располагает обширной встроенной справочной системой. Сказав это, White Knight и я рассмотрим лишь несколько функций IA, оставив изучение более редких опций читателю.

PEOPLE FINDER (Поиск людей)

Сила People Finder заключается не только в возможности обращаться к различным крупным хранилищам данных, но и в гибкости критериев поиска. (Примечание: People Finder доступен с понедельника по пятницу с 7:00 до полуночи по восточному стандартному времени. Праздничные дни исключены.)

People Finder состоит из четырёх сервисов: SKIP TRACER, TELEPHONE TRACKER, PERSON LOCATOR и PEOPLE FINDER MULTITRACK.

В зависимости от доступной информации профиль People Finder может включать: текущий адрес, номер телефона, тип жилья, срок проживания, пол, дату рождения, до четырёх членов домохозяйства с их датами рождения, а также список соседей.

SKIP TRACER отслеживает перемещения человека или подтверждает текущий адрес, когда у вас есть только старый адрес. Вводите имя человека, номер дома, название улицы и либо почтовый индекс, либо город/штат. Если субъект есть в файлах IA, отобразится профиль с адресом, куда он переехал (или текущим адресом), номером телефона, сроком проживания и прочим. Можно также запросить список 10 соседей. Профиль текущего жильца по старому адресу субъекта и до 10 его соседей также может быть доступен.

TELEPHONE TRACKER устанавливает владельца телефонного номера. Необходимо ввести номер телефона и либо код города, либо город/штат. При совпадении можно просмотреть профиль этого лица или домохозяйства и список до 10 соседей.

PERSON LOCATOR помогает найти человека при отсутствии конкретных адресных данных. Введите имя человека и укажите, хотите ли вы искать по городу, штату(ам), почтовому индексу или по всей стране*. PERSON LOCATOR составит список имён (до 300 имён для общенационального поиска и до 100 — для поиска по отдельному штату), совпадающих с введёнными данными. Найдя нужное имя, вы можете запросить профиль и список соседей для этого лица.

PEOPLE FINDER MULTITRACK помогает искать несколько человек в рамках одного запроса. Результаты поиска будут доступны на следующий рабочий день. По каждому субъекту введите имя и укажите географическую область поиска — по всей стране*, нескольким штатам, штату, городу или почтовому индексу. За один раз можно ввести до 25 имён. Выйдите из системы и дайте Information America сделать всё за вас. На следующий рабочий день войдите в систему и перейдите в меню People Finder, введя `PF` в главном меню Information America. Из меню People Finder просмотрите результаты People Finder MultiTrack, введя `RR` (Review People Finder MultiTrack).

REVIEW PEOPLE FINDER MULTITRACK позволяет просмотреть статус каждого из запрошенных поисков. Вы можете выбрать просмотр результатов каждого завершённого поиска. Результаты хранятся семь дней с момента запроса. В течение этого периода их можно просматривать в любое время.

* Общенациональный поиск недоступен для ряда распространённых фамилий. Чтобы просмотреть их список, введите #92 View Common Names (VC) из меню People Finder.

```
------------------------[ People Finder Menu ]------------------------

INFORMATION AMERICA NETWORK

                        P E O P L E    F I N D E R
                (Copyright 1991, Information America, Inc.)
           Client Billing Code: 123456

   1. Person Locator (PL)           (Search by name & location)
   2. Skip Tracer (ST)              (Search by name & last known address)
   3. Telephone Tracker (TT)        (Search by telephone number)
   4. People Finder MultiTrack (PX) (Multiple searches by name & location
                                     with results available next business day)
   5. Review People Finder MultiTrack Results (RR)

                  70. Revise Client Billing Code  (BC)
                  75. Help Screen  (?)
                  92. View Common Names (VC)
                  95. Description of Service  (DES)
                  99. Go to Beginning Menu  (BEG)
                  OFF Exit off the System  (OFF)

------------------------[ People Finder Menu ]------------------------
```

Если People Finder находит вашего субъекта, может отобразиться профиль со следующими полями:

Поле	Описание
Name (Имя)	Обычно имя и фамилия главы домохозяйства
Address (Адрес)	Улица или маршрут, город, штат и ZIP-код
Phone Number (Телефон)	Текущий номер, если указан в телефонном справочнике
Approx. Birth Date (Примерная дата рождения)	Дата рождения лица, указанного в поле Name (может быть приблизительной)
Gender (Пол)	FEMALE / MALE / UNKNOWN — относится к лицу в поле Name
Length of Residence (Срок проживания)	Число последовательных лет, в течение которых это лицо значится по данному адресу
Residence Type (Тип жилья)	Число различных фамилий по данному адресу (полезно для выявления многосемейного жилья): single, double, triple, quad, 5–9, 10–19, 20–49, 50–100, 100+

Additional Household Members (Доп. члены домохозяйства)	Имена и примерные даты рождения до 4 лиц, проживающих по этому адресу с той же фамилией (обычно из записей актов о рождении)

People Finder: пример поиска

```
-----------------------[ People Finder Search ]-----------------------

Last Name:   public                    First Name:   jane
Enter City or ZIP code.
City: ANYTOWN                          ZIP Code: 90210


Searching...


 INFORMATION AMERICA NETWORK--PEOPLE FINDER
 Name Searched: PUBLIC JANE

                             PERSON LOCATOR
                           Last Name Summary

 No.  First Name       Street               City/State      ZIP   Phone No.
 --- ------------ ----------------------  ---------------- ----- ------------
   1 JANE         27 AVENIDA AVE          ANYTOWN       CA 90210 213-727-8023
*  2 JOHN         69 CALLE DE LOS PUTOS   ANYTOWN       CA 90211 213-000-0000

* PUBLIC JANE has been found as an additional household member.

Searching...


 INFORMATION AMERICA NETWORK--PEOPLE FINDER  -  Detail
 Name Searched: PUBLIC JANE

                          PERSON LOCATOR
                         Resident Profile

                     Name: JANE PUBLIC
                  Address: 27 AVENIDA AVE
                           ANYTOWN, CA 90210
  Approximate Date of Birth: 10/66
                   Gender: FEMALE
        Length of Residence: 3 YEARS
             Residence Type: SINGLE

                  **** Additional Household Names ****
                  Name       Approximate Date of Birth
                  MICHAEL              04/68


Searching...

 INFORMATION AMERICA NETWORK--PEOPLE FINDER  -  Detail
 Name Searched: PUBLIC JANE

                             PERSON LOCATOR
                           Neighbor Listing

       Resident: JANE PUBLIC
        Address: 27 AVENIDA AVE
                 ANYTOWN, CA 90210
                                                              Residence
     Name               Phone#           Address            Length(yrs)/Type
```

```
------------------------------------------------------------------------------
WILLIAM PRESTON       (818) 727-8125  12 BOGUS AVE              12 SINGLE
THEODORE LOGAN        (818) 725-8643  17 BOGUS AVE              04 DOUBLE
KRIS APPLEGATE        (818) 685-2112  19 BOGUS AVE              03 TRIPLE
MARTIN MCFLY          (818) 727-0353  26 BOGUS AVE              23 SINGLE
STAN CISNEROS         (818) 727-4973  30 BOGUS AVE              16 SINGLE
LUCY BYRNE            (818) 727-8765  33 BOGUS AVE              10 SINGLE
JONATHAN DEPP         (818) 725-2012  35 BOGUS AVE              06 SINGLE

-----------------------[ People Finder Search ]-----------------------
```

Gender (Пол)	FEMALE / MALE / UNKNOWN — относится к лицу в поле Name
Length of Residence (Срок проживания)	Число последовательных лет, в течение которых это лицо значится по данному адресу
Residence Type (Тип жилья)	Число различных фамилий по данному адресу (полезно для выявления многосемейного жилья): single, double, triple, quad, 5–9, 10–19, 20–49, 50–100, 100+
Additional Household Members (Доп. члены домохозяйства)	Имена и примерные даты рождения до 4 лиц, проживающих по этому адресу с той же фамилией (обычно из записей актов о рождении)

Примечания к People Finder

IA настолько точна, насколько точны публичные записи. Люди, часто переезжающие или меняющие квартиры (например, студенты), скорее всего, либо не будут найдены в IA, либо предоставленная информация окажется устаревшей. В одном из наших поисков IA установила, что субъект прожил по своему адресу 3 года, тогда как на самом деле он жил там более 15 лет.

Незарегистрированные телефонные номера нередко доступны через IA — например, если номер вашего субъекта фигурировал в городском справочнике. Любопытно, что в ряде случаев информация, похоже, исчезает из IA. Год назад White Knight и я находили адрес и телефон одной знаменитости — IA успешно их выдала. Недавно тот же поиск не дал результата. Поиски по другим лицам, которые прежде выдавали их незарегистрированные номера, теперь возвращают «000-0000». Объяснения этому у нас нет.

Обзор прочих функций IA

SLEUTH

Создавая список связанных имён — «улик» — Sleuth помогает выявить связи между предприятиями и физическими лицами. Введите имя и проверьте официальные записи из до 49 государственных ведомств.

Содержимое: Более 100 поисков в совокупности — из следующих источников:

• Государственные UCC/залоговые файлы: CA, CO, IL, IA, MD, MA, MO, NE, NC, PA, SC, TX

• Корпоративные/LP-записи в перечисленных штатах, а также: AZ, CT, DE, GA, IN, MI, NV, OK, OR, UT, WI
• Данные о налогах с продаж и использования: CA, TX
• Условные/вымышленные наименования округов: Los Angeles, San Francisco (CA); Dallas, Harris (TX)
• Файлы UCC округов: Fulton, Cobb, DeKalb, Gwinnett (GA); Dallas, Harris (TX)

LITIGATION PREP (Подготовка к судебному процессу)

Содержимое: Корпоративные данные и данные об ограниченных партнёрствах от штатов: Аризона*, Калифорния, Колорадо, Коннектикут*, Делавэр, Флорида, Джорджия, Иллинойс*, Индиана, Айова, Мэриленд, Массачусетс, Мичиган, Миссури, Небраска, Невада, Северная Каролина*, Оклахома, Орегон, Пенсильвания, Южная Каролина, Техас, Юта, Вашингтон и Висконсин (* — данные об ограниченных партнёрствах недоступны из этих штатов).

Поиски включают (при наличии): названия компаний, имена владельцев, прежние названия, условные наименования, вымышленные имена владельцев, торговые наименования, названия DBA и имена, объединённые/консолидированные в другие структуры.

Общее описание: Litigation Prep позволяет одновременно искать корпоративную и LP-информацию по штатам, а также вымышленные и условные деловые наименования, зарегистрированные на уровне округов, — для сбора данных, необходимых при подготовке иска.

Информация о статусе «Good Standing/Existence» доступна в штатах: AZ, CT, DE, GA, IL, IN, IA, MA, MI, MO, NE, NC, OK, OR, PA, SC, TX, UT, WA и WI.

Часы работы: Litigation Prep доступен с понедельника по пятницу с 8:00 до 24:00 EST. Компонент FLORIDA доступен только с 8:30 до 19:00 EST, пн–пт.

CORPORATE GLOBAL, CORPORATE & LIMITED PARTNERSHIPS

Содержимое: Корпоративные данные и данные ограниченных партнёрств от штатов: AZ*, CA, CO, CT*, DE, FL, GA, IL*, IN, IA, MD, MA, MI, MO, NE, NV, NC*, OK, OR, PA, SC, TX, UT, WA, WI (* — данные LP недоступны).

Поиск по имени директора/партнёра доступен в штатах: CA, CO, FL, GA, IL, IN, IA, MA, MI, MO, NV, OR, PA, TX, UT.

Записи доступны по одному штату или сразу по всем (CORPORATE GLOBAL). При поиске по CORPORATE GLOBAL индексный экран перечислит штаты, в которых найдены совпадения.

Варианты поиска в меню CORPORATE GLOBAL:

• **Business Name** — охватывает все юридические лица, доступные в онлайн-файлах корпораций/LP штата.
• **Officer/Partner Name** — варьируется по штатам; может включать директоров, учредителей и партнёров.

В Калифорнии и Техасе доступен уникальный вариант поиска — **BUSINESS LOCATOR**: в Калифорнии — поиск по базе налогового ведомства BOE (данные о лицах, имеющих разрешение на уплату налога с продаж); в Техасе — поиск по данным налогоплательщиков из Office of the Comptroller of Public Accounts.

STATE & COUNTY UCCs (Государственные и окружные UCC)

Содержимое: Государственные файлы UCC и залогов из штатов: Калифорния*, Колорадо*, Флорида, Иллинойс, Айова*, Мэриленд, Массачусетс*, Миссури, Небраска*, Северная Каролина, Пенсильвания, Южная Каролина и Техас* (* — доступны залоговые файлы). Окружные файлы UCC, залогов и судебных решений: округа Los Angeles и San Francisco (CA); Cobb, DeKalb, Fulton, Gwinnett (GA); Dallas Metroplex и Harris (TX).

Файлы по Флориде содержат только активные записи; поиск по неактивным файлам предлагается бесплатно по завершении просмотра детального отчёта.

Часы работы: пн–пт, 8:00–24:00 EST. Компонент FLORIDA — только 8:30–19:00 EST.

STATE UCC & LIEN FILINGS (Государственные UCC и залоги)

Охватывает UCC из: Калифорнии, Колорадо, Флориды, Иллинойса, Айовы, Мэриленда, Массачусетса, Миссури, Небраски, Северной Каролины, Пенсильвании, Южной Каролины, Техаса.

Дополнительные залоги по штатам:
• **Калифорния:** федеральные и государственные налоговые залоги, обеспечительные залоги, залоги судебных решений
• **Колорадо:** федеральные налоговые залоги и залоги судебных решений
• **Айова:** федеральные налоговые залоги, удостоверенные залоги и залоги молотилок (thresherman's liens)
• **Массачусетс:** государственные налоговые залоги и залоги по алиментам
• **Небраска:** залоги сельскохозяйственных материальных ресурсов, потребительские и статутные залоги
• **Техас:** федеральные налоговые залоги, инструменты обеспечения коммунальных услуг и фермерские регистрации

COUNTY COURT RECORDS (Записи судов округов)

Information America предоставляет онлайн-доступ к местным судебным записям из четырёх штатов:

• **Калифорния:** округа Los Angeles, Orange, San Francisco. Real Property Asset Locator — по всему штату.
• **Джорджия:** столичный район Атланты: округа Cobb, DeKalb, Fulton, Gwinnett.
• **Пенсильвания:** округ Philadelphia.
• **Техас:** мегаполис Dallas/Fort Worth (округа Collin, Dallas, Denton, Tarrant) и округ Harris (Хьюстон).

Записи варьируются от округа к округу, но могут включать: акты о судебных решениях, условные наименования, гражданские иски, UCC округов, общие реестры исполнения, ограниченные партнёрства, lis pendens, дела о наследстве и семейные дела, регистрации недвижимости, налоговые залоги и индекс торговых наименований.

LAWSUITS (Судебные иски)

[Таблица из ~40 записей — опущена]

Таблица содержит информацию о датах эффективности файлов судебных исков по округам штатов Калифорния (Los Angeles, Orange, San Mateo, Santa Clara, Contra Costa, San Diego), Джорджия (Cobb, DeKalb, Fulton, Gwinnett), Иллинойс (Cook — Civil Law и Civil Municipal), Нью-Джерси (21 округ), Нью-Йорк (Supreme & Suffolk County), Пенсильвания (Philadelphia) и Техас (Dallas), с указанием источника данных и диапазонов дат охвата.

REAL PROPERTY ASSET LOCATOR (Поиск активов в недвижимости)

Интегрирует данные из нескольких источников для выявления и оценки реальных активов или установления владельца конкретного объекта недвижимости. Информация основана на официальных оценочных ведомостях налоговых органов каждого округа, дополненных частными базами данных.

Четыре варианта поиска:

1. **Asset Locator** — выявить имущество, принадлежащее физическому лицу или компании, по имени. Поиск — глобальный, по штату, мегаполису, округу или городу.
2. **Ownership Locator** — установить владельца объекта по его адресу.
3. **Property of Comparable Value** — оценить стоимость недвижимости по сделкам с аналогичными объектами в данном районе.
4. **Assessor's Parcel Number** — установить владельца по кадастровому номеру объекта.

Доступно в штатах: Аризона, Калифорния, Вашингтон (округ Колумбия), Делавэр, Флорида, Джорджия, Иллинойс, Канзас, Мэриленд, Массачусетс, Миссури, Нью-Джерси, Нью-Йорк, Пенсильвания, Техас, Вирджиния.

REAL PROPERTY ASSET TRANSFERS (Переходы права собственности на недвижимость)

Интегрирует данные из нескольких источников для выявления недавних переходов права собственности на недвижимость.

Два варианта поиска:

1. **Asset Transfers** — выявить приобретённое или проданное имущество физического лица или компании по имени (поиск по штату, мегаполису или округу).
2. **Ownership Transfers** — установить продавца и покупателя по адресу объекта.

Данные получены из записей о переходе права собственности окружных органов регистрации. Доступно в избранных округах штатов: Аризона, Калифорния, Колорадо, Вашингтон (округ Колумбия), Флорида, Джорджия, Гавайи, Иллинойс, Мэриленд, Массачусетс, Невада, Нью-Джерси, Нью-Йорк, Огайо, Пенсильвания, Теннесси, Вирджиния, Вашингтон.

EXECUTIVE AFFILIATION (Аффилиации руководителей)

Содержимое: Более 30 миллионов руководителей по всей стране. Один поиск покажет компании по всей стране, где данное лицо числится руководителем. Доступны два типа отчётов: Executive Profile и Executive Brief.

Executive Profile формируется на основе данных компании American Business Information, Inc. (ABI). ABI составляет деловые справочники на основе «жёлтых страниц» 5 000 телефонных справочников с последующим обзвоном каждой компании для получения имени и должности руководителя.

Executive Brief формируется на основе корпоративных данных и данных LP, поданных в штатах: AZ, CA, CO, CT, FL, GA, IL, IN, IA, MD, MA, MI, MO, NE, NV, NC, OK, OR, PA, SC, TX, UT, WA, WI. Данные Делавэра не включены.

Применение Executive Affiliation:

• Проверка деловых аффилиаций противоположной стороны в ходе проверки биографии
• Проверка имён и адресов для исковых заявлений и показаний

• Выявление участия руководителя в различных компаниях по стране для установления возможного перевода активов
• Проверка конфликтов интересов
• Сбор досье на перспективного клиента

BUSINESS FINDER (Поиск компаний)

Источник: American Business Information, Inc.

Содержимое: Более 14 миллионов американских и 1,7 миллиона канадских деловых справочников из «жёлтых страниц» почти 5 000 телефонных справочников. Более 9,5 миллиона отдельных компаний и 2 миллиона специалистов.

Обновление: ABI непрерывно пересматривает информацию и обновляет данные из доступных телефонных справочников в течение шести месяцев после их публикации. Information America получает обновления от ABI ежеквартально.

BUSINESS NEWS (Деловые новости)

Источник: Comtex Scientific Corporation

Содержимое: Новостные материалы крупных национальных и международных информационных агентств (UPI, Kyodo, TASS), пресс-релизы и прочие источники. Материалы доступны с ноября 1989 года.

Обновление: дважды в сутки.

Business News позволяет искать статьи по имени, биржевому тикеру, отрасли или теме. Отраслевые категории Business News включают 53 сектора: реклама, авиакосмос, сельское хозяйство, автомобильная промышленность, банковское дело, биотехнологии, телерадиовещание, химическая промышленность, компьютеры, строительство, оборона, электроника, развлечения, финансовые услуги, здравоохранение, страхование, машиностроение, недвижимость, телекоммуникации, коммунальные услуги и другие.

BANKRUPTCY RECORDS (Записи о банкротстве)

Источник: Официальные записи Судов по делам о банкротстве США по штатам: Калифорния, Джорджия (Северный округ — только Атланта и Гейнсвилл), Нью-Джерси, Пенсильвания (Восточный округ), Техас.

Содержимое: Записи о банкротстве физических лиц и компаний, включая имена должников, номера дел, место и дату подачи, номер главы и прочее.

Обновление: еженедельно (CA, GA, PA, TX); раз в две недели (NJ).

Поиск возможен по имени должника, номеру социального страхования/FEIN или номеру дела.

SEC FILINGS (Отчётность в SEC)

Источник: SEC Online, Inc.

Содержимое: Полные тексты документов, поданных в Комиссию по ценным бумагам и биржам публичными компаниями, торгующимися на NYSE и Американской фондовой бирже, а также отдельными компаниями NASDAQ NMS. Доступные онлайн документы — 10-K, 10-Q, годовые

отчёты, доверенности, а также форма 20-F для иностранных компаний — содержат все сноски и избранные приложения. Также включён корпоративный профиль с базовой информацией о компании.

Дата начала: информация актуальна с 01.07.1987.

Обновление: еженедельно.

Поиск по названию компании или биржевому тикеру.

Примечания об Information America

Мы упоминали, что имена пользователей, начинающиеся с «BIDA», распознаются системой IA как аккаунты IA (в отличие от аккаунтов командной оболочки). Вполне вероятно, что и другие форматы имён пользователей также являются действительными аккаунтами IA.

Как и в большинстве систем, пароли IA нередко легко угадать. Начальные пароли, назначаемые при создании аккаунта, как правило, состоят из имени владельца аккаунта или имени плюс средней или заглавной буквы фамилии. В ряде случаев пароль составляется из цифр в имени пользователя плюс имя владельца аккаунта. В других случаях пароль — это две случайные буквы плюс двузначное число (напр.: PG13). Если пользователей когда-либо и побуждают сменить начальный пароль, они, судя по всему, делают это крайне редко.

Вы, вероятно, заметили, что у IA есть конкретные часы работы (восточное стандартное время). Большинство функций IA не работает по выходным, праздничным дням и за пределами указанного времени. Иногда по выходным IA вовсе недоступна. Или, что особенно интересно, по выходным интерактивная среда IA даёт сбой, выбрасывая вас в командную оболочку VAX.

Клиентами IA являются преимущественно юристы и помощники юристов в юридических фирмах, однако ФБР также является крупным клиентом IA. Телевизионные программы 1960–70-х годов, изображавшие «Большой Брат» — компьютерную систему ФБР, — достаточно напугали общество и Конгресс, чтобы те последовательно противостояли попыткам ФБР внедрить подобную систему. В середине 1980-х, например, Конгресс проголосовал против создания компьютерной системы ФБР, которая позволила бы прослушивать телефонные переговоры. Information America — идеальное решение бюрократической головоломки ФБР.

IA существует как минимум два с половиной года, однако оставалась относительно неизвестной в телекоммуникационном сообществе вплоть до прошлого года, когда MoD начала использовать People Finder IA для поиска и запугивания людей. Низкий профиль IA не удивителен: общественная реакция против Lotus «MarketPlace» CD ROM — который содержал маркетинговые данные лишь на несколько миллионов человек — вынудила Lotus полностью закрыть проект, вложив десятки тысяч долларов только в рекламу, буквально накануне выпуска. То, что делала Lotus, не было чем-то из ряда вон выходящим: крупные компании прямого маркетинга, такие как National Demographics & Lifestyles (NDL), годами относительно скрытно продавали имена потребителей и информацию о них на CD ROM (в том числе: сколько телефонов у вас есть, приблизительный возраст членов домохозяйства, пол главы домохозяйства, количество и тип автомобилей, стоимость ипотеки, предполагаемые доходы глав домохозяйства и т. д.). Разница заключалась в том, что Lotus предлагала свой CD ROM в розничной продаже, так что любой желающий мог бы, по словам общественности, иметь возможности «Большого Брата» под рукой. Если бы общество узнало об Information America — узнало, что любой может воспользоваться её шпионскими возможностями, — возмущение было бы колоссальным.

Продвигая свои сервисы баз данных, IA, по всей видимости, избрала стратегию работы «с земли»: IA нанимает представителей в крупных городах, чья задача — исследовать рынок и выходить на

потенциальных клиентов, например юристов. О какой-либо рекламе в специализированных изданиях нам неизвестно.

Мы воспринимаем как должное существование государственных баз данных, содержащих об американцах ещё более детальную информацию, чем та, которой располагает IA. Однако эти базы существенно меньше и, что важнее, жёстко регулируются: управляющие ими ведомства несут юридическую ответственность. Потенциал злоупотреблений системой вроде Information America — лишённой каких-либо сдержек и противовесов — колоссален. MoD уже продемонстрировала это в небольшом масштабе. Те же технологические достижения, которые должны были сделать покупки на дому удобнее и адаптировать маркетинг под ваши нужды, теперь сделали слежку за вами экономически выгодной, точной и такой же простой, как нажатие клавиши.

Один из наименее освещавшихся фактов, всплывших в ходе слушаний по делу Иран-Контрас, заключается в следующем: будучи главой Федерального агентства по чрезвычайным ситуациям (FEMA) — организации, координирующей ликвидацию последствий стихийных бедствий по всей стране, — Оливер Норт разработал для FEMA планы действий в чрезвычайных ситуациях совершенно иного рода. В случае войны в Центральной Америке предполагалось приостановить действие Конституции, а FEMA должна была выявлять и помещать в лагеря — напоминающие Манзанар — иностранцев (в первую очередь испаноязычных) и граждан США, признанных «подрывными элементами», для допросов. Базы данных, подобные Information America, несомненно, были бы задействованы для установления местонахождения этих людей.

Значение Information America — не в том, что она может сделать для вас. А в том, что с её помощью можно сделать с вами.

White Knight и я доступны по адресам WKnight@ATDT.ORG и Omega@ATDT.ORG соответственно. Также с нами можно связаться через Demon Roach Underground или Pure Nihilism. Мы приветствуем любые вопросы и комментарии — особенно любую новую информацию, которую вы можете добавить. Пожалуйста, не обращайтесь к нам с просьбами предоставить аккаунты или пароли.

Как уйти от штрафа за радар (Часть 1 из 2): «Ваш день в суде»

Автор: Dispater

Введение

Добро пожаловать в первую из двух частей серии, призванной рассказать вам о некоторых аспектах — как юридических, так и технических — связанных с дорожными радарами. Вторая часть выйдет в Phrack 38. Рекомендую прочитать обе части, прежде чем пытаться применить информацию из этого файла.

Любой хакер скажет вам: **всегда** узнавайте как можно больше о любом деле и взвешивайте риски, прежде чем действовать. Для большинства из нас вождение — это необходимость: работа, учёба, досуг. Поэтому крайне важно знать правила дорожного движения и понимать, что произойдёт, если вы совершите ошибку. Для большинства из нас эта ошибка означает штраф за превышение скорости или иное нарушение.

Этот файл объяснит, как действовать, если вам когда-либо придётся идти в суд из-за штрафа за превышение скорости. Я намерен дать вам базовые знания, чтобы шансы стали чуть более равными.

Одна из неприятных особенностей дорожного суда состоит в том, что по какой-то причине бремя доказательства перевернулось: теперь не государство должно доказывать вашу вину (как оно и должно быть), а ответчик вынужден доказывать свою невиновность.

Прежде всего — вы не одиноки в своём стремлении к справедливости. Большинство судей не злобные садисты. Если вы придёте в суд аккуратно одетым (не нарядно, просто выглядя как «почти нормальный» человек), хорошо разбирающимся в деле, вежливым и слегка смирившимся с ситуацией, судья, возможно, склонится немного в вашу сторону. Если вы пойдёте в суд, то увидите немало идиотов, которые встанут перед судьёй и начнут спорить или говорить: «Я ничего не делал. Меня просто домогаются. Я прав, а этот легавый не прав. Ня!» Очевидно, судья не воспримет такое поведение благосклонно. Вы бы восприняли?

Чтобы быть подготовленным, я **настоятельно** рекомендую обратиться в:

```
National Motorists Association              Членство: $20 для студентов
6678 Pertzborn Rd.                          в год     $35 для всех остальных
Dane, WI  53529
Телефон: 1-800-882-2785
```

NMA предоставляет огромное количество ресурсов для тех, кто водит машину. Они предоставляют (при наличии членства) юридический набор ресурсов в аренду примерно за $20,00 в месяц. Этот набор состоит из 2 видеокассет, 2 книг и ОГРОМНОЙ стопки информации. Большая часть этой «ОГРОМНОЙ стопки» состоит из прецедентных дел, где победила защита, из ВСЕХ руководств к радарным пистолетам, множества соответствующих газетных статей, анализа погрешностей VASCAR и других полезных сведений. Это превосходный ресурс, и я призываю всех, кто водит машину, принять в этом участие. NMA, помимо прочего, — это элегантное название для «людей, выступающих против ограничения 55 миль/ч». Они утверждают, что местные правительства и штаты сами должны устанавливать ограничения скорости. Не дело Вашингтона указывать всем нам, как жить!

Последнее, что хочу упомянуть: это **не** исчерпывающий документ. Прочитав его, вы **не** станете юристом. Если можете позволить себе адвоката — наймите его. Этот файл предназначен для таких людей, как я: тех, кто не может позволить себе адвоката, но обладает определённым умом и смекалкой. Есть больше одного способа снять шкуру с кота (копа), и не стоит воспринимать всё написанное как пошаговое руководство к действию, если вас поймали на превышении. Я намерен дать вам основу для построения хорошей защиты и подсказать несколько идей о том, как можно действовать. Не заходите в зал суда неподготовленными. Хороший адвокат всегда знает исход дела ещё до того, как переступает порог зала суда.

Вас остановили!

Итак, за вами мигают красные огни, а радар-детектор сходит с ума, потому что вы не следили за дорогой — слишком увлечённо крутили радио и слушали MC 900' Jesus на такой громкости, что трясутся окна соседней машины. Первое, что нужно сделать — немедленно остановитесь! Не пытайтесь строить из себя крутого и уходить от погони. В большинстве случаев машина копа едет быстрее вашей, да к тому же у него есть рация. После остановки просто отдайте ему всё, что он просит, и потакайте его желанию «быть главным».

Всегда говорите «Да, сэр» и «Нет, сэр». Они это **обожают**. Будьте как можно **вежливее**. Прикиньтесь смиренным. Знаю, это может показаться сложным, но просто **попробуйте**. ВСЕ — подчёркиваю, ВСЕ — люди, которые становятся сотрудниками правоохранительных органов, выбрали эту работу из-за расстройства личности: им **нужно** чувствовать себя хозяевами положения и **нужно**, чтобы другие их уважали. На мой взгляд, это слабость их характера. В любом случае, если у него сегодня удался гольф, он может обойтись лишь предупреждением. Если он всё равно настаивает на выписывании штрафа, он по крайней мере будет знать, что вы не представляете угрозы. ВСЕ полицейские, особенно в крупных городах, всегда подходят к вашей машине так, будто вы собираетесь их застрелить. Создайте у офицера впечатление, что вы хороший человек (на данный момент) и что просто не следили за дорогой и совершили ошибку. Как только вы докажете ему, что не представляете угрозы, он расслабится, и всё пройдёт гораздо проще. Я всегда так делаю, и в большинстве случаев офицер в ответ ведёт себя по-настоящему **нормально**. Даже если его первое впечатление — «длинноволосый парень в крутой машине в футболке Metallica», встреча, как правило, заканчивается «Хорошего дня» или «Просто будьте осторожны, ладно?»

ПРИМЕЧАНИЕ: Если вас остановила женщина-коп в дурном настроении — вы полностью облажались. Социальная инженерия здесь абсолютно бесполезна. Копы с плохой репутацией просто стремятся что-то доказать. У них скверный характер, и они считают, что большинство мужчин будут воспринимать их как менее авторитетных, если не будут компенсировать (с лихвой) тот факт, что они женщины. Если вы — женщина-полицейский, читающая это, и вы не похожи на то, что я только что описал, — просто проигнорируйте и скажите своим коллегам, чтобы исправили отношение!

Продолжаем... Пока вы сидите там, наблюдая, как все замедляются и пялятся на вас, записывайте **ВСЁ!** Запишите следующее:

1) Место (перекрёстки, повороты, состояние дороги)
2) Погода (дождь, туман, снег — всё это мешает дорожному радару)
3) Трафик и все типы транспортных средств (большие грузовики?)
4) Время (час пик?)
5) Здания поблизости (аэропорт? радиостанция? банк? микроволновые вышки? линии электропередач? больница? телефонный узел?)
6) Поведение офицера (если он зол — это сыграет в вашу пользу позже)
7) Прочее (всё, что я забыл упомянуть)

Ваш штраф и досудебные действия

Итак, теперь у вас в руках маленький подарок от того, у кого был плохой рабочий день. Первое, что нужно сделать — убедиться, что вся информация в штрафной квитанции верна. Если нет — обязательно запишите это и упомяните сразу, как только начнётся ваш процесс! Возможно, вы сможете отделаться на формальных основаниях. Ещё одна вещь для проверки: не написал ли офицер никаких сообщений судье на обороте квитанции. Если там написано «радар-детектор» или что-то ещё нерелевантное — обязательно укажите судье, что штрафная квитанция недопустима в качестве доказательства в суде, так как содержит информацию, не относящуюся к делу. Идея в том, что большинство пойманных на превышении имеют радар-детекторы. Поэтому коп попытается косвенно сыграть на этом факте. Даже если это доказательство нерелевантно, он попытается его представить. Если судья адекватный — вы отделаетесь на формальных основаниях. Другие способы выйти на технических основаниях: убедитесь, что **каждая** деталь в квитанции **верна**. Неверная информация — отличный способ выйти сухим из воды. Это называется «процессуальная ошибка» и может привести к прекращению дела. Продолжаем...

Итак, в квитанции написано, что вам нужно явиться в суд 21 декабря в 16:00. Это означает лишь то, что если вы хотите оплатить штраф, это нужно сделать до этой даты и времени. Это обычно не означает, что вы реально пойдёте в суд именно в этот день. Что делать дальше: идёте в канцелярию и отдаёте дежурной за стойкой квитанцию, говоря, что хотите её оспорить. Они назначат дату (обычно значительно позже в году, иногда через год, если всё совсем забито) и дадут вам бумагу, которую нужно принести в суд. Я настоятельно рекомендую всем и всегда, **всегда**, **всегда** оспаривать штраф. Чёрт, вы платите судебные издержки в любом случае — так почему бы не прийти, верно? Суть в том, чтобы заставить их отрабатывать ваши деньги!

Хороший план действий — прийти в суд за несколько недель и посмотреть, как проходят слушания в вашем местном зале суда. Просто скажите приставу, что вы студент юридического факультета и хотите увидеть, как работает дорожный суд — наблюдать, что **реально** происходит, вместо того чтобы читать об этом в учебнике. Если вы достаточно смышлёны, можете попросить одного из копов взять вас с собой посмотреть, как сотрудники полиции ловят нарушителей. Используйте старейший и самый классический приём социальной инженерии: «Это для реферата в классе». Дайте им думать, что вы заинтересованы в том, чтобы стать копом. Мне всё равно, чем они занимаются и кем являются — если кто-то подходит к ним и проявляет интерес к их профессии, они всегда будут польщены. Всегда льстите тому, кого хотите инженерить!

Первое, что нужно сделать перед фактическим походом в суд, — не идти в суд. Примерно за неделю до слушания или менее позвоните в канцелярию и попросите «перенос дела». Скажите, что ваш начальник отправляет вас в командировку в день суда, и они назначат новую дату. Это важно, потому что большинство полицейских менее охотно приходят повторно. Таким образом, если его там нет, чтобы вас обвинять, — вы выходите победителем!

Суд начинается!

Итак, вы теперь сидите там среди других бедолаг, оказавшихся в схожей ситуации. Пока вы там нервничаете (это же ваш первый раз в суде, надеюсь), обязательно следите за другими делами. Что говорят офицеры, когда кто-то упоминает дорожный радар? Смотрите описание в предыдущем

абзаце о том, чтобы сначала прощупать почву. Я получил тонну информации о том, как отделы реально работают, когда знают, что на них не давят. Используйте хлипкие заявления офицеров против других офицеров и всего отдела, когда настанет ваша очередь. Однажды, ещё до того, как наступила моя очередь, я наблюдал, как один коп сказал: «Радарные устройства калибруются производителем и отправляются нам». Излишне говорить, что то дело я выиграл!

Теперь пристав вызывает: **ШТАТ ТЕХАС ПРОТИВ ГРАЖДАНИНА НАРУШИТЕЛЯ!** К этому моменту вы должны знать процедуру. Как только судья открывает слушание, попросите его/её разрешить вам допросить свидетеля. Они скажут «да». Вот здесь вы и начинаете строить своё дело.

Предварительные вопросы

«Что?!?!?!» — вот что сейчас творится в голове у копа. Вы больше не тот невинный дурак, каким выглядели в своей машине. Он немедленно поднимает защиту, и вам нужно её снизить несколькими вопросами, изматывая его. Эта часть допроса нужна для того, чтобы проверить, помнит ли он точные обстоятельства, при которых вас остановил, и приучить его к тому, что вы берёте контроль над допросом.

A. Какой тип радара вы использовали в день выдачи протокола?

> *Убедитесь, что он назовёт модель и номер. Ответы вроде «дорожный радар» или «доплеровский радар» не должны приниматься.*

B. Пожалуйста, изложите факты, касающиеся протокола, так, как вы их помните.

> *Обратите внимание, если что-то расходится с тем, что вы помните.*

C. Был ли у вас включён аудиодоплер на момент выдачи протокола?

> *Если он скажет, что не знает, что это такое, — значит, он не проходил обучение! Это функция ручных устройств (серия Speedgun не имеет аудиодоплера!). Это хороший вопрос, чтобы поставить его в тупик! Если он скажет, что включал, просто достаньте руководство и попросите указать, где именно эта функция. ИЛИ можете попросить вызвать само устройство в суд и попросить его найти!*

D. На какую скорость была установлена ваша звуковая сигнализация?

> *Если он скажет, что не знает, что это такое, — значит, он не проходил обучение!*

E. Была ли у вас включена автоматическая блокировка скорости?

> *Если да — вы уже начали строить дело о допущенной ошибке. Если нет — продолжайте.*

F. Вы стояли или двигались в момент срабатывания сигнализации вашего радара?

> *Не важно, если только вы не хотите предоставить доказательства «косинусной ошибки» позднее.*

G. Я двигался в вашу сторону или от вас?

> *Опять же, это неважно.*

H. Видели ли вы меня до того, как сработала звуковая сигнализация вашего радара?

> *Это важно — вы фактически спрашиваете, следил ли он за трафиком, прежде чем занять позицию в кустах и поджидать нарушителей.*

I. Могли ли вы оценить мою скорость?

Нерелевантно.

J. Какова была видимая скорость?

Нерелевантно.

K. Сколько секунд прошло между тем, как вы впервые увидели мою машину, и тем, как сработала ваша звуковая сигнализация?

Не важно, если только это не был случай, когда вы появились из-за поворота или из-за горки, а там уже стоит старина Смоки, готовый поймать всё, что заставит его машинку пищать. Он должен был отслеживать вас достаточно долго, чтобы получить хорошие показания — около 5–8 секунд, чтобы исключить случайные показания. Если он не ждал так долго — он нарушает своё обучение.

L. Могли бы вы нарисовать карту местности на этом листе бумаги?

Чаще всего полицейский не сможет вспомнить детали окружающей обстановки, так как каждый день выписывает много штрафов. Это хорошее место для установления сомнения.

Установление уровня квалификации офицера

Это делается для того, чтобы представить полицейского как можно менее квалифицированным. Чем большим дураком вы сможете выставить копа, тем больше очков заработаете у судьи.

A. Как долго вы работаете полицейским?

Нерелевантно, если только он не вышел прямо из академии.

B. Как долго вы работаете с радаром?

Нерелевантно, если только это не год и меньше.

C. Проходили ли вы официальную подготовку по работе с радаром?

*Если **НЕТ** — вы нашли золото.*

D. При каких обстоятельствах вы прошли эту подготовку?

Нерелевантно, если только он не скажет «в раздевалке». В этом случае, возможно, он на вашей стороне.

E. Сколько часов аудиторного обучения вы прошли?

Это важный ответ. Если он скажет «четыре или меньше» — он, скорее всего, недостаточно квалифицирован. Отметьте.

F. Как давно вы прошли это обучение?

Нерелевантно, если только ответ не «пять-шесть лет назад». Он мог потерять практику и, скорее всего, не был обучен на той модели, которой поймал вас.

G. Кто вёл занятие?

Если это был его сержант — это случай слепого, ведущего слепого. Если производитель радара — потенциально предвзятый источник, поскольку производитель сделает всё, чтобы продать своё оборудование! Если его отправили в школу производителя — это лучше, чем у большинства.

H. С момента начального обучения проходили ли вы какие-либо курсы повышения квалификации?

Если говорит «да» — это сомнительно. Спросите, кто их проводил и когда.

I. Считаете ли вы себя компетентным оператором радара?

Конечно, считает.

J. Есть ли у вас сертификат?

*В некоторых штатах он **обязан** пройти обучение у производителя. Если скажет, что его сертифицировал сержант — вы можете прямо сейчас выйти из зала суда победителем. Это случай слепого, ведущего слепого.*

K. Проходили ли вы начальное обучение именно на данной модели (той, которой поймал вас)?

Если его официальное обучение проходило на другом устройстве — вы снова нашли золото!

L. Сколько индивидуальных занятий с выездом на место он прошёл?

Ответы типа «я ездил с другим офицером, пока он выписывал штрафы» не годятся. Продолжайте давить на этот вопрос. Скорее всего, такого обучения у него не было, если только оно не проводилось представителем завода — а тогда в машине одновременно находились ещё трое офицеров.

Установление степени доверия офицера к своему радару

Эти вопросы используются для того, чтобы создать впечатление, что сам полицейский сомневается в надёжности дорожного радара. Вот где всё становится интересным, и он может даже лжесвидетельствовать, если не будет осторожен — в этом случае вы снова побеждаете!

A. Считаете ли вы (модель радара, которым он вас поймал) хорошим устройством?

Конечно, считает. Если нет — он может быть на вашей стороне.

B. Сталкивались ли вы когда-либо с проблемами с этой моделью радара?

Если говорит «да» — убедитесь, что он называет детали, а не просто «однажды он перестал работать».

C. Закреплены ли вы постоянно за одним конкретным радарным устройством?

Они всегда меняют устройства. Скорее всего, он скажет, что использует одно и то же название марки, но разные модели.

D. Считаете ли вы, что между марками или моделями радарных устройств есть различия? Может ли у одного быть особенности, которых нет у других?

Скорее всего, скажет, что все работают одинаково. Если скажет, что есть различия — попросите рассказать, какие именно и как он их заметил.

E. Считаете ли вы, что данная модель радара когда-либо даёт ложные или паразитные показания?

Если скажет «нет» — убедитесь, что у вас есть задокументированные доказательства этого. Это отличный способ выставить его дураком. Повторите вопрос с акцентом на слово «НИКОГДА». После того как он снова скажет «нет», передайте документ судье и скажите что-то вроде: «У меня здесь есть письменные доказательства от независимой инженерной фирмы, подтверждающие, что данная

модель радара способна давать ложные показания». Заметьте: в суде вам не разрешено защищать себя, допрашивая свидетеля, — однако, поскольку вы не адвокат, судья может разрешить вам дать показания.

*Если офицер скажет «да», что видел ложные показания, — спросите, в каком проценте случаев они возникают. В деле **ШТАТ ВИСКОНСИН против ХАНСЕНА**, которое ХАНСЕН выиграл, было доказано, что радар может давать ложные показания до 20% времени.*

F. Считаете ли вы, что всегда можете определить, что радарное устройство даёт ложное показание?

Он всегда будет говорить «да». Если скажет «нет» — вы уже установили разумное сомнение. Когда он говорит «да» — переходите к следующим двум вопросам, а затем вернитесь к этому.

G. Появляется ли на экране специальный номер, указывающий на ложное показание?

Нет!

H. Даёт ли устройство какую-либо визуальную индикацию того, что показание подозрительно?

Нет! (Верите или нет — на самом первом деле, которое я защищал, тупой коп сказал, что существует «индикаторная лампа, которая показывает, когда в районе есть помехи радара». АХАХАХА!!! Что за бред. Я попросил его показать её мне — и, конечно, он не смог. Тем самым он просто солгал под присягой. Он сам себя закопал! Судья тоже не был доволен, видя лгущего полицейского! ;-)

I. Как же тогда вы определяете, что получаемое вами показание является ложным?

Он ответит, что цели нет или что машина явно не превышает.

J. Вы сказали, что нет какой-то особой скорости, которая появляется на экране. Все показания, например, 86 миль/ч, не являются ложными?

Конечно, нет.

K. Значит, ложное показание может быть и 20 миль/ч, и 70 миль/ч?

Конечно. Если говорит «нет» — он вышел из своей лиги и пытается уходить от ответов.

L. Радар мог бы показать 20 или 70 миль/ч, но вы могли бы ясно видеть, например, что машина едет лишь 30 миль/ч?

Он должен с этим согласиться.

M. А если машина едет 55 миль/ч, а вы получаете показание 70 миль/ч? Это возможно?

Он должен согласиться.

N. Допустим, машина приближается к вам на скорости 55 миль/ч. Вы могли бы это распознать?

Скорее всего, скажет «да». Если так — продолжайте. Если скажет «нет» — вы уже установили сомнение.

O. Если машина приближается на 55 миль/ч, а вы получаете показание 56 миль/ч — могли бы вы определить, что это ложное показание?

Конечно, нет. На этом этапе давите всё сильнее, быстро задавая вопрос снова и снова, увеличивая ложное показание на 1 миль/ч, пока он не сдастся. Если вы загнали копа в эту ловушку — вы отлично справляетесь! Он полностью в ловушке, как бы ни ответил — «да» или «нет». Каждый ответ «нет» усиливает сомнение, а если он скажет «да»

слишком рано — будет выглядеть, будто обладает сверхчеловеческими способностями!

Все радарные устройства включают функции, облегчающие работу офицера. **АУДИОДОПЛЕР** можно приглушить или отключить — что обычно и делается — поэтому он ничуть не способствует надёжности. **ЗВУКОВАЯ СИГНАЛИЗАЦИЯ** — это предупредительный тон, сообщающий офицеру, что радар «поймал» нарушителя; она встроена во все радарные устройства. Офицер должен выставить скорость, выше которой должна срабатывать сигнализация. Единственный способ отключить сигнализацию — выставить 99 миль/ч или 199 миль/ч на некоторых моделях. **АВТОМАТИЧЕСКАЯ БЛОКИРОВКА СКОРОСТИ** — худшая функция, когда-либо встроенная в радарное устройство. Она автоматически фиксирует показание скорости, когда оно превышает заданный уровень. Если показание ложное — офицер об этом никогда не узнает. Ваша задача здесь — установить его обычные рабочие привычки. Позже вы узнаете, как он пользовался радаром в день, когда вас поймал.

A. Есть ли в вашем радарном устройстве аудиодоплер? То есть непрерывный монотонный звуковой сигнал, преобразующий доплеровский сдвиг в слышимый сигнал?

Он скажет, что есть, — если только это не Speedgun, у которого его нет. Если это был Speedgun — переходите к вопросу «M».

B. Есть ли у аудиодоплера регулятор громкости?

Да.

C. Используете ли вы аудиодоплер?

Если «да» — продолжайте. Если «нет» — переходите к вопросу «M».

D. В каком примерно проценте случаев вы слушаете аудиодоплер?

Запишите процент.

E. Когда вы работаете с аудиодоплером, вы используете его на полную громкость?

Ха, как же!

F. На какой громкости вы его используете?

Вопрос полезен, только если он скажет, что использует его на малой громкости. Попробуйте задать несколько похожих вопросов, которые заставят его ответить «малая громкость». Например: «Знаю, этот звук здорово раздражает, не так ли?»

G. Отключаете ли вы его иногда?

Конечно, отключает.

H. Почему вы его отключаете?

Потому что это ужасно раздражает!

I. Мешает ли использование аудиодоплера вашей работе с полицейской рацией или переговорам с другими офицерами?

Должен сказать «да».

J. Значит, вы работаете с отключённым аудиодоплером примерно ___ процентов времени?

Вставьте процент, который он назвал раньше.

K. Из оставшегося времени — как часто вы работаете с включённым, но приглушённым звуком?

Запишите процент.

L. Считаете ли вы аудиодоплер важным инструментом предотвращения ошибок оператора?

Важно, только если скажет «нет».

M. Оснащено ли ваше радарное устройство регулятором, позволяющим задать скорость, выше которой будет звучать звуковой сигнал при обнаружении нарушения?

Да, все радарные устройства имеют эту функцию.

N. Назовём эту функцию ЗВУКОВОЙ СИГНАЛИЗАЦИЕЙ. Используете ли вы её обычно?

Обязан использовать.

O. Какой процент времени вы её используете?

Если ответит менее 100% — спросите, как он её отключает. Ему пришлось бы разобрать всё устройство.

P. Если на шоссе ограничение скорости 55 миль/ч, на какую скорость вы обычно устанавливаете порог срабатывания сигнализации?

Запишите скорость. Ответ не принципиален.

Q. Считаете ли вы эту функцию полезной?

Скорее всего, скажет «иногда полезна».

R. Если нарушение скорости вызывает срабатывание сигнализации, вам достаточно лишь потянуться и зафиксировать эту скорость, верно?

Именно так это и работает.

S. Есть ли в вашем радарном устройстве кнопка или переключатель, позволяющий автоматически фиксировать скорость нарушения?

Да, есть.

T. Используете ли вы когда-либо функцию автоматической блокировки скорости?

Если скажет «нет» — повторите вопрос с акцентом на «когда-либо» и смотрите скептически. Если всё равно «нет» — переходите к следующему разделу.

U. В каком примерно проценте случаев вы используете автоматическую блокировку скорости?

Запишите процент.

V. Считаете ли вы автоматическую блокировку скорости удобной?

Конечно, считает. Так ему можно читать журнал или дремать, пока радарное устройство делает всё за него!

W. Используете ли вы автоматическую блокировку скорости по каким-либо иным причинам?

Запишите причины, если они есть.

X. Было ли использование автоматической блокировки скорости включено в ваше обучение?

Ответ не важен.

Установление того, использовал ли офицер визуальное подтверждение

Когда копы идут в суд, у них есть «образцовые показания», используемые для обоснования причины выдачи штрафа. Одна из частей этих показаний обычно сводится к тому, что радарное

устройство использовалось лишь как резервное средство подтверждения их визуального восприятия того, что вы, ответчик, двигались с «высокой скоростью» или «на X миль/ч». Проще говоря, это полная чушь. Обученный офицер может визуально определить скорость с расстояния примерно 500 футов. Радар теоретически может сделать то же самое определение с расстояния 5000 футов. Сигнализация радара сработает за много секунд до того, как полицейский сможет визуально определить скорость. По сути, наблюдение за машиной лишь подтверждает то, что ему уже сообщил радар. **ЭТО НЕПРАВИЛЬНО!** Закон гласит, что «показания радара могут использоваться ТОЛЬКО как подтверждающее доказательство». Если коп видит, что машина едет медленнее, чем показывает радар, он просто предположит, что водитель его заметил и притормозил. Следующие вопросы используются для установления того, применял ли коп визуальное подтверждение, и для того, чтобы поймать его на заявлении, которое впоследствии можно использовать против него!

A. Я начну этот вопрос, определив понятие, которое я называю «историей трафика». История трафика — это непрерывное наблюдение за трафиком полицейским. Если офицер составляет историю трафика, это означает, что он **непрерывно наблюдает за трафиком**: ищет нарушителей скорости, пьяных водителей и иных нарушителей. Вы понимаете, что я имею в виду под историей трафика?

Если офицер не понимает — объясняйте, пока не поймёт.

B. Применительно к штрафам за превышение скорости: офицер, который говорит, что обычно составляет историю трафика, может утверждать, что он наблюдает за паттернами движения в течение нескольких секунд — обычно от трёх до пяти — прежде чем заметить то, что считает нарушением. То есть за три-пять секунд до того, как сработает сигнализация его радарного устройства. Затем он продолжает наблюдать за трафиком ещё несколько секунд, пока определяет, следует ли выписывать протокол. Вы понимаете это определение истории трафика применительно к штрафам за превышение?

Офицер должен понять.

C. Используя это определение, составляли ли вы **когда-либо** историю трафика до выдачи протокола за превышение?

Скорее всего, ответит «да». Если «нет» — смотрите ответ E.

D. Примерно в каком проценте случаев вы можете сказать, что составляли историю трафика, выписывая штраф за превышение?

Запишите процент. Он, скорее всего, будет очень высоким.

E. Считаете ли вы важным составлять историю трафика в делах о превышении скорости?

Скорее всего, скажет «да». Если «нет» — у вас сильный аргумент в суде: что у него не было визуального подтверждения; что он полностью полагался на своё радарное устройство. Ответ «да» в сочетании с тем, что он не делал этого в вашем случае, может быть использован против него.

F. Примерно с какого расстояния вы можете определить, что машина едет с определённой скоростью в милях в час?

Большинство полицейских отвечают «примерно 500». Если уклоняется или говорит «зависит от ситуации» — задайте конкретный сценарий. Например: он стоит на разделительной полосе прямого и незагроможённого шоссе. С какого расстояния он может визуально определить скорость приближающейся машины? Если говорит, что всё равно не может сказать — назовите 500 футов и посмотрите, согласится ли он. Увеличивайте и уменьшайте цифру, чтобы получить оценку, с которой он может согласиться.

G. Когда вы составляете историю трафика и визуально предполагаете скорость, вы делаете это **до** того, как звуковая сигнализация вашего радара сработала?

> ***ЭТО ВОПРОС-ЛОВУШКА.*** *Если скажет «да» — у него проблемы, потому что дальность его радара, несомненно, больше, чем его зрительная острота. Если скажет «нет» — значит, он по-настоящему не составлял историю трафика. Если «да» — задайте вопросы H и I. Если «нет» — задайте вопросы J, K, L, M, N, O, P, Q, R.*

H. Примерно какова дальность вашего радарного устройства?

> *Скорее всего, скажет, что не знает. Называйте цифры от 3000 до 5000 футов и смотрите, с какой он согласится. Если всё равно не знает — спросите, удивит ли его то, что дальность его радарного устройства составляет не менее 3000 футов. Если скажет «да» — вы только что его припёрли к стене по ключевому техническому вопросу.*

I. Но вы всё равно настаиваете на своём заявлении, что радарное устройство не подаёт сигнал до того, как вы способны распознать истинную скорость машины?

> *Какой бы ни был ответ — вы уже сделали своё дело.*

J. Значит, вы на самом деле не составляете историю трафика.

> *Лучший ответ — «нет», но он, скорее всего, его не даст. Вместо этого скажет: «Иногда да, иногда нет». Для «иногда нет» — вернитесь к вопросам H и I. Для «иногда да» — продолжайте.*

K. Если радарное устройство подаёт сигнал раньше, чем у вас было время установить, что машина превышает скорость, — как вы можете говорить, что составляли историю трафика?

> *Скорее всего, скажет, что сигнал предупреждает его искать нарушителя.*

L. Смотрите ли вы на экран, чтобы увидеть, какую скорость показывает радар?

> *Скорее всего, скажет «да». Если скажет «нет» — скажите ему: «Но вы знаете, что машина точно едет по меньшей мере на X миль/ч сверх ограничения?» На это он должен ответить «да».*

M. Влияет ли знание о том, что радарное устройство уже «поймало» нарушителя, на ваши суждения при визуальном определении скорости машины? То есть будете ли вы более склонны согласиться с тем, что машина едет с определённой скоростью после того, как радар уже сообщил, что она едет именно с такой скоростью?

> *Должен согласиться. Если нет — спросите, почему он не устанавливает порог сигнализации на 99 миль/ч, чтобы она никогда не влияла на его суждение. Его ответ не будет иметь значения.*

N. Были бы вы более склонны считать, что машина в левой полосе четырёхполосного шоссе является нарушителем, если бы услышали срабатывание звуковой сигнализации?

> *Если честен — скажет «да». Если нет — скажет: «если она обгоняет другую машину». Возразите: «А что, если рядом не было транспортного средства для ориентира, но машина всё равно была в левой полосе?» Если всё равно «нет» — снова спросите, почему он не устанавливает счётчик сигнализации на 99 миль/ч.*

O. Если в правой полосе едет машина медленнее ограничения, а в левой — машина, едущая точно по ограничению и явно обгоняющая её, и ваше радарное устройство вышло из строя или неправильно определило цель, — могли бы вы ошибочно решить, что машина в левой полосе превышает скорость, и выписать ей штраф?

Если честен — ответит «да», укрепляя ваш довод об ошибке оператора. Если «нет» — что он мог сказать, что машина в левой полосе не превышала скорость, — вы возвращаетесь к вопросу F.

P. Если ваше радарное устройство показало, что поймало машину, едущую, скажем, 70 миль/ч, и когда вы смогли разглядеть её скорость, она явно ехала по ограничению, — были бы вы склонны считать, что водитель заметил вас и быстро сбросил скорость?

Честный офицер скажет «да».

Q. Выписали бы вы всё равно штраф на основании показаний радара?

Снова должен сказать «да».

R. Почему вы устанавливаете счётчик сигнализации на определённое количество миль в час сверх ограничения?

Его ответ может быть, что так его учили (бесполезно), или что это нужно для особых обстоятельств (стоит уточнить). Любая отговорка будет неубедительной.

Установление уровня знаний об ширине луча и дальности

По делу **HONEYCUTT** полицейскому офицеру не нужно знать внутреннее устройство своего радарного устройства, чтобы его показания были приняты судом. Ошибка многих людей, оспаривающих штрафы за превышение скорости на основании радара, состоит в попытке доказать суду, что они знают о радаре больше, чем коп, выписавший им штраф.

На самом деле не важно, сколько вы знаете о радаре. Суду нужно лишь знать, сколько знает офицер. Мало какие судьи когда-либо ставили под сомнение квалификацию цитирующего офицера. Ваша задача как ответчика — заставить судью сделать именно это! Вам нужно посеять зерно сомнения в его/её сознании, показав, что в нескольких ключевых областях офицер не знает фундаментальных аспектов работы радара.

A. Применительно к повседневной эксплуатации вашего радарного устройства — знаете ли вы, какова его приблизительная дальность?

В зависимости от модели, ответ может варьироваться от 3000 до 7000 футов. Смотрите вторую статью этой серии в следующем захватывающем номере Phrack!

B. На расстоянии 1000 футов — какова ширина радарного луча?

C. Примерно на каком расстоянии от антенны радара луч будет шириной в одну полосу движения, то есть около 11 футов?

D. С какой степенью уверенности вы можете направить антенну вашего радара, скажем, на левую полосу встречного трафика и на расстоянии, допустим, 500 футов быть сосредоточенным именно на этой полосе?

Ответ — ноль. Любой другой ответ неверен.

E. В стационарном режиме вы можете фиксировать скорость транспортного потока в любом направлении, то есть можете переключить антенну для регистрации трафика, движущегося от вас или к вам. Верно?

Да, верно.

F. Может ли ваш радар различать направление движения трафика? Например, если вы стоите вдоль шоссе и направили радарное устройство на встречный трафик, — будет ли ваше радарное

устройство фиксировать только встречный трафик, или также может фиксировать трафик по другую сторону разделительной полосы, движущийся от вас?

> *Оно будет фиксировать трафик в обоих направлениях. Любое иное заявление (например, «иногда да, иногда нет») — невежество.*

G. В движущемся режиме может ли ваш радар фиксировать как трафик, движущийся к вам, так и трафик, движущийся от вас?

> *Speedgun 8 — **ЕДИНСТВЕННЫЙ** радар, который умеет это делать. Он может фиксировать только машины, движущиеся к нему. Никакое другое радарное устройство этого не умеет!*

H. [В следующих двух вопросах вам нужно будет нарисовать схему. Нарисуйте вертикальную дорогу с машиной (#), движущейся вверх, и полицейской машиной, расположенной перпендикулярно дороге (<:=). Затем нарисуйте линию, перпендикулярную дороге (<---). Это радарный луч. Покажите это судье и копу и задайте следующий вопрос:]

```
  | . |
  | . |
  | . |
<-------<:=
  | . |
  | .^|
  | .#|
```

> *На этой схеме радар направлен под прямым углом к дороге. Движущаяся на север машина со скоростью 55 миль/ч въезжает в радарный луч. Зафиксирует ли радарное устройство эту машину?*
> *Нет, не может. Доплеровского сдвига нет, потому что нет скорости сближения между транспортным средством и радарным устройством. Если он ответит верно — переходите к вопросу «J».*

I. [Снова нарисуйте схему, но на этот раз добавьте машину, движущуюся в обратном направлении, в другой полосе. Покажите это копу и судье и спросите следующее:]

```
  |#. |
  |~  |
  | . |
<-------<:=
  | . |
  | .^|
  | .#|
```

> *На этой схеме две машины приближаются с противоположных направлений, а радарное устройство по-прежнему направлено перпендикулярно шоссе. Машина, движущаяся на север (справа), едет 55 миль/ч. Машина, движущаяся на юг (слева), едет 65 миль/ч. Какую машину зафиксирует радарное устройство и как вы сможете различить их?*
> *Если он вообще думает над ответом — он идиот. Ни одна из машин не будет зарегистрирована. (см. вопрос «H»)*

J. Что может остановить луч? Остановят ли его кусты, или можно получить показания сквозь высокую траву, сорняки и кусты?

> *Радар проходит сквозь всё это.*

K. Существуют ли обстоятельства, при которых вы можете получить скорость транспортного средства, которое не видите? Например, можете ли вы получить скорость машины за поворотом или за холмом?

> *В этом мире — нет.*

L. Будет ли ваш радарный луч отражаться от металлической поверхности — знака, машины, металлического здания или стального или бетонного путепровода?

Конечно, будет.

M. Что происходит с лучом при отражении от металлического объекта? Может ли он зафиксировать скорость машины под углом к направлению, на которое у вас направлен радар?

Да, может.

N. Может ли высоковольтная линия электропередачи создать помехи радарному устройству?

Да.

O. Может ли аэродромный или военный радар создать помехи?

Конечно.

P. Замечали ли вы когда-либо помехи от неоновых вывесок или уличных фонарей?

Такие вещи действительно создают помехи.

Заключительные вопросы

К этому моменту вы либо нажили себе врага в лице офицера (наиболее вероятный исход), либо заставили его задуматься об инциденте (если он хороший полицейский). Офицер, конечно, не знает, на какие вопросы он ответил правильно, а на какие — нет. Следите за расхождениями в ответах или, особенно, за любым ослаблением его уверенности в том, что именно ваша машина зарегистрировалась на радарном устройстве.

Вопросы с «N» по «Q» вместе представляют критические процессуальные вопросы. Важно различать внутреннюю калибровку (нажатие кнопки) и внешнюю проверку (прикладывание камертона к антенне).

A. Офицер (имярек), давайте ещё раз вернёмся к вашим воспоминаниям об инциденте. Не могли бы вы изложить факты, касающиеся протокола, так, как вы их помните?

B. Был ли у вас включён аудиодоплер в момент инцидента? Насколько громко или тихо?

C. На какую скорость была установлена ваша звуковая сигнализация? Меняли ли вы её во время смены?

D. Была ли включена ваша автоматическая блокировка скорости?

E. Использовали ли вы ручной переключатель включения/выключения?

F. Вы находились в стационарном или движущемся режиме в тот момент?

G. Ответчик двигался к вам или от вас?

H. Видели ли вы другие транспортные средства перед ответчиком или за ним? Различались ли они по размеру? Различались ли по направлению движения?

I. Был ли трафик, движущийся в том же направлении, что и вы? (если двигались)

J. Видели ли вы ответчика до того, как сработала ваша звуковая сигнализация?

K. Смогли ли вы получить приблизительные данные о скорости на основе визуального наблюдения? Какой был ваш ориентир?

L. Сколько секунд прошло между тем, как вы впервые заметили ответчика, и тем, как сработала ваша звуковая сигнализация?

M. Были ли в этом районе линии электропередачи? Машины или дома с антеннами СВ? Здания с антеннами двустороннего радио? Вы разговаривали по рации в тот момент?

N. Что касается калибровки радарного устройства: используя функцию **внутренней** калибровки, в какое время до и после выдачи протокола вы проверяли радар?

O. Используя **внешний камертон**, в какое время до и после выдачи протокола вы проверяли радар?

P. По вашей оценке, в чём разница между функцией внутренней и внешней калибровки?

Q. Считаете ли вы одну из проверок калибровки более точным индикатором точности? Какую именно?

Заключительное слово

Если вы справились хорошо, вы создали в сознании судьи значительные сомнения в способности данного офицера работать с радарным устройством. Вы заставили его/её задуматься о «большой картине». То есть: «Насколько точен дорожный радар в действительности?» Именно этого вы и хотите добиться — но это нужно делать тонко.

Вы ещё не вышли из ямы! Теперь, когда вы посеяли сомнения в голове судьи, вы **должны** дать показания, которые свяжут воедино всё, что сказал офицер, с вашей версией событий. Здесь вам придётся думать самостоятельно. Как это делается — должно быть вполне очевидно. Ваша задача — разобрать показания. Вы ищете: 1) процессуальные ошибки, 2) недостаточную компетентность офицера, 3) возможные ошибки радара. Если вам удастся зацепить его по двум из трёх пунктов — вы в порядке!

К процессуальным ошибкам относятся вещи вроде упомянутой ранее неверной квитанции. Другая легко разыгрываемая процессуальная ошибка: офицер обязан использовать внешний камертон, сертифицированный по точности, для проверки радарного устройства непосредственно перед выдачей протокола. Два судебных дела, иллюстрирующих это: **ВИСКОНСИН против ХАНСЕНА** и **МИННЕСОТА против ГЕРДЕСА**. Проще говоря, если вам нужно бросить немного веса в суде — просто цитируйте эти два дела. Они великолепны!

Некомпетентность офицера достаточно очевидна. Если он путается в вопросах — он некомпетентен. Все они вполне просты, на мой взгляд. Если коп делает такие вещи, как использует автоматическую блокировку скорости или не использует аудиодоплер, — он откровенно игнорирует своё обучение. Чаще всего они приносят в суд копию своего руководства по обучению. Просто укажите им на это!

Потенциальных ошибок радара слишком много, чтобы перечислять их здесь. Вам нужно постараться найти их в окрестностях места, где вас оштрафовали. Всё, что передаёт на нестандартных частотах, — отличная зацепка (например, охранная сигнализация, гаражные ворота, СВ-рации, любительское радио, дождь, туман, полицейская рация, больницы и т.д.).

В заключение надеюсь, что вы нашли эту информацию полезной, и с нетерпением жду выхода второй части серии: «Как уйти от штрафа за радар: Техническая сторона». В ней я подробно разберу конкретные недостатки, присущие отдельным радарным пистолетам.

Card-O-Rama: Технология магнитных полос и не только

или
«Один день из жизни изменения потока»

Автор: Count Zero (Restricted Data Transmissions)

22 ноября 1992 г.

Загляни в свой кошелёк. Вероятнее всего, у тебя найдётся не менее трёх карточек с магнитными полосами на обороте. Карты банкоматов, кредитные карты, телефонные карты, карты постоянного пассажира, удостоверения личности, пропуска… карточки, карточки, карточки! И, скорее всего, ты понятия не имеешь, какая информация записана на этих полосах и как она закодирована. Этот подробный документ просветит тебя и, надеюсь, пробудит интерес к этой увлекательной области. Ничего из написанного здесь не является «незаконным»… но МНОГИЕ организации (правительство, компании кредитных карт, охранные фирмы и т. д.) предпочли бы держать тебя в неведении. Кроме того, многие люди НЕМЕДЛЕННО решат, что ты ПРЕСТУПНИК, если ты просто «упомянешь», что «интересуешься принципом работы карточек с магнитной полосой». Держи ухо востро, договорились? Просто помни: желание понять, как устроены вещи, — это не преступление, хотя в нашем нынешнем обществе тебя могут навесить ярлык «девианта» (или того хуже — «хакера»)!

В общем, я подробно объясню принцип кодирования магнитных полос и приведу несколько примеров данных, обнаруженных на распространённых карточках. Я также расскажу о теоретических основах магнитной записи и рассмотрю альтернативные технологии кодирования — Wiegand и феррит бария. Будут описаны немагнитные карточные технологии (штрих-код, инфракрасное излучение и т. д.). В заключение будет рассмотрена безопасность систем и последствия распространения технологий «смарт-карт» и биометрии.

Отказ от ответственности

Используй эту информацию для ИЗУЧЕНИЯ, а не для ЗЛОУПОТРЕБЛЕНИЯ. Текст представлен исключительно в информационных целях, и я не несу никакой ответственности за твои действия и их последствия. Я не одобряю мошенничество, кражу и любую другую преступную деятельность.

Предупреждение

В последнее время я заметил несколько «книг» и «журналов», которые ПРОДАЮТСЯ и НАБИТЫ файлами на самые разные компьютерные темы. Изначально эти файлы были выпущены в Сеть с намерением распространять их БЕСПЛАТНО. ОДНАКО теперь эти файлы УПАКОВАНЫ и продаются РАДИ ПРИБЫЛИ. Это меня жутко злит. Я пишу это, чтобы ДЕЛИТЬСЯ БЕСПЛАТНО, и не прошу никакой оплаты. Свободно перепечатывай в твёрдой копии и продавай, если надо, но НИКАКОЙ ПРИБЫЛИ не должно быть. Ни единого чёртова цента! Если КТО-ТО перепечатает этот файл и попытается продать его РАДИ ПРИБЫЛИ, я найду тебя и сделаю твою жизнь невыносимой.

Как? Включи воображение. Реальность окажется хуже.

Поля, головки, запись и считывание магнитных полос

Итак, приступим!

Сначала я объясню основы: поля, головки, кодирование и считывание. Постарайся усвоить ТЕОРИЮ кодирования/считывания. Это очень поможет, если ты когда-нибудь решишь собрать собственный кодировщик/считыватель с нуля (подробнее об этом позже). ФЕРРОМАГНИТНЫЕ материалы — вещества, которые сохраняют намагниченность после снятия внешнего намагничивающего поля. Именно этот принцип лежит в основе ВСЕЙ магнитной записи и воспроизведения. Магнитные ПОЛЮСА всегда существуют попарно внутри намагниченного материала, а линии МАГНИТНОГО ПОТОКА выходят из СЕВЕРНОГО полюса и оканчиваются на ЮЖНОМ. Элементарные частицы МАГНИТНЫХ ПОЛОС — это ферромагнитные частицы длиной около 20 миллионных долей дюйма, каждая из которых действует как крошечный постоянный магнит. Эти частицы жёстко скреплены смоляным связующим. Магнитные частицы производят компании, изготавливающие красящие пигменты для лакокрасочной промышленности, и обычно их называют пигментами. При производстве носителя магнитной полосы элементарные магнитные частицы выравниваются так, чтобы их оси «Север–Юг» были параллельны магнитной полосе, — это делается с помощью внешнего магнитного поля, пока связующее затвердевает.

Эти частицы фактически являются постоянными стержневыми магнитами с ДВУМЯ УСТОЙЧИВЫМИ ПОЛЯРНОСТЯМИ. Если поместить магнитную частицу в сильное внешнее магнитное поле противоположной полярности, она ПЕРЕВЕРНЁТ собственную полярность (Север становится Югом, Юг становится Севером). Напряжённость внешнего магнитного поля, необходимая для этого переворота, называется КОЭРЦИТИВНОЙ СИЛОЙ, или КОЭРЦИТИВНОСТЬЮ частицы. Магнитные пигменты выпускаются с различной коэрцитивностью (подробнее об этом позже).

Незакодированная магнитная полоса — это в действительности серия магнитных доменов «Север–Юг» (см. Рисунок 1). Соседние потоки N–S сливаются, и вся полоса действует как единый стержневой магнит с полюсами Север и Юг на концах.

```
Рисунок 1:               N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S <- частицы в полосе
---------
       представлено как-> N----------------------------S
```

Однако если где-то на полосе создать интерфейс S–S, потоки будут ОТТАЛКИВАТЬСЯ, и мы получим концентрацию линий потока вокруг интерфейса S–S (то же самое с интерфейсом N–N). КОДИРОВАНИЕ состоит в создании интерфейсов S–S и N–N, а СЧИТЫВАНИЕ (как ты уже догадался) — в их обнаружении. Интерфейсы S–S и N–N называются ИЗМЕНЕНИЯМИ ПОТОКА.

```
                            ||| ||| <- линии потока
Рисунок 2:      N------------N-N-S-S-----------------S
---------     линии потока -> ||| |||
```

Внешнее магнитное поле, используемое для переворота полярностей, создаётся СОЛЕНОИДОМ, который может ИЗМЕНЯТЬ полярность, изменяя направление ТОКА. ЗАПИСЫВАЮЩАЯ головка соленоида похожа на стержневой магнит, согнутый в форме кольца так, что полюсы Север/Юг оказываются очень близко и смотрят друг на друга через крошечный зазор. Поле соленоида сосредоточено в этом зазоре, и когда элементарные магнитные частицы магнитной полосы попадают в это поле, они поляризуются в ПРОТИВОПОЛОЖНУЮ сторону (непохожие полюса притягиваются). Если при движении полосы мимо зазора соленоида полярность соленоида МЕНЯЕТСЯ, создаётся ЕДИНСТВЕННОЕ изменение потока (см. Рисунок 3). Чтобы стереть

магнитную полосу, записывающая головка удерживается при ПОСТОЯННОЙ полярности, и ВСЯ полоса проводится мимо неё. Нет изменений потока — нет данных.

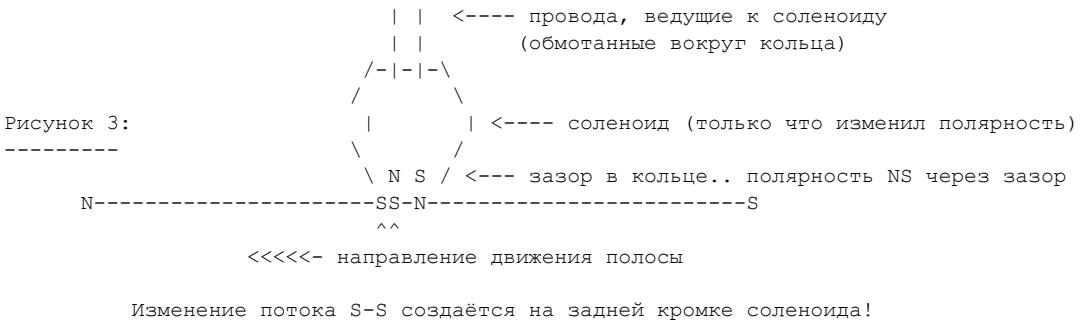


Рисунок 3:

Итак, теперь мы знаем, что изменения потока создаются только В МОМЕНТ ИЗМЕНЕНИЯ полярности соленоида. Если бы соленоид на Рисунке 3 оставался при текущей полярности, дальнейших изменений потока при движении полосы справа налево не создавалось бы. Но если изменить полярность зазора соленоида с NS на *SN*, то (как ты уже догадался) мгновенно создастся изменение потока *N–N*. Просто запомни: на каждое изменение полярности соленоида приходится одно изменение потока (заучи наизусть). Закодированная магнитная полоса — это, таким образом, просто серия изменений потока (NN следует за SS, которое следует за NN).

ДАННЫЕ! ДАННЫЕ! ДАННЫЕ! Вот что тебе нужно! Как, чёрт возьми, изменения потока считываются и интерпретируются как данные? Для обнаружения этих изменений потока используется другой соленоид — ЧИТАЮЩАЯ ГОЛОВКА. Читающая головка работает на принципе ЭЛЕКТРОМАГНИТНОЙ ВЗАИМНОСТИ: ток, протекающий через соленоид, создаёт магнитное поле в зазоре; следовательно, наличие магнитного поля в зазоре соленоидной катушки *порождает ток в катушке*! Наиболее сильные магнитные поля на магнитной полосе находятся в точках изменений потока. Считыватель фиксирует их как пики напряжения, причём полярности +/- соответствуют изменениям потока NN/SS (напомним, изменения потока бывают двух видов).

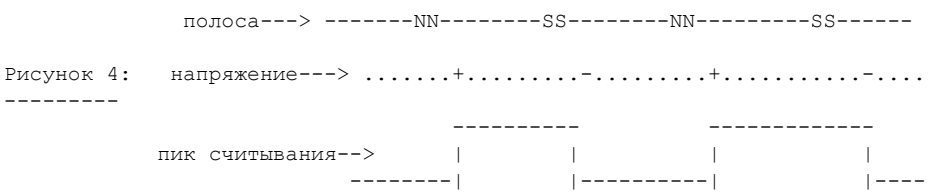


Рисунок 4:

Прямоугольная форма «пика считывания» принципиально важна. Обрати внимание: пик напряжения остаётся неизменным до тех пор, пока не встретится новое изменение потока.

Как же можно закодировать ДАННЫЕ? Наиболее распространённой техникой является так называемая Двухфазная кодировка Айкена (Aiken Biphase), или «двухчастотное когерентное фазовое кодирование» (звучит впечатляюще, не правда ли?). Сначала разберись с диаграммами на Рисунке 5.

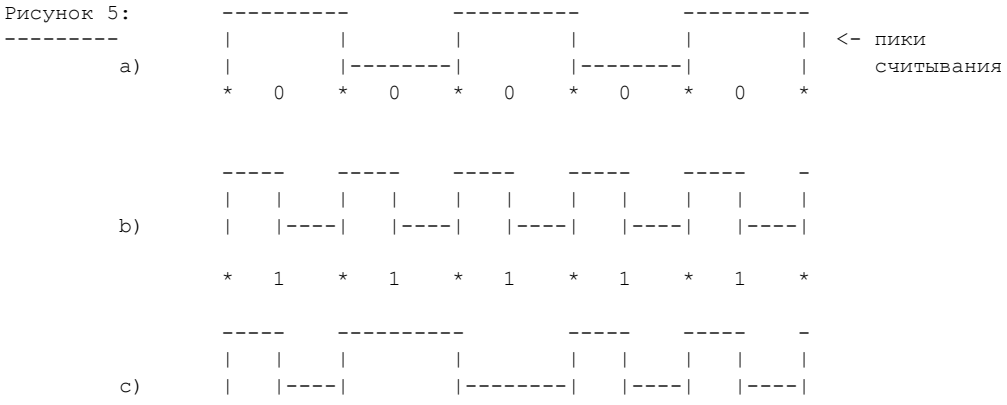


Рисунок 5:

```
                *   1   *   0   *   0   *   1   *   1   *
```

Вот и всё. Данные кодируются в «битовых ячейках», частота которых соответствует частоте сигналов «0». Сигналы «1» имеют частоту ВДВОЕ ВЫШЕ, чем сигналы «0». Таким образом, хотя фактическая частота данных, проходящих мимо считывающей головки, будет варьироваться в зависимости от скорости проведения карты, плотности записи и т. д., частота «1» ВСЕГДА будет ВДВОЕ ВЫШЕ частоты «0». Рисунок 5C показывает точно, как данные «1» и «0» существуют рядом.

Мы приближаемся к считыванию ДАННЫХ! Мы все знакомы с двоичным кодом и тем, как числа и буквы легко представляются в двоичном виде. Очевидно, что возможных стандартов *бесконечное* множество, но, к счастью, Американский национальный институт стандартов (ANSI) и Международная организация по стандартизации (ISO) выбрали 2 стандарта.

Формат данных ANSI/ISO BCD

Это 5-битный формат двоично-десятичного кодирования (BCD). Он использует набор из 16 символов, для которых задействованы 4 из 5 доступных битов. 5-й бит является битом НЕЧЁТНОЙ чётности: это означает, что в 5-битном символе должно быть нечётное количество единиц, и бит чётности «принудительно» делает итог нечётным. Кроме того, на полосе ПЕРВЫМ считывается НАИМЕНЕЕ ЗНАЧИМЫЙ БИТ. См. Рисунок 6.

Сумма единиц в каждом случае нечётна благодаря биту чётности. Если считывающая система сложит 5 битов и получит ЧЁТНОЕ число, она пометит считывание как ОШИБКУ, и тебе придётся снова провести картой (я *знаю*, что многие из вас *уже* понимают чётность, но нужно охватить все основы… не все засыпают с модемом и могут наизусть рассказать весь набор AT-команд).

```
Рисунок 6:        Формат данных ANSI/ISO BCD
---------

 * Помни, что b1 (бит №1) — это МЗБ (наименее значимый бит)!
 * МЗБ считывается ПЕРВЫМ!
 * Шестнадцатеричные представления битов данных указаны в скобках (xH).

       --Биты данных--   Чётность
       b1  b2  b3  b4   b5    Символ   Функция

       0   0   0   0    1       0 (0H)    Данные
       1   0   0   0    0       1 (1H)      "
       0   1   0   0    0       2 (2H)      "
       1   1   0   0    1       3 (3H)      "
       0   0   1   0    0       4 (4H)      "
       1   0   1   0    1       5 (5H)      "
       0   1   1   0    1       6 (6H)      "
       1   1   1   0    0       7 (7H)      "
       0   0   0   1    0       8 (8H)      "
       1   0   0   1    1       9 (9H)      "
       0   1   0   1    1       : (AH)    Управляющий
       1   1   0   1    0       ; (BH)    Начальный маркер
       0   0   1   1    1       < (CH)    Управляющий
       1   0   1   1    0       = (DH)    Разделитель полей
       0   1   1   1    0       > (EH)    Управляющий
       1   1   1   1    1       ? (FH)    Конечный маркер


          ***** 16-символьный 5-битный набор *****
               10 символов числовых данных
               3 символа обрамления/разделителей полей
               3 управляющих символа
```

Магнитная полоса начинается со строки нулевых битовых ячеек, чтобы функция самосинхронизации двухфазного кодирования могла «синхронизироваться» и начать декодирование. Затем символ «Начальный маркер» сообщает процессу переформатирования, где начать группировать декодированный битовый поток в группы по 5 битов. В конце данных встречается «Конечный маркер», за которым следует символ «Продольной проверки избыточности» (LRC). LRC — это проверка чётности для сумм всех битов b1, b2, b3 и b4 данных всех предшествующих символов. Символ LRC позволяет обнаружить редкую ошибку, которая может возникнуть, если отдельный символ имеет две компенсирующие ошибки в битовом шаблоне (что обманет проверку 5-го бита чётности).

Начальный маркер, конечный маркер и LRC называются «Символами обрамления» и отбрасываются в конце процесса переформатирования.

Формат данных ANSI/ISO ALPHA

На магнитных полосах могут быть закодированы и буквенно-цифровые данные. Второй формат ANSI/ISO — ALPHA (буквенно-цифровой) — использует 7-битный набор из 64 символов. Как и прежде, к необходимым 6 битам данных для каждого из 64 символов добавляется бит нечётной чётности. См. Рисунок 7.

Рисунок 7:
--------- Формат данных ANSI/ISO ALPHA

* Помни, что b1 (бит №1) — это МЗБ (наименее значимый бит)!
* МЗБ считывается ПЕРВЫМ!
* Шестнадцатеричные представления битов данных указаны в скобках (xH).

------Биты данных-------						Чётность		
b1	b2	b3	b4	b5	b6	b7	Символ	Функция
0	0	0	0	0	0	1	пробел (0H)	Специальный
1	0	0	0	0	0	0	! (1H)	"
0	1	0	0	0	0	0	" (2H)	"
1	1	0	0	0	0	1	# (3H)	"
0	0	1	0	0	0	0	$ (4H)	"
1	0	1	0	0	0	1	% (5H)	Начальный маркер
0	1	1	0	0	0	1	& (6H)	Специальный
1	1	1	0	0	0	0	' (7H)	"
0	0	0	1	0	0	0	((8H)	"
1	0	0	1	0	0	1	) (9H)	"
0	1	0	1	0	0	1	* (AH)	"
1	1	0	1	0	0	0	+ (BH)	"
0	0	1	1	0	0	1	, (CH)	"
1	0	1	1	0	0	0	- (DH)	"
0	1	1	1	0	0	0	. (EH)	"
1	1	1	1	0	0	1	/ (FH)	"
0	0	0	0	1	0	0	0 (10H)	Данные (числовые)
1	0	0	0	1	0	1	1 (11H)	"
0	1	0	0	1	0	1	2 (12H)	"
1	1	0	0	1	0	0	3 (13H)	"
0	0	1	0	1	0	1	4 (14H)	"
1	0	1	0	1	0	0	5 (15H)	"
0	1	1	0	1	0	0	6 (16H)	"
1	1	1	0	1	0	1	7 (17H)	"
0	0	0	1	1	0	1	8 (18H)	"
1	0	0	1	1	0	0	9 (19H)	"
0	1	0	1	1	0	0	: (1AH)	Специальный
1	1	0	1	1	0	1	; (1BH)	"
0	0	1	1	1	0	0	< (1CH)	"

```
1   0   1   1   1   0     1        = (1DH)     "
0   1   1   1   1   0     1        > (1EH)     "
1   1   1   1   1   0     0        ? (1FH)  Конечный маркер
0   0   0   0   0   1     0        @ (20H)  Специальный

1   0   0   0   0   1     1        A (21H)  Данные (буква)
0   1   0   0   0   1     1        B (22H)     "
1   1   0   0   0   1     0        C (23H)     "
0   0   1   0   0   1     1        D (24H)     "
1   0   1   0   0   1     0        E (25H)     "
0   1   1   0   0   1     0        F (26H)     "
1   1   1   0   0   1     1        G (27H)     "
0   0   0   1   0   1     1        H (28H)     "
1   0   0   1   0   1     0        I (29H)     "
0   1   0   1   0   1     0        J (2AH)     "
1   1   0   1   0   1     1        K (2BH)     "
0   0   1   1   0   1     0        L (2CH)     "
1   0   1   1   0   1     1        M (2DH)     "
0   1   1   1   0   1     1        N (2EH)     "
1   1   1   1   0   1     0        O (2FH)     "
0   0   0   0   1   1     1        P (30H)     "
1   0   0   0   1   1     0        Q (31H)     "
0   1   0   0   1   1     0        R (32H)     "
1   1   0   0   1   1     1        S (33H)     "
0   0   1   0   1   1     0        T (34H)     "
1   0   1   0   1   1     1        U (35H)     "
0   1   1   0   1   1     1        V (36H)     "
1   1   1   0   1   1     0        W (37H)     "
0   0   0   1   1   1     0        X (38H)     "
1   0   0   1   1   1     1        Y (39H)     "
0   1   0   1   1   1     1        Z (3AH)     "

1   1   0   1   1   1     0        [ (3BH)   Специальный
0   0   1   1   1   1     1        \ (3DH)   Специальный
1   0   1   1   1   1     0        ] (3EH)   Специальный
0   1   1   1   1   1     0        ^ (3FH)   Разделитель полей
1   1   1   1   1   1     1        _ (40H)   Специальный
```

```
***** 64-символьный 7-битный набор *****
    * 43 буквенно-цифровых символа данных
    * 3 символа обрамления/разделителей полей
    * 18 управляющих/специальных символов
```

^ ^ ^			
----------	0.223"--	---------	----------
		0.353"	^
.....	.....	.....	0.493"
Дорожка №1 0.110"			
.....	.....	... <МАГН. ПОЛОСА>	
.....	.....	...	
Дорожка №2 0.110"			
.....	...		
.....	...		
Дорожка №3 0.110"			

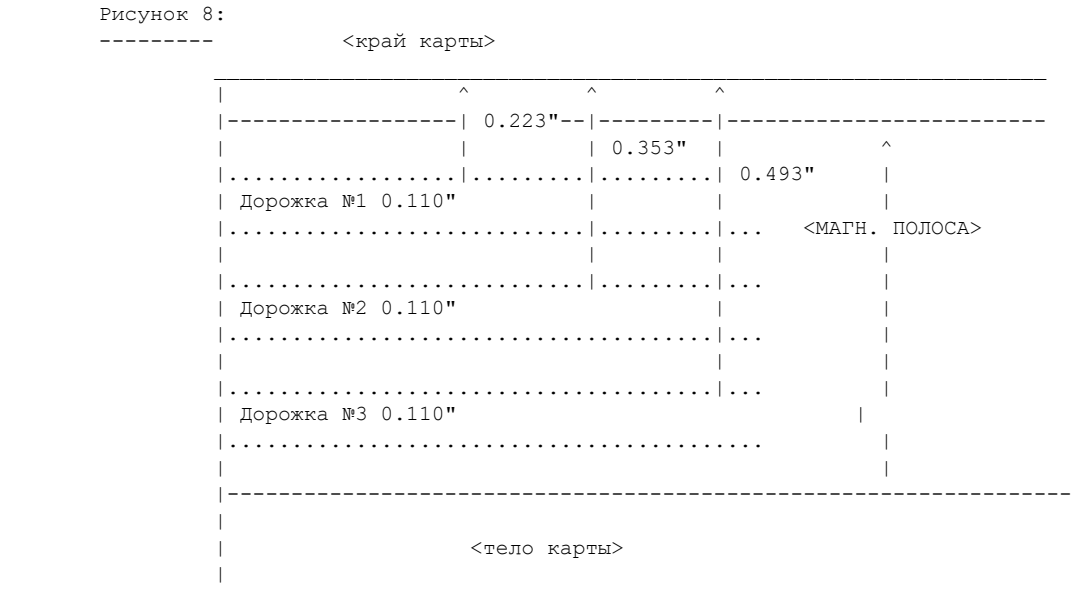
.....			
<тело карты>			

Два формата ANSI/ISO — ALPHA и BCD — позволяют хранить на магнитных полосах самые разнообразные данные. Большинство карточек с магнитными полосами используют именно эти форматы, хотя иногда встречаются и исключения. Подробнее об этом ниже.

Дорожки и протоколы кодирования

Теперь мы знаем, как хранятся данные. Но ГДЕ именно они хранятся на магнитной полосе? Стандарты ANSI/ISO определяют *3* дорожки, каждая из которых используется для различных целей. Дорожки определяются исключительно их расположением на магнитной полосе, поскольку магнитная полоса в целом однородна по своим магнитным свойствам. См. Рисунок 8.

Рисунок 8:



Видны точные расстояния каждой дорожки от края карты, а также одинаковая ширина и интервал. Положи карту с магнитной полосой перед собой так, чтобы магнитная полоса была видна в нижней части карты. Данные кодируются слева направо (как при чтении книги). См. Рисунок 9.

Рисунок 9:

Стандарты ANSI/ISO, Дорожки 1, 2, 3

Дор.	Название	Плотность	Формат	Символов	Функция
1	IATA	210 bpi	ALPHA	79	Имя и счёт держателя
2	ABA	75 bpi	BCD	40	Счёт держателя
3	THRIFT	210 bpi	BCD	107	Чтение счёта & *Запись* транзакции

*** Структура Дорожки 1: ***

НМ	КФ	PAN	Имя	РП	Дополнительные данные	КМ	LRC

НМ = Начальный маркер "%"
КФ = Код формата
PAN = Основной номер счёта (до 19 цифр)
РП = Разделитель полей "^"

```
 Имя = до 26 буквенно-цифровых символов
 Дополнительные данные = Срок действия, смещение, зашифрованный PIN и т. д.
 КМ = Конечный маркер "?"
 LRC = Продольная проверка избыточности


*** Структура Дорожки 2: ***

        | НМ |  PAN  | РП | Дополнительные данные | КМ | LRC |

 НМ = Начальный маркер ";"
 PAN = Основной номер счёта (до 19 цифр)
 РП = Разделитель полей "="
 Дополнительные данные = Срок действия, смещение, зашифрованный PIN и т. д.
 КМ = Конечный маркер "?"
 LRC = Продольная проверка избыточности


*** Структура Дорожки 3: ** Аналогична дорожкам 1 и 2. Почти не используется.
                            Применяется множество различных стандартов данных.
```

Дорожка 2, «American Banking Association» (ABA), используется наиболее широко. Именно её считывают банкоматы и устройства проверки кредитных карт. Ассоциация ABA разработала спецификации этой дорожки, и все мировые банки обязаны им следовать. Она содержит счёт держателя карты, зашифрованный PIN и прочие данные на усмотрение эмитента.

Дорожка 1 названа в честь «Международной ассоциации воздушного транспорта» (IATA) и содержит имя держателя карты, а также счёт и прочие данные. Иногда её используют авиакомпании при бронировании рейса с оплатой кредитной картой: твоё имя «всплывает» на их терминале, когда они проводят картой!

Поскольку дорожка 1 позволяет хранить ЗНАЧИТЕЛЬНО больше информации, компании кредитных карт стараются убедить розничных продавцов приобретать считыватели карт, читающие дорожку 1. *Проблема* в том, что большинство считывателей карт читают либо дорожку 1, либо дорожку 2, но НЕ ОБЕ СРАЗУ! А установленная база считывателей в настоящее время ориентирована на дорожку 2. VISA USA находится в авангарде этой «миграции» на дорожку 1, предлагая считыватели дорожки 1 по сниженным ценам через банки-партнёры. Представитель VISA прокомментировал:

> *«Мы считаем, что Дорожка 1 обеспечивает большую гибкость и потенциал для передачи большего объёма информации, и мы намерены строить новые сервисы на основе расширенных возможностей этой информации.»*

Что за новые сервисы? Остаётся только ждать и смотреть.

Дорожка 3 уникальна. Предполагалось, что данные на ней будут как считываться, так и ЗАПИСЫВАТЬСЯ. Информация о счёте держателя карты должна была ОБНОВЛЯТЬСЯ прямо на магнитной полосе. К сожалению, дорожка 3 — это практически заброшенный стандарт. Изначально она предназначалась для управления офлайн-транзакциями банкоматов, но поскольку банкоматы теперь работают в режиме онлайн ПОСТОЯННО, она почти бесполезна. К тому же розничные продавцы и банки должны были бы установить НОВЫЕ считыватели карт для считывания этой дорожки, а это стоит денег.

Протокол кодирования предусматривает, что каждая дорожка должна начинаться и заканчиваться последовательностью из нулевых битов, называемых БИТАМИ СИНХРОНИЗАЦИИ. Они используются для синхронизации функции самосинхронизации двухфазного декодирования. См. Рисунок 10.

```
Рисунок 10:                              конечный маркер
                    начальный маркер       |  продольная проверка избыточности
                     |                     |  |
      000000000000000 НМ.................КМ LRC 0000000000000000
       ведущие           данные, данные         ведомые
       биты              данные                 биты
```

```
синхронизации                    синхронизации
(длина варьируется)              (длина варьируется)
```

ВОТ И ВСЁ! Перед тобой стандарты ANSI/ISO, полностью объяснённые. Теперь плохие новости. НЕ КАЖДАЯ КАРТА ИМ СЛЕДУЕТ! Кредитные карты и карты банкоматов будут соответствовать этим стандартам. НО существует много других типов карточек. Пропуска безопасности, карточки ксероксов, значки-удостоверения — и КАЖДАЯ из них может использовать СОБСТВЕННУЮ систему плотности/формата/расположения дорожек. ANSI/ISO ОБЯЗАТЕЛЕН для финансовых транзакционных карт, используемых в международной межбанковской сети. Все остальные карты могут играть по своим правилам.

Хорошая новость. БОЛЬШИНСТВО других карточек всё же следуют стандартам, потому что ПРОЩЕ следовать стандарту, чем РАЗРАБАТЫВАТЬ СОБСТВЕННЫЙ! Большинство карточек с магнитными полосами, помимо кредитных карт и карт банкоматов, будут использовать те же спецификации дорожек и форматы BCD или ALPHA.

Немного об оборудовании для работы с магнитными полосами

«Вау, теперь я знаю, как интерпретировать все данные на магнитных полосах! Но… подождите-ка, какое оборудование нужно для считывания полос? Где купить считыватель? Я не вижу ни одного в Radio Shack!»

К сожалению, оборудование для работы с магнитными полосами трудно достать. По очевидным причинам считыватели карт не находятся в свободном доступе для потребителей. Как его собрать — тема для отдельного файла (этот и так уже слишком длинный).

Лучший вариант — попытаться найти что-нибудь в магазинах распродажи электроники и на барахолках. Даже не пытайся купить напрямую у производителя: они немедленно решат, что у тебя «преступные намерения». А что касается того, чтобы раздобыть КОДИРОВЩИК магнитных полос… ну, удачи! Эти редкие красавцы стоят на вес золота. Держи глаза открытыми, осматривайся — и МОЖЕТ БЫТЬ, тебе повезёт! Немного социальной инженерии может оказаться весьма полезным.

Существуют различные виды считывателей/кодировщиков магнитных полос. Наиболее распространённые — «свайп»-машины: те, через которые нужно физически провести картой. Другие — «вставные» машины: как банкоматы, они «проглатывают» карту, а затем выдают обратно после транзакции. Стоимость исчисляется тысячами долларов, но, как я и говорил, на барахолках и в магазинах распродажи на них нередко можно найти ОТЛИЧНЫЕ предложения. Ещё одна проблема — документация к этим машинам. Если позвонить производителю и просто попросить её, тебе, скорее всего, откажут. «Эй, парень, что ты делаешь с нашим свайп-считывателем модели XYZ? Он предназначен для "квалифицированных" торговцев или розничных продавцов, а не для какого-то панка, пытающегося "разобраться, как всё работает!"» Снова может потребоваться социальная инженерия. Скажи им, что открываешь новый бизнес. Скажи, что работаешь над научным проектом. Говори им всё, что работает!

В журнале 2600 недавно вышла хорошая статья о том, как собрать машину, копирующую карточки с магнитными полосами. Подробностей о форматах данных и схемах кодирования маловато, но описанное устройство — хорошее начало. С некоторыми доработками, держу пари, можно направить выходной сигнал на «тупой» терминал (или через нуль-модемный кабель), чтобы ЧИТАТЬ данные. Стоит поизучать схемы.

Что касается изготовления собственных карточек: просто приклей кусок ленты из видеомагнитофона, катушечного магнитофона или аудиокассеты к вырезанной из картона или пластика карточке. Работает так же хорошо, как настоящее, и полезно для экспериментов, если под

рукой нет просроченных или «мёртвых» карт банкоматов или телефонных карт (СОХРАНЯЙ их, не ВЫБРАСЫВАЙ!).

Примеры данных на магнитных полосах

Настоящий кайф в экспериментах с технологией магнитных полос — это ЧИТАТЬ карточки и выяснять, ЧТО ЧЁРТ ПОБЕРИ на них ЗАПИСАНО! Ты разве не интересовался? Следующие карточки — результат моих собственных «исследований». Такие данные, как конкретные номера счетов и имена, изменены для защиты невиновных. Ни одна из использованных карточек не была украдена или получена незаконным путём.

Обрати внимание, что я тщательно отмечаю «общие данные» — данные, которые одинаковы для всех карточек определённого типа. Ниже они выделены звёздочками (*). Там, где я обнаружил переменные данные, я указываю их «x»-ами. В таких случаях КОЛИЧЕСТВО СИМВОЛОВ оставалось неизменным (количество «x» равно количеству символов — соответствие один к одному).

Некоторые поля данных мне по-прежнему непонятны, но я надеюсь написать продолжение этого файла после сбора дополнительных данных. Найти много карточек для изучения НЕ так просто. Проси друзей, родственников и коллег помочь! «Эй, можно я, ну, типа ВОЗЬМУ твою карточку MCI на вечер? Я работаю над, ну, ЭКСПЕРИМЕНТОМ. Пожалуйста?» Просто… будь честен! Ещё порывшись в мусоре, можно поживиться. Люди часто складывают просроченные карточки пополам, а потом выбрасывают. Просто разогни их обратно в нормальную форму, и они, как правило, заработают (я так делал!). Они могут быть просрочены, но они не СТЁРТЫ!

```
--------------------------------------------------------------------------------
-=Mastercard=-  Номер на лицевой стороне -> 1111 2222 3333 4444
                Срок действия -> 12/99

Дорожка 2 (BCD, 75 bpi)-> ;1111222233334444=99121010000000000000?
                                            ***

Дорожка 1 (ALPHA, 210 bpi)-> %B1111222233334444^PUBLIC/JOHN?
                              *

Примечание: «101» было общим для всех проверенных карт MC, как и «B».
--------------------------------------------------------------------------------
-=VISA=-  Номер на лицевой стороне -> 1111 2222 3333 4444
          Срок действия -> 12/99

Дорожка 2 (BCD, 75 bpi)-> ;1111222233334444=9912101xxxxxxxxxxxxx?
                                            ***
Дорожка 1 (ALPHA, 210 bpi)-> %B1111222233334444^PUBLIC/JOHN^9912101xxxxxxxxxxxxx?
                              *

Примечание: «101» было общим для всех проверенных карт VISA, как и «B».
Кроме того, «xxx» означает числовые данные, которые варьировались от карты к
карте без видимой закономерности. Я полагаю, это зашифрованный PIN для получения
«наличных авансов» в банкоматах. Во всех случаях я находил *13* цифр.
--------------------------------------------------------------------------------
-=Discover=-  Номер на лицевой стороне -> 1111 2222 3333 4444
              Срок действия -> 12/99

Дорожка 2 (BCD, 75 bpi)-> ;1111222233334444=991210100000?
                                            ********

Дорожка 1 (ALPHA, 210 bpi)-> %B1111222233334444^PUBLIC/JOHN___^991210100000?
                                                          ********
Примечание: «10100000» и «B» были общими для большинства проверенных карт
DISCOVER. Некоторые имели «10110000» — значение этого отличия неизвестно.
```

```
Обрати внимание на подчёркивания после имени JOHN. Я стабильно обнаруживал, что
поле имени содержит *26* символов. Всё оставшееся место после имени
«дополняется» ПРОБЕЛАМИ. Итак, всем, чьё имя длиннее 25 символов (исключая «/»),
ГОТОВЬТЕСЬ К УСЕЧЕНИЮ! ;)
--------------------------------------------------------------------------------
-=US Sprint FON=-  Номер на лицевой стороне -> 111 222 3333 4444

Дорожка 2 (BCD, 75 bpi)-> ;xxxxxx11122233339==xxx4444xxxxxxxxxx=?
                                          *

Дорожка 1 (ALPHA, 210 bpi)-> %B^ /^^xxxxxxxxxxxxxxxxx?
                               *

Странно. Ни на одной из проверенных карт не было имён в полях Дорожки 1.
Дорожка 1 выглядит неиспользованной, однако всегда была отформатирована с
разделителями полей. «xxx» варьировались от карты к карте без видимой
закономерности. Я знаю, что это не PIN, значит, это должны быть данные счёта.
--------------------------------------------------------------------------------
-=Fleet Bank=-  Номер на лицевой стороне -> 111111 222 3333333
                Срок действия -> 12/99

Дорожка 2 (BCD, 75 bpi)-> ;1111112223333333=9912120100000000xxxx?
                                             ****

Дорожка 1 (ALPHA, 210 bpi) ->
         %B1111112223333333^PUBLIC/JOHN___^99121201000000000000xxxx000000?
          *                                 ****

Примечание: «xxx» данные варьировались — это смещение зашифрованного PIN.
Всегда 4 цифры (хм...). «1201» было всегда одинаковым. Я проверил много карт
банкоматов из РАЗНЫХ БАНКОВ — и у всех было «1201».
--------------------------------------------------------------------------------
(Без этой нельзя уйти ;)
-=Radio Shack=-  Номер на лицевой стороне -> 1111 222 333333
                 Данных о СРОКЕ ДЕЙСТВИЯ на карте нет

Дорожка 2 (BCD, 75 dpi)-> ;1111222333333=9912101?
                                       *******

Примечание: «9912101» было ОДИНАКОВЫМ для КАЖДОЙ карты Radio Shack, которую
я видел. Похоже, когда для поля срока действия нет «настоящих» данных,
туда всё равно нужно что-то вставить.
--------------------------------------------------------------------------------
```

Вот, собственно, и всё, что я хочу показать прямо сейчас. Как видно, основные типы карточек (банкоматы, кредитные карты) в целом следуют одним и тем же правилам. Я проверил несколько пропусков безопасности и карточек для отметки рабочего времени — и у ВСЕХ на Дорожке 2 была записана случайная информация. Дорожка 2 БЕЗУСЛОВНО является САМОЙ ИСПОЛЬЗУЕМОЙ дорожкой на карте. И формат почти всегда ANSI/ISO BCD. Мне *действительно* попались карточки-ключи от гостиничных номеров, которые при сканировании выдавали МУСОР. Скорее всего, они использовали набор символов, отличный от ASCII (если бы там были аудиотоны, мой считыватель выдал бы НИЧЕГО… а не МУСОР). Как видишь, по типам данных на карточках можно написать целую КНИГУ. Я хотел лишь привести несколько примеров. Мои исследования ограничены, но я старался делать логические выводы на основе полученных данных.

Карточки на любой вкус

Людям хотелось хранить МНОГО данных на пластиковых карточках. И они хотели, чтобы эти данные были «невидимы» для держателей карт. Вот различные карточные технологии, которые были изобретены и доступны сегодня.

HOLLERITH — в этой системе в пластиковых или бумажных карточках пробиваются отверстия, считываемые оптически. Одна из старейших технологий, сегодня встречается в виде кодированных гостиничных ключей. Технология не защищена, но карточки дёшевы в изготовлении.

ШТРИХ-КОД — применение штрих-кодов ограничено. Они дёшевы, но практически не обеспечивают безопасности, а полоса со штрих-кодом легко повреждается.

ИНФРАКРАСНЫЙ — не получил широкого распространения; карточки кодируются на заводе путём создания «теневого рисунка» внутри карточки. Карточка проводится через свайп- или вставной считыватель, использующий инфракрасный сканер. Цены на инфракрасные карточки — от умеренных до высоких, кодирование достаточно надёжно. Инфракрасные сканеры оптические и поэтому уязвимы к загрязнению.

БЕСКОНТАКТНЫЙ (proximity) — основное преимущество этой карточки — работа без физического контакта. Хотя используются различные схемотехнические решения, все бесконтактные карточки позволяют передавать код простым поднесением карточки к считывателю (на 6–12 дюймов). Эти карточки довольно толстые — до 0,15" (стандарт ABA — 0,030"!).

WIEGAND — названная в честь своего изобретателя, эта технология использует серию тонких проволочек, которые при воздействии изменяющегося магнитного поля индуцируют дискретный выходной сигнал напряжения в сенсорной катушке. Два ряда проволочек встроены в кодированную полоску. Когда проволочки проходят мимо считывающей головки, считывается серия импульсов, интерпретируемых как двоичный код. Эта технология создаёт карточки, которые ОЧЕНЬ сложно скопировать или изменить; карточки стоят умеренно дорого. Считыватели на основе этой технологии залиты эпоксидной смолой, что делает их нечувствительными к погодным условиям; ни карточки, ни считыватели не подвержены воздействию внешних магнитных полей (можешь смело класть эти карточки на телевизор — не повредишь!). Вот пример расположения проволочек в полоске Wiegand:

Проволочки СНАРУЖИ карточки НЕ видны, но если твоя карточка белая, поднеси её к ОЧЕНЬ яркому источнику света и загляни внутрь. Обрати внимание, что расстояния между проволочками одинаковые.

ФЕРРИТ БАРИЯ — старейшая технология магнитного кодирования (существует уже 40 лет!), использует небольшие кусочки намагниченного феррита бария, помещённые внутрь пластиковой карточки. Полярность и расположение «пятен» определяют кодирование. Эти карточки имеют короткий срок службы и ШИРОКО используются на парковках (высокая частота смены, минимальная безопасность). Карточки с ферритом бария используются ТОЛЬКО со вставными считывателями.

Вот и все наиболее распространённые типы карточек. Магнитные полосы популярны потому, что они ДЁШЕВЫ и относительно надёжны.

Коэрцитивность магнитных полос

Сами магнитные полосы бывают разных видов. Необходимо задать КОЭРЦИТИВНОСТЬ магнитного носителя. Коэрцитивность — это напряжённость магнитного поля, необходимая для размагничивания закодированной полосы, и, следовательно, она определяет требуемую напряжённость поля записывающей головки. Доступны носители с коэрцитивностью от 300 до 4000 Эрстед. Это сводится к ВЫСОКОЭНЕРГЕТИЧЕСКИМ магнитным полосам (4000 Э) и

НИЗКОЭНЕРГЕТИЧЕСКИМ магнитным полосам (300 Э).

ПОМНИ: поскольку все магнитные полосы имеют одинаковую остаточную намагниченность независимо от их коэрцитивности, считыватели НЕ МОГУТ отличить ВЫСОКО- и НИЗКОЭНЕРГЕТИЧЕСКИЕ полосы. Оба типа считываются одинаково одними и теми же машинами.

НИЗКОЭНЕРГЕТИЧЕСКИЙ носитель наиболее распространён. Он используется на всех финансовых карточках, но его недостаток — подверженность случайному размагничиванию от контакта с обычными магнитами (поля магнитов холодильника, телевизора и т. д.). Однако эти карточки большую часть времени хранятся в кошельках и сумочках.

ВЫСОКОЭНЕРГЕТИЧЕСКИЙ носитель используется для служебных пропусков и карточек контроля доступа, которые применяются в «агрессивных» условиях (носятся на форме, используются на складах). Обычные магниты не влияют на эти карточки, а низкоэнергетические кодировщики не могут на них записывать.

Не всё, что меняется в потоке, — цифровое

Не все карточки с магнитными полосами работают на методе цифрового кодирования. НЕКОТОРЫЕ карточки кодируют ЗВУКОВЫЕ ТОНЫ, а не цифровые данные. Такие карточки, как правило, используются со старым устаревшим промышленным оборудованием, где безопасность не критична и не нужно кодировать большой объём данных. Некоторые проездные на метро именно такие. Им нужны только данные о сроке действия на магнитной полосе, и короткой последовательности меняющихся частот и длительностей вполне достаточно. Частоты будут варьироваться в зависимости от скорости проведения картой, но ОТНОСИТЕЛЬНЫЕ частоты останутся неизменными (например, тон 1 вдвое выше по частоте, чем тон 2, и вдвое ниже, чем тон 3, вне зависимости от исходных частот!). Возьми осциллограф, чтобы визуализировать тоны, и послушай их на стереосистеме. Я сам с такими карточками не экспериментировал.

Безопасность и смарт-карты

Многие системы безопасности используют карточки с магнитными полосами — в виде пропусков и удостоверений личности. Интересно, что в РЯДЕ случаев я обнаружил серьёзный ИЗЪЯН в системе безопасности. В этих случаях на карточке был НАПЕЧАТАН код. При сканировании оказывалось, что именно этот номер закодирован на магнитной полосе. Проблема была в том, что КОД был ЕДИНСТВЕННЫМ, что я находил на магнитной полосе! То есть, просто взглянув на лицевую сторону карточки, я сразу знал, что на ней закодировано. Ооопс! Это делает чертовски простым дело — мельком взглянуть на карточку Джо за обедом, затем прийти домой и сделать СОБСТВЕННУЮ копию пропуска Джо! К счастью, этот изъян я обнаружил только в «небольших» компаниях (а иногда даже в университетах). Крупные компании, по всей видимости, понимают лучше и НЕ ПЕЧАТАЮТ ВСЕ данные магнитной полосы прямо на карточке крупными, легко читаемыми цифрами. По крайней мере, те крупные компании, которые *я* проверял. ;)

К другим просчётам в безопасности относятся магнитные полосы пропусков, закодированные ИСКЛЮЧИТЕЛЬНО с номером социального страхования владельца (да, очень сложно узнать чей-то номер SS… ОТЛИЧНАЯ идея), а также пропуска с кодами всего из 3–4 цифр.

Технология смарт-карт предполагает использование чипов, встроенных в пластиковые карточки, с контактными площадками, которые временно соединяются с оборудованием считывателя.

Очевидно, что таким образом можно хранить ОГРОМНЫЙ объём данных, а несанкционированное копирование было бы очень затруднено. Что интересно, крупные компании кредитных карт не прилагают особых усилий к развитию смарт-карт. Они считают, что технология слишком дорога, и полагают, что на магнитных полосах (особенно на Дорожке 1) в будущем можно будет разместить ещё больше данных. Мне это чем-то напоминает использование металлооксидных дисковых носителей. Конечно, они не самые лучшие (по сравнению со стираемо-записываемыми оптическими дисками), но они ДЁШЕВЫ… и мы просто продолжаем их совершенствовать. Магнитные полосы будут с нами ещё долго. Носители будут совершенствоваться, плотность данных — расти. Но для обычных приложений огромные возможности хранения смарт-карт просто не нужны.

Биометрия: выброси свои карточки!

Хочу закончить упоминанием биометрии: технологии, основанной на считывании физических характеристик человека с помощью сканирования сетчатки, верификации подписи, голосовой верификации и других методов. Когда-то это было ограничено государственным применением и сверхсекретными объектами. Однако биометрия вскоре займёт большую долю рынка средств контроля доступа, поскольку этап её разработки в значительной мере завершён, а стоимость станет доступной для большего числа покупателей. В конечном счёте можно ожидать, что биометрия заменит практически ВСЕ карточки… потому что все эти пластиковые карточки в твоём кошельке существуют ТОЛЬКО для того, чтобы помочь КОМПАНИЯМ *идентифицировать* ТЕБЯ. А при биометрии они будут знать тебя без необходимости считывать карточки.

Я не параноик и не придерживаюсь никакого грандиозного «корпоративного заговора», но меня немного тревожит, что наши физические характеристики, скорее всего, когда-нибудь окажутся в холодных, бескрайних электронных базах данных КОРПОРАТИВНОГО мира. Доступных каждому, кто готов заплатить. Представь себе базы данных CBI и TRW с твоим изображением сетчатки, отпечатком пальца и голосовым образцом в режиме онлайн для мгновенного удобного поиска. Сегодня человек МОЖЕТ ВЫБРАТЬ не иметь кредитной карты или банковской карты… мы можем разрезать наши пластиковые удостоверения личности! Без карточки считыватель бесполезен и не может тебя идентифицировать.

Оплата наличными делает тебя невидимым! Однако при биометрии машине достаточно лишь наблюдать… слушать… и записывать. При этом правительство и корпоративная Америка нажимают на все кнопки. «Платите наличными?.. Спасибо… Пожалуйста, посмотрите в камеру. О, вижу, вас зовут Мистер Смит… упс… мой компьютер говорит, что вы не оплатили счёт за газ… боюсь, мне придётся оставить эти деньги и зачислить их на ваш газовый счёт… у вас есть ещё наличные?.. или вы предпочитаете, чтобы я вычел долг из вашей зарплаты?» Хе-хе.

Заключительные замечания (НАКОНЕЦ-ТО!!!!)

Фу… это был МОНСТР из файлов. Надеюсь, было интересно, и надеюсь, ты распространишь его среди всех своих друзей. Этот файл — производство «Restricted Data Transmissions»… группы технарей из района Бостона, убеждённых, что «Информация — это Сила»… и мы намерены выпустить ряд высокотехнических, но увлекательных файлов в наступающем году… СЛЕДИ ЗА НИМИ!! Завтра я отправляюсь на Xmascon '91… мы сделали несколько отличных кнопок в честь этого события… если ты когда-нибудь увидишь одну из них (зелёный венок, надпись XMASCON

1991 на ней)… береги её! Это коллекционный предмет… (хахахах)
Парень, я хочу спать…

Помни: «Правда дёшева, но информация стоит денег!»

Но -=RDT это изменит… ;) Освободи информацию!

Мир.

..oooOO Count Zero OOooo..

Обычные приветствия Magic Man, Brian Oblivion, Omega, White Knight и всем, у кого я когда-либо стрелял сигарету.

(Добавление от 1/18/92: Привет всем, кого встретил на Xmascon… включая, но не ограничиваясь: Crimson Death, Dispater, Sterling, Mack Hammer, Erik Bloodaxe, Holistic Hacker, Pain Hertz, Swamp Ratte, G.A.Ellsworth, Phaedrus, Moebius, Lord MacDuff, Judge Dredd, и конечно снимаю шляпу перед Drunkfux *за организацию и принятие на себя ответственности за всё это дело. Надеюсь увидеть вас всех на SummerCon '92! Ищи Cyber-striper GIF'ы на BBS рядом с тобой… хе-хе)*

Комментарии, критика и обсуждения этого файла приветствуются. Со мной можно связаться по адресам:

• count0@world.std.com
• count0@spica.bu.edu
• count0@atdt.org

Magic Man и я являемся сисопами BBS «ATDT»… расположенной где-то в Массачусетсе. Отличные форумы, технические дискуссии… данные, ставшие плотью… электронное подполье… собственный интернет-адрес (atdt.org)… вылазки в тоннели под MIT в Кембридже… звони… пиши мне за подробностями.. ;)

Руководство пользователя VAX/VMS. Часть II из III

Автор: Black Kat

```
<:===:><:=--=:><:=--=:><:===:>\|/<:===:><:=--=:><:=--=:><:===:>
<:===:>                                                     <:===:>
<:===:>    >>>>>=-*  Users Guide to VAX/VMS  *-=<<<<<     <:===:>
<:===:>                                                     <:===:>
<:===:>                   Part II of III                    <:===:>
<:===:>                                                     <:===:>
<:===:>            Part C: Using the Utilities              <:===:>
<:===:>         Part D: Advanced Guide to VAX/VMS           <:===:>
<:===:>                                                     <:===:>
<:===:>                    By Black Kat                     <:===:>
<:===:>                                                     <:===:>
<:===:><:=--=:><:=--=:><:===:>/|\<:===:><:=--=:><:=--=:><:===:>
```

Содержание

Часть C охватывает следующие темы:

• Утилита Help - Утилита Phone
• Утилита Backup - Утилита Library
• Утилита Mail - Утилита Sort

Часть D охватывает следующие темы:

• Подпроцессы - DECnet
• Подключение к процессу - Proxy Access (прокси-доступ)
• Прерывание процесса - Межзадачное взаимодействие
• Пакетная обработка - Удалённая печать
• Управление пакетными заданиями - VAXclusters

Часть C: Использование утилит

Утилита Help

Утилита VAX/VMS Help — это что-то вроде онлайн-словаря DCL-команд. Она содержит описание каждой DCL-команды и может дополнительно пояснить допустимые параметры. Help также предоставляет сведения о других утилитах VAX/VMS и системных сервисах.

Утилита Help поддерживает два режима работы. Если вы знаете нужную DCL-команду, утилиту или системный сервис, используйте прямой режим. Если нет — используйте режим запроса. Режим запроса также позволяет просмотреть, какие команды и темы доступны в справочной системе.

Чтобы войти в режим запроса, просто введите `HELP` на уровне DCL-командной строки. Help выведет алфавитный список всех DCL-команд и тем, по которым доступна информация, и выдаст приглашение: "`Topic?`"

Выйти из Help можно нажатием `, или , либо получить информацию, введя название команды или темы и нажав . При запросе информации по команде Help отобразит подробности: как вызвать команду, что она делает и значения по умолчанию. У большинства тем есть подтемы — они будут перечислены в алфавитном порядке, после чего появится приглашение: "COMMAND-NAME Subtopic?"`

Можно выбрать подтему или нажать ` для возврата к приглашению "Topic?". Чтобы получить всю доступную информацию по команде, введите "HELP command_name ..." или "HELP command_name *"`.

Для прямого режима введите `HELP topic_name` . Это позволит обойти вывод списка тем. В этом режиме также можно вводить допустимые DCL-команды с квалификаторами или без. Например, чтобы получить сведения о квалификаторе `/TERMINAL` команды DCL SET, введите:

```
$ HELP SET TERMINAL
```

Утилита Help предоставит информацию о команде `SET/TERMINAL` и предложит ввести подтему, так как доступны сведения и о других квалификаторах.

Для получения дополнительных сведений об утилите Help используйте:

```
$ HELP HINTS   или   $ HELP HELP/INSTRUCTIONS
```

Утилита Backup

Утилита Backup обычно применяется системными администраторами для резервного копирования системных дисков — чтобы при ненадёжности системных дисков иметь свежую копию данных. Как правило, системные диски копируются на магнитную ленту или съёмные дисковые пакеты, которые затем извлекаются и хранятся в надёжном месте в отключённом от сети состоянии. Пользователи могут применять утилиту Backup для файлов в своих собственных учётных записях — для создания резервных копий, переноса на другую систему или автономного хранения.

Прежде чем использовать утилиту Backup, нужно определить, что именно нужно скопировать и каким способом. Доступны следующие варианты:

Выборочное копирование (Selective): Файлы копируются согласно заданному критерию. Для указания критериев используются квалификаторы (например, `/DATE`) и спецификации файлов (например, `*.TXT`).

Побайловое (File by File): Отдельные файлы или целые каталоги. При копировании каталоги создаются автоматически — в отличие от команды COPY.

Инкрементное (Incremental): Сохраняются файлы, созданные после последнего резервного копирования. Обычно выполняется операторами системы.

Физическое (Physical): Создаётся точная копия тома. Все файловые структуры игнорируются, копия является побитовым дубликатом.

Образное (Image): Создаётся функционально эквивалентная копия исходного тома. Обычно применяется для загрузочных томов и системных дисков.

Резервное копирование файлов в подкаталог:

```
$ BACKUP F1.TXT,F2.TXT,*.DAT [BY.JUNK]
```

Копирование дерева каталогов:

```
$ BACKUP [dir...]file_spec [dir...]file_spec
```

Копирование дисковых томов:

```
$ MOUNT/FOREIGN DJA1:
$ BACKUP/IMAGE DUA2: DUA1:
```

Копирование на ленту:

```
$ INITIALIXE MUA0: TAPE  (при первом использовании)
$ MOUNT/FOREIGH MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP [.DRV]MV_DYDRV.MAR MUA0:[]MV_DYDRV.MAR
```

Резервный набор (save set) — это единый файл, содержащий несколько скопированных файлов. Создание резервного набора:

```
$ MOUNT/FOREIGN MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP DUB1:[BY.JUNK]*.*;* MUA0:08JUN.BAK/SAVE_SET
```

Отдельный файл можно извлечь из резервного набора с помощью квалификатора `/SELECT`. Например, чтобы восстановить файл `LOGIN.COM` из ранее созданного резервного набора:

```
$ MOUNT/FOREIGH MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP
__From: MUA0:08:JUN.BAK/SAVE_SET/SELECT=[BY.JUNK]LOGIN.COM
__To: *.*
```

Просмотр содержимого резервного набора:

```
$ MOUNT/FOREIGN MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP/LIST MUA0:08JUN.BAK/SAVE_SET
```

Выборочное резервное копирование:

```
$ BACKUP *.*/SINCE=12-APR-1988 MUA0:08JUN.BAK/SAVE_SET
$ BACKUP
__From: *.*/SINCE=12-APR-1988/EXCLUDE=[*.TMP,*.LOG]
__To: MUA0:08JUN.BAK/SAVE_SET
```

Ниже приведены некоторые полезные квалификаторы:

Квалификатор	Функция
/LOG	Записывает сообщение в терминал при обработке каждого файла.
/VERIFY	Проверяет соответствие копии или резервного набора оригиналу после копирования.
/CONFIRM	Показывает имя каждого файла и запрашивает подтверждение перед копированием.
/DELETE	Удаляет исходный файл после записи целевого.

Утилита Mail

Когда вы получаете новое письмо, на ваш терминал будет выведено сообщение — если только для команды SET TERMINAL не задан квалификатор /NOBROADCAST. Mail — это интерактивная утилита, поддерживающая множество команд в формате, идентичном DCL-командам. Утилита вызывается командой $ MAIL на уровне DCL. В Mail есть встроенная справка, работающая так же, как утилита Help в VAX/VMS. Письма можно отправлять в интерактивном или прямом режиме.

Интерактивный режим подразумевает работу с Mail в диалоговом режиме: вызовите утилиту из DCL-командной строки, введите команду SEND, после чего Mail запросит имя получателя (или получателей), ваше имя, тему и текст сообщения, который завершается нажатием `. После нажатия сообщение отправляется, и вы возвращаетесь в приглашение Mail, где можно ввести EXIT` для выхода.

Чтобы отправить письмо в прямом режиме из командной строки DCL, используйте следующий формат:

```
$ MAIL file_spec user /SUBJECT="character string"
```

где file_spec — допустимая спецификация файла VAX/VMS, содержащего тело письма, а user — имя пользователя на вашей локальной системе или удалённом узле. Квалификатор /SUBJECT необязателен.

Для отправки письма нескольким пользователям (по списку рассылки) создайте файл, содержащий имена учётных записей всех адресатов. Затем в приглашении "To:" введите @FILENAME — каждый пользователь из списка получит копию письма. Список рассылки может включать другой список — для этого перед его именем нужно поставить знак «at» (@). Комментарии добавляются с помощью восклицательного знака (!). Пример списка рассылки:

```
! VAX.DIS
!
! Staff
JONES
OPER
BYNON
!
! Accounting personnel
@ACTLIST
```

Чтобы прочитать почту, введите MAIL — система сообщит, сколько сообщений ожидает. Команда READ является командой по умолчанию, поэтому можно просто нажать ` для начала чтения. Чтобы ответить на письмо, используйте команды REPLY или ANSWER — Mail автоматически заполнит заголовок. Письма можно хранить в папках для последующего обращения. В системе есть три стандартные папки: MAIL, NEWMAIL и WASTEBASKET`.

MAIL — папка по умолчанию, существует всегда. В ней хранятся прочитанные письма, если вы не переместили их в другие папки.

NEWMAIL — папка для непрочитанных сообщений, аналог почтового ящика. После прочтения письма автоматически перемещаются в папку MAIL, если командой MOVE не задана иная папка назначения.

WASTEBASKET — временная папка для удалённых сообщений. Они хранятся здесь до выхода из утилиты, после чего удаляются безвозвратно.

Чтобы создать новую папку, выберите сообщение и введите команду MOVE. Если указанная папка не существует, система спросит, хотите ли вы её создать. Например:

```
MAIL> 11
MAIL> MOVE MEMOS
Folder MEMOS does not exist. Create it (Y/N, default is N)? Y
MAIL-NEWFOLDER, folder MEMOS created MAIL>
```

Команда SELECT позволяет переключаться между папками. Например, если ввести SELECT JUNK в приглашении "MAIL>", вы перейдёте в папку JUNK, и Mail выдаст количество сообщений в ней.

Команда DELETE принимает номер сообщения в качестве параметра или удаляет текущее сообщение, если номер не указан. Чтобы удалить папку, нужно удалить все сообщения в ней с помощью квалификатора /ALL.

Чтобы сохранить сообщение в файл, используйте команду EXTRACT. Если задан квалификатор /NOHEADER, заголовок включён не будет. Например, EXTRACT/NOHEADER MEMO.TXT сохранит текущее выбранное сообщение в файл MEMO.TXT.

Для получения дополнительных сведений об утилите Mail используйте её команду HELP.

Утилита Phone

Утилита VAX/VMS Phone позволяет общаться с другими пользователями системы. Она имитирует настоящий телефон: удержание вызова, конференц-связь, телефонный справочник. Утилита Phone работает только с терминалами VT100, VT200 или совместимыми.

Чтобы позвонить кому-либо, введите $ PHONE username, где username — имя нужного пользователя. Экран разделится горизонтально пополам: в верхней части будет отображаться ваша часть разговора, в нижней — ответы собеседника. При этом система сообщит, что вызов поступил другому пользователю.

Утилиту Phone можно также использовать в интерактивном режиме, введя $ PHONE. Вы перейдёте к приглашению Phone (%) и сможете вводить команды напрямую (например, % DIRECTORY). Утилита Phone имеет встроенную справку, аналогичную справке утилиты Mail.

Утилита Library

Иногда проще работать с одним файлом, чем с группой связанных файлов. Утилита VAX/VMS Library позволяет создавать и обслуживать специально форматированный файл — библиотеку, в которой хранятся группы отдельных файлов, называемых модулями. Предопределённые типы библиотек: текстовые, справочные, объектные, разделяемых образов и макро. Многие утилиты VAX/VMS, такие как HELP и LINK, умеют работать с файлами библиотек. Если вы не программист и не системный администратор, скорее всего, вам понадобятся только текстовые и справочные библиотеки.

Для создания библиотеки используйте команду LIBRARY с квалификатором типа и квалификатором /CREATE. Квалификаторы типа: /TEXT, /SHARE, /HELP, /OBJECT, /MACRO. Например, чтобы создать текстовую библиотеку BOOK.TLB:

```
$ LIBRARY/TEXT/CREATE BOOK.
```

При создании библиотеки можно сразу указать список файлов, которые будут в неё включены. Например:

```
$ LIBRARY/TEXT/CREATE BOOK TOC,C1,C2,INDEX
```

Чтобы вывести список модулей в библиотеке, используйте квалификатор /LIST:

```
$ LIBRARY/TEXT/LIST BOOK
Directory of TEXT library BOOK.TLB;1 on 12-JUN-1989 14:12:07
```

```
TOC
C1
C2
INDEX
```

С помощью квалификатора `/HISTORY` совместно с `/LIST` можно отобразить историю изменений библиотеки.

Чтобы добавить модули в существующую библиотеку, используйте квалификатор `/INSERT`:

```
$ LIBRARY/TEXT/INSERT BOOK CH3
```

Чтобы обновить модуль в библиотеке, выполните следующие шаги:

• Извлеките модуль с помощью квалификатора `/EXTRACT`.
• Внесите необходимые изменения.
• Перезапишите старый модуль с помощью квалификатора `/REPLACE`.

Например:

```
$ LIBRARY/TEXT/EXTRACT BOOK CH2
$ EDIT CHAP2.TXT
  .
  .    (редактирование файла)
  .
$ LIBRARY/TEXT/REPLACE BOOK CH2
```

Утилита Sort

Утилита VAX/VMS Sort реорганизует записи в файле. Простейшая форма команды сортирует записи в порядке возрастания алфавита. Например, для сортировки файла `BOOK.TXT`:

```
$ SORT BOOK.TXT SORTED.TXT
```

Утилита Sort сортирует по первому символу поля в каждой записи входного файла. Если в записи несколько полей или столбцов, упорядочивается вся запись целиком, а не только первое поле.

Пример сортировки по убыванию числового значения с несколькими полями. Файл `JUNK.TXT` содержит два поля: первое — имя, второе — двузначное число, начинающееся с 9-й позиции, по которому и ведётся сортировка:

```
PAT     47
PAT     47
JIM     09
TOM     23
RICH    43
GARY    02
KURT    13
KEVIN   27
```

Команда сортировки:

```
$ SORT/KEY=(POSITION=9,SIZE=2,DESCENDING) JUNK.TXT SORTED.TXT
```

Отсортированный файл `SORTED.TXT` будет выглядеть так:

```
PAT     47
RICH    43
KEVIN   27
TOM     23
KURT    13
JIM     09
GARY    02
```

Часть D: Продвинутое руководство по VAX/VMS

Подпроцессы

Одним из главных преимуществ операционной системы VAX/VMS является поддержка многозадачности. Это не ограничивается лишь несколькими пользователями, подключёнными к разным терминалам. Пользователи VAX/VMS могут создавать несколько процессов, называемых подпроцессами, в рамках своего основного процесса.

Для создания подпроцесса используется DCL-команда `SPAWN`. Если не указано иное, подпроцесс наследует атрибуты родительского процесса: рабочий каталог по умолчанию, привилегии, память и т.д. Например:

```
$ SPAWN
% DCL-S-SPAWNED, process BYNON_1 spawned
% DCL-S-ATTACHED, terminal now attached to process BYNON_1
```

В данном случае родительский процесс переходит в состояние ожидания, подпроцесс получает управление клавиатурой, и вы оказываетесь в DCL-приглашении. Теперь можно вводить любые DCL-команды, запускать утилиты и другие программы. Чтобы вернуться к родительскому процессу, достаточно выполнить `$ LOGOUT` из подпроцесса:

```
$ LOGOUT
  Process BYNON_1 logged out at 12-JUL-1981 13:04:17.10
$ DCL-S-RETURNED, control returned to process BYNON
```

Квалификатор `/NOLOG` команды `SPAWN` подавляет информационные сообщения, выводимые при создании подпроцесса или его выходе. DCL-команды, процедуры и образы VAX/VMS (утилиты и программы) можно выполнять напрямую через `SPAWN`, указав нужный синтаксис после команды `SPAWN`. Например:

```
$ SPAWN/NOLOG MAIL
```

Если задача не требует вмешательства пользователя (например, компилятор программы), её можно запустить как фоновый процесс по отношению к текущему. Например:

```
$ SPAWN/NOWAIT FORTRAN VAXBBS
```

Квалификатор `/NOWAIT` запускает задачу параллельно родительскому процессу. Оба процесса будут совместно использовать терминал, и сообщения от фонового задания будут на нём отображаться. Чтобы избежать возможных конфликтов, используйте квалификатор `/OUTPUT`:

```
$ SPAWN/NOWAIT/OUTPUT=COMPILE.LOG FORTRAN.VAXBBS
```

По завершении задачи подпроцесс прекращает работу и удаляется из системы.

Подключение к процессу (ATTACH)

Команда DCL `ATTACH` позволяет подключить клавиатуру к любому созданному вами процессу или подпроцессу. Чтобы вернуться из `BYNON_1` к `BYNON` с помощью команды `ATTACH`, введите `$ ATTACH BYNON` — подпроцесс перейдёт в режим ожидания, а вы вернётесь к родительскому

процессу.

Прерывание процесса

Вы можете прервать любой процесс в любой момент, нажав `, а затем используя команду SPAWN для создания подпроцесса. Завершив работу с подпроцессом и вернувшись к прерванному процессу, введите CONTINUE, чтобы продолжить выполнение с того места, где оно было прервано. Некоторые утилиты VAX/VMS, например Mail, поддерживают SPAWN внутренне, поэтому в них можно порождать подпроцесс, вводя команду SPAWN без предварительного нажатия `.

Пакетная обработка

Команда SUBMIT кратко рассматривалась в Части II: Программирование на VAX. Пакетное задание — это одна или несколько DCL-командных процедур, выполняемых из отдельного процесса с вашими привилегиями и квотами. Контроллером процесса является очередь пакетных заданий, которая принимает задания через команду SUBMIT. Пакетные задания выполняются без участия пользователя, что позволяет работать за терминалом в интерактивном режиме, пока система выполняет пакетное задание (командную процедуру). Пакетные задания используются для задач, требующих длительного времени выполнения, больших системных ресурсов или запуска в определённое время.

Команда SUBMIT помещает командную процедуру в очередь пакетных заданий по умолчанию (SYS$BATCH), если конкретная очередь не задана. Поданному на пакетное выполнение заданию присваивается имя, которое по умолчанию соответствует имени командной процедуры. Присвоенный номер записи используется для управления заданием (удаление, переименование и т.д.).

Управление пакетными заданиями

Задать имя пакетного задания с помощью квалификатора /NAME:

```
$ SUBMIT BACKUP /NAME=DAILY_BACK
```

Выполнить несколько командных процедур, разделив их имена запятой:

```
$ SUMBIT SORT_DATA,REPORT /NAME=WEEKLY_REPORT
```

Запланировать пакетное задание на определённое время:

```
$ SUMBIT CLEANUP /AFTER=11:40
Job CLEANUP (queue SYS$BATCH, entry 39) holding until 1-JUN-1989 11:40
```

Задержать задание в очереди для последующего запуска:

```
$ SUMBIT REMINDER /HOLD
Job REMINDER (queue SYS$BATCH, entry 12) holding
$
$ SET QUEUE/ENTRY=32/RELEASE SYS$BATCH
```

Отправить задание в другую очередь:

```
$ SUBMIT TESTJOB /QUEUE=SLOW
```

Снизить приоритет (например, для интенсивных задач по использованию ЦПУ):

```
$ SUBMIT CRUNCH /PRIORITY=2
```

Передать параметры:

```
$ SUBMIT COMPILE / PARAMETERS=(WINDOWS,MISC,DISP_IO)
```

Отключить автоматическую печать журнала пакетного задания (сохранить в файл):

```
$ SUBMIT GOJOB /NOPRINT /LOG_FILE=DUA2:[BYNON]
```

Это создаст файл `DUA2:[BYNON]GOJOB.LOG`. Если квалификатор `/NOPRINT` не указан, журнал будет распечатан и удалён. Чтобы распечатать и сохранить журнал, используйте квалификатор `/KEEP` совместно с `/LOG_FILE`.

После постановки процедуры в очередь пакетных заданий можно следить за её состоянием и характеристиками с помощью команды `SHOW QUEUE`. Она отображает имя, номер записи и статус всех заданий в очереди. Квалификатор `/ALL` показывает все задания, доступные вам по привилегиям, а квалификатор `/FULL` предоставляет расширенную информацию: рабочие характеристики, время постановки в очередь и т.д.

Для изменения приоритета задания (`/PRIORITY`), имени (`/NAME`) или статуса (`/RELEASE` или `/AFTER`) используйте команду `SET QUEUE/ENTRY`. Например:

```
$ SET QUEUE /ENTRY=217 /PRIORITY=2 SYS$BATCH
```

Для удаления заданий используйте команду `DELETE /ENTRY`:

```
$ DELETE /ENTRY=18 SYS$BATCH
```

Использование DECnet

DECnet использует стандартные спецификации файлов VAX/VMS для удалённого доступа к файлам. Помимо указания узла, можно включить в команду информацию управления доступом (имя пользователя и пароль) в кавычках. Например:

```
BURG"JONES MYPW"::DUA2:JUNK.TXT
 |     |    |       |     |
 |     |    |       |     +---- Имя файла.Расширение
 |     |    |       |
 |     |    |       +---------- Имя устройства
 |     |    |
 |     |    +------------------ Пароль
 |     |
 |     +----------------------- Имя пользователя
 |
 +------------------------------ Имя узла
```

Если на узле-получателе нет специальной учётной записи DECnet или прокси-доступа, для выполнения команды на удалённой системе необходимо указать информацию управления доступом (например: `$ TYPE BURG"JONES MYPW"::DUA2:JUNK.TXT`).

Прокси-доступ (Proxy Access)

Поскольку указание информации управления доступом в командной строке является угрозой безопасности, Digital предоставляет механизм прокси-доступа, работающий на основе базы данных пользователей и узлов, которым разрешён доступ к системе через DECnet. Формат базы данных: `SYSTEM::REMOTE_USERNAME LOCAL_USERNAME`.

Межзадачное взаимодействие (Task-to-Task Communication)

Это функция DECnet, позволяющая программам на одной системе взаимодействовать с программами на другой (например, команда DCL `TYPE`). Для выполнения процедуры на удалённой системе используйте команду `TYPE` с параметром `TASK=xxx`. Например:

```
$ TYPE VAX1::"TASK=SHOW_USERS"
```

Чтобы отобразить пользователей удалённой системы, можно написать командную процедуру примерно следующего содержания:

```
$! Show_Users.Com
$!
$       IF FMODE() .EQS. "NETWORK" THEN GOTO NETWORK
$       SHOW USERS
$       EXIT
$  NETWORK:
$       DEFINE/USER_MODE SYS$OUTPUT SYS$NET
$       SHOW USERS
$       EXIT
```

Поскольку `SYS$OUTPUT` перенаправлен в `SYS$NET`, вывод передаётся на ваш терминал через DECnet. Межзадачное взаимодействие может быть простым (как `Show_Users`) или сложным (как программы, обменивающиеся данными).

Удалённая печать

Если ваша сеть DECnet содержит LAN-сегмент, например Ethernet, вам, скорее всего, придётся совместно использовать принтеры с другими узлами сети. Проще всего распечатать файл, скопировав его непосредственно на устройство печати. Это работает, пока устройство имеет спулинг и настроено с правом записи для всех. Например:

```
$ COPY JUNK.TXT BURG::LCA0:
```

Эта команда скопирует файл `JUNK.TXT` на устройство `LCA0:` узла `BURG`.

Другой способ — использовать команду DCL `PRINT/REMOTE`. Однако файл должен находиться на удалённой системе, что неудобно, если он хранится локально. Тем не менее это возможно:

```
$ COPY JUNK.TXT BURG::[BYNON]
$ PRINT /REMOTE BURG::[BYNON]JUNK.TXT
   Job JUNK (queue SYS$PRINT, entry 512) started on LCA0
$ DELETE BURG::[BYNON]JUNK.TXT
```

VAXclusters

Основное назначение VAXcluster — высокая производительность вычислений, совместное использование ресурсов и единая среда безопасности и управления. Существует два основных типа VAXcluster: гомогенный и гетерогенный, хотя возможно и их сочетание. Ключевое различие — в том, как они совместно используют ресурсы, прежде всего среду VAX/VMS OS.

В гомогенном VAXcluster среда VAX/VMS OS идентична на каждом узле кластера. Это достигается использованием общего системного диска для всех узлов. Учётные записи пользователей, системные файлы, очереди и устройства хранения являются общими, и все компьютеры ведут себя одинаково.

В гетерогенном VAXcluster среда на каждой системе различна. Каждый VAX имеет собственный системный диск, учётные записи пользователей и системные файлы. Очереди и устройства хранения могут использоваться совместно, а могут и нет. Пользователи могут работать в разных операционных средах в зависимости от того, к какой системе подключены.

Как правило, доступ к VAXcluster осуществляется через терминальный сервер на базе Ethernet. С его помощью пользователь может установить сеанс с любым членом VAXcluster, причём соединение ничем не отличается от соединения с напрямую подключённым терминалом. При этом терминальные сеансы поддерживают одновременное подключение к нескольким узлам. В маловероятном случае, когда VAXcluster настроен с прямым подключением терминалов и вам нужно получить доступ к другой системе, можно воспользоваться DECnet через средство `SET HOST`. Все системы VAXcluster поддерживают DECnet внутри кластера.

Узлы (члены) VAXcluster нередко совместно используют вычислительные ресурсы через кластерные очереди печати и пакетных заданий, называемые кластерными очередями (cluster-wide queues). Они работают так же, как обычные очереди. Единственное дополнение — необходимость знать имя очереди. Список всех очередей кластера можно вывести командой DCL `SHOW QUEUE`. При отправке задания в кластерную очередь необходимо убедиться, что узел, на котором она находится, имеет доступ к нужному файлу для печати или командной процедуре для обработки.

Основные команды системы VOS

```
##############################
#*#     Basic Commands     #*#
#*#      for the VOS       #*#
#*#         System         #*#
##############################
```

Автор: Dr. No-Good [Echo]

Введение

Это простой текстовый файл, объясняющий основные команды системы VOS. VOS расшифровывается как Virtual Operating System (Виртуальная операционная система) и используется преимущественно в корпоративной среде, хотя ею пользуются и другие группы.

Если у вас возникнут вопросы, со мной можно связаться на этой системе:

```
Legion (202)337=2844
```

Или написать по электронной почте:

```
Internet:  ukelele!kclahan@UUNET.UU.NET
```

Особая благодарность: Nat X, Beta Raider, Tomellicus и анонимному сайту, приютившему мои скромные труды.

> ***Примечание.*** *Все материалы в этом файле предназначены исключительно в информационных целях. Любое злоупотребление данной информацией, по всей видимости, является противозаконным; авторы этого текстового файла не несут ответственности за действия читателя.*

Системы VOS встречаются в самых разных местах по всему миру, а также во многих сетях — например, TELENET. Систему VOS можно распознать по её приглашению, которое выглядит так:

```
Prompt->     (Name of System)
             System ???, VOS Release v.(version), Module ???

             (Or it just says something about a Release ver# and Module#)
```

После получения приветственного сообщения начинается самое сложное — подбор правильной комбинации имени пользователя и пароля. Для входа в систему наберите:

```
Login <name> <password> <CRT>
```

или

```
Login <CRT>
'User_name:' <name>
'Password?' <password>
```

(Здесь `` означает нажатие Enter — оно ставится после того, что нужно ввести; слова в одинарных кавычках выводит сам компьютер.)

При успешном вводе имени и пароля система ответит:

```
<name> logged in on <module#> at <year>-<month>-<day> at <time> ETA.
```

(после чего запускается start_up.cm)

Команды

```
HELP                       =  Открыть встроенный справочник.

LIST или LS                =  Вывести содержимое каталога.
          -dirs            =      только подкаталоги.
          -dirs <dir>      =  Проверить существование каталога.

CHANGE_CURRENT_DIR или CCD =  Сменить текущий каталог.

DISPLAY <file>             =  Просмотреть содержимое файла.
          -match <string>  =  Найти строку в файле.

SEND_MESSAGE <name> <msg>  =  Отправить сообщение на экран указанного
                               пользователя. Длина — не более 80 символов.

CALL_THRU                  =  Подключить свой терминал к удалённому
                               хосту в качестве терминала входа или
                               подчинённого устройства.

SET_TERMINAL_PARAMETERS    =  Задать параметры работы терминала:
                               прокрутку, длину экрана и т. д.

LOCATE_FILES <file names>  =  Найти расположение файла (файлов) в системе.

WHO                        =  Вывести список текущих пользователей системы.

LIST_MODULES               =  Показать, какие модули запущены.

DISPLAY_DIR_STATUS         =  Показать информацию о каталоге: дату
                               последнего сохранения, дату создания,
                               имя создателя, дату последнего
                               использования или изменения.

DISPLAY_CURRENT_DIR        =  Показать текущий каталог.

DISPLAY_ACCESS_LIST        =  Вывести списки управления доступом (ACL)
                               для указанных файлов или каталогов.

DISPLAY_DEFAULT_ACCESS     =  Вывести список управления доступом
                               по умолчанию для указанных каталогов.

GIVE_ACCESS                =  Предоставить пользователю или группе
                               доступ к файлу или каталогу.

GIVE_DEFAULT_ACCESS        =  Добавить записи в ACL по умолчанию
                               для каталога или набора каталогов.

PROPAGATE_ACCESS           =  Скопировать права доступа каталога
                               на все каталоги в его подиерархии.

REMOVE_ACCESS              =  Удалить записи из ACL файла, каталога
                               или набора таких объектов.

REMOVE_DEFAULT_ACCESS      =  Удалить записи из ACL по умолчанию
                               каталога или набора каталогов.

EDIT                       =  Редактировать или создать файл.
                               (Разобраться с этим пока не удалось.)

BIND                       =  Преобразовать .OBJ-файл в .PM-файл,
                               пригодный для запуска.

ANY_NAME.PM                =  .PM — программный модуль; аналог
                               исполняемых файлов .COM или .EXE.
BATCH                      =  Запустить пакет команд .PM.
```

```
UPDATE_BATCH_REQUESTS     =  Обновить очередь пакетных заданий.

CANCEL_BATCH_REQUESTS     =  Полностью отменить все программы
                              в очереди пакетных заданий.

LIST_BATCH_REQUESTS       =  Вывести список программ в очереди
                              пакетных заданий.

RESERVE_DEVICE            =  Зарезервировать устройство для очереди
                              пакетных заданий.
                              (Используется администраторами при
                               управлении пакетной обработкой.)

CANCEL_DEVICE_RESERVATION =  Отменить резервирование устройства.

MOVE_DEVICE_RESERVATION   =  Переместить резервирование устройства
                              на другой путь.

DISPLAY_BATCH_STATUS      =  Показать статус пакетного процесса.

COMPARE_FILE              =  Сравнить два файла между собой.

COPY_FILE                 =  Скопировать файл в другой файл
                              или каталог.

LOCATE_FILE               =  Найти каталог, в котором находится файл.

RENAME                    =  Переименовать файл.

MOVE_FILE                 =  Переместить файл в другой каталог.

DELETE_FILE               =  Удалить файл.

SET_EXPIRATION_DATE       =  Установить дату, до наступления которой
                              файл не может быть удалён.

CREATE_FILE               =  Создать и именовать новый файл.

CREATE_INDEX              =  Создать новый индекс для файла.

CREATE_DELETED_RECORD_INDEX = Создать список повторно используемых
                              позиций в файле.

CREATE_RECORD_INDEX       =  Создать индекс для отображения записей
                              в файле и повторного использования
                              пространства, освобождённого удалениями.
                              (После создания обновляется постоянно.)

DELETE_INDEX              =  Удалить набор индексов файла.

DISPLAY_FILE_STATUS       =  Показать сведения об указанных файлах.

DUMP_FILE                 =  Вывести содержимое файла в шестнадцатеричном
                              и ASCII-форматах для отладки.

DUMP_RECORDS              =  Вывести одну или несколько записей
                              из фиксированного, последовательного,
                              относительного или потокового файла.

ENFORCE_REGION_LOCKING    =  Включить/выключить обязательную блокировку
                              регионов для одного или нескольких
                              потоковых файлов.

SET_FILE_ALLOCATION       =  Задать количество дополнительных дисковых
                              блоков, выделяемых операционной системой
                              файлу при каждом расширении.

SET_IMPLICIT_LOCKING      =  Включить/выключить неявную блокировку
                              для файла или файлов. При включённом режиме
                              система отклоняет попытку открыть файл
                              с иной спецификацией блокировки.
```

Уровень	Описание
NULL	Никаких действий с файлом невозможно.
READ	Файл можно читать, но не изменять.
WRITE	Есть права чтения и записи: файл можно изменять.
EXECUTE	Файл можно читать и запускать на исполнение.

Уровень	Описание
NULL	Никаких действий с файлом невозможно.
READ	Файл можно читать, но не изменять.
WRITE	Есть права чтения и записи: файл можно изменять.
EXECUTE	Файл можно читать и запускать на исполнение.

> ***Примечание.*** *Если вам нужна дополнительная справка по командам, воспользуйтесь встроенной справочной системой: наберите* `HELP` *после входа в систему или* `HELP .` *Извините за формат листинга команд; если вам нужен более удобный список, ищите полное информационное руководство по системам VOS от Dr. No-Good.*

Безопасность

Базовая система безопасности VOS основана на ACL (Access Control Lists — списках управления доступом). Это списки, которые создатель каталога или файла формирует с помощью команды `GIVE_ACCESS`. Существует четыре вида прав доступа.

Для файлов:

Уровень	Описание
NULL	Никаких действий с файлом невозможно.
READ	Файл можно читать, но не изменять.
WRITE	Есть права чтения и записи: файл можно изменять.
EXECUTE	Файл можно читать и запускать на исполнение.

Для каталогов:

NULL	Никаких действий с файлом невозможно.

READ	Файл можно читать, но не изменять.
WRITE	Есть права чтения и записи: файл можно изменять.
EXECUTE	Файл можно читать и запускать на исполнение.

Если у вас нет соответствующих прав на каталог или файл, это означает, что владелец или создатель файла либо каталога не внёс вас в список доступа. Поскольку данный информационный файл не содержит сведений, необходимых для получения доступа к файлам, доступ к которым вам не предоставлен, рекомендуется искать дополнительные информационные файлы от [ECHO].

Дело CompuServe: шаг вперёд в защите онлайн-сервисов по Первой поправке

Представлено: Electronic Frontier Foundation

Введение

Автор: Mike Godwin (mnemonic@eff.org), EFFector Online 3.03

К этому времени вы, возможно, уже слышали о решении о суммарном судопроизводстве по делу Cubby, Inc. против CompuServe — делу о клевете. Однако вы, возможно, не знаете, почему это решение столь важно. Признав, что CompuServe не должна нести ответственность за диффамацию, размещённую сторонним пользователем, суд в данном деле верно проанализировал потребности большинства онлайн-сервисов в контексте Первой поправки. И поскольку это первое решение, напрямую затрагивающее данные вопросы, оно может стать образцом для будущих решений в других судах.

Полное наименование дела, рассмотренного в Южном округе Нью-Йорка, — Cubby Inc. против CompuServe. По существу, CompuServe заключила договор со сторонней организацией на ведение специализированного форума в системе CompuServe. Истец утверждал, что в этом форуме пользователем были размещены клеветнические материалы о его бизнесе, и предъявил иск как к организатору форума, так и к CompuServe. CompuServe подала ходатайство о суммарном решении в свою пользу и его получила.

Судья Лежер в своём решении пришёл к выводу, что CompuServe ближе не к издателю, а к владельцу книжного магазина или дистрибьютору книг. Законодательство в рамках Первой поправки допускает привлечение издателей к ответственности за диффамацию, тогда как владельцев книжных магазинов — нет, поскольку возложение такой ответственности на последних создало бы обязанность проверять каждую книгу на предмет клеветнического содержания. Это бремя «заморозило» бы распространение книг (не говоря уже о том, что некоторые люди ушли бы из книжного бизнеса) и тем самым вступило бы в серьёзное противоречие с Первой поправкой.

Итак, хотя мы нередко говорим о BBS как об обладателях прав издателей и изданий, данное дело обнажает важное различие. Чем издатель отличается от владельца книжного магазина? Тем, что мы ожидаем от издателя (или его агентов) рецензирования всего материала до публикации. Но мы *не* ожидаем от владельцев книжных магазинов проверки всего до продажи. Точно так же в деле CompuServe, как и в любом деле с онлайн-сервисом, где пользователи свободно размещают сообщения для широкой аудитории (это не относится к Prodigy), мы не стали бы ожидать от провайдера онлайн-коммуникаций прочтения всего публикуемого *до* того, как это появится в сети.

Стоит отметить, что прецедент Верховного суда, на который опирается судья Лежер, — это дело Смит против Калифорнии, касающееся непристойности, а не диффамации. Смит — это дело Верховного суда, в котором впервые возникает тезис о том, что привлечение владельцев книжных магазинов к ответственности за содержимое в целом неконституционно. Таким образом, если дело Смит против Калифорнии применимо в делах о диффамации в онлайн-сервисах или на BBS, оно безусловно должно применяться и в делах о непристойности.

Таким образом, дело Cubby, Inc. против CompuServe проливает свет не только на законодательство о диффамации в применении к новым медиа, но и на законодательство о непристойности. Это решение должно многое прояснить обеспокоенным системным операторам

относительно их обязательств и ответственности по закону.

Ключевые положения решения по делу CompuServe

Автор: Danny Weitzner (djw@eff.org), EFFector Online 3.03

«Продукт CompuServe CIS [CS Information Service] представляет собой по существу электронную коммерческую библиотеку, располагающую огромным количеством изданий и взимающую с подписчиков абонентскую плату и плату за использование в обмен на доступ к этим изданиям. CompuServe и подобные ей компании находятся на переднем крае революции в информационной индустрии. Высокие технологии существенно ускорили сбор и обработку информации; теперь физическое лицо, имеющее персональный компьютер, модем и телефонную линию, может получить мгновенный доступ к тысячам новостных изданий по всей территории Соединённых Штатов и по всему миру. Хотя CompuServe вправе полностью отказаться от публикации того или иного издания, на практике, приняв решение публиковать издание, она будет иметь незначительный редакционный контроль над его содержанием или не иметь его вовсе. Это особенно верно, когда CompuServe публикует издание в рамках форума, которым управляет компания, не связанная с CompuServe. "...У CompuServe не больше редакционного контроля над ...[рассматриваемым изданием]..., чем у публичной библиотеки, книжного магазина или газетного киоска, и для CompuServe столь же нецелесообразно проверять каждое издание на предмет потенциально клеветнических высказываний, как и для любого другого дистрибьютора."»

«...С учётом соответствующих соображений, касающихся Первой поправки, надлежащим стандартом ответственности, применяемым к CompuServe, является вопрос о том, знала ли она или имела ли основания знать о предположительно клеветных высказываниях Rumorville.»

Cubby, Inc. против CompuServe, Inc. (90 Civ. 6571, SDNY)

Полный текст решения

CUBBY, INC., корпорация d/b/a SKUTTLEBUT, и ROBERT G. BLANCHARD, истцы, против COMPUSERVE INC., d/b/a RUMORVILLE, и DON FITZPATRICK, в индивидуальном качестве, ответчики

Дело № 90 Civ. 6571 (PKL)

ФЕДЕРАЛЬНЫЙ ОКРУЖНОЙ СУД ЮЖНОГО ОКРУГА НЬЮ-ЙОРКА

Решение вынесено: 29 октября 1991 г.
Подано на регистрацию: 29 октября 1991 г.

WeenieFest '92: Встреча с Джоном Маркоффом

Автор: Count Zero

```
PWN ^*^ PWN ^*^ PWN { WeenieFest'92 } PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN         P h r a c k   W o r l d   N e w s         PWN
^*^         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~         ^*^
PWN            Special Edition Issue Five             PWN
^*^                                                   ^*^
PWN                  "WeenieFest '92"                 PWN
^*^                                                   ^*^
PWN           ~A Meeting With John Markoff~           PWN
^*^                                                   ^*^
PWN               Written by Count Zero               PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN { WeenieFest'92 } PWN ^*^ PWN ^*^ PWN
```

count0@world.std.com

Вступление

> *«Общее собрание Бостонского компьютерного общества, среда, 22 января, 19:30. Кэти Хафнер, соавтор книги _Cyberpunk_ (написанной вместе с мужем Джоном Маркоффом), расскажет о компьютерной этике [ну да, конечно] и компьютерных преступлениях. _Cyberpunk_ описывает истории трёх хакеров: Кевина Митника — опытного фрикера, доведшего своё увлечение до одержимости [это что, духи?] и зависимости, сеющей хаос [ёлки зелёные!] в компьютерных сетях и секретных исследовательских центрах; Пенго из Германии, взломавшего американские военные компьютеры и продавшего информацию Советскому Союзу; и Роберта Морриса — выпускника Гарварда и Корнелла, выпустившего вирусную [ЧЕРВЬ!] программу, парализовавшую тысячи компьютеров в Internet. Эта дискуссия, возможно, изменит ваши взгляды на доступность компьютеров [уж мою-то жизнь точно изменила... дааа].»*

Именно таким было объявление в журнале UPDATE Бостонского компьютерного общества (разумеется, без моих ехидных комментариев в квадратных скобках). Knight Lightning сообщил мне об этом мероприятии по электронной почте, и я прочитал письмо В ТОТ САМЫЙ день, когда оно проходило. К тому моменту я осилил примерно половину книги CYBERPUNK, и большинство из вас наверняка уже с ней знакомы. Да, это кусок дерьма. Значительная часть информации там *выдумана*, а авторы пытаются объяснить хакерство как «социальное расстройство»... сродни малолетней преступности.

Конечно, немалая часть хакерства — это просто дети, развлекающиеся от безделья, но в этой теме есть НЕЧТО БОЛЬШЕЕ. А как насчёт нарушений гражданских свобод со стороны федерального правительства и его агентов? Что с приватностью в сетях? Что насчёт НАСТОЯЩЕГО ДВИЖУЩЕГО МОТИВА большинства сегодняшних хакеров — поиска ТЕХНИЧЕСКИХ ЗНАНИЙ? Эти темы в книге так и не были раскрыты должным образом.

Усмотрев в этом собрании ОТЛИЧНУЮ возможность как следует прижать Хафнер к стенке и послушать, что скажут члены BCS, я попытался срочно поднять весь

экипаж RDT и утащить его на встречу. Увы, пойти смог *только* я один. «Да ладно, — подумал я, — наверняка там будет немало народу, который сделает обсуждение живым и *острым*.» Как же я ошибался...

Знакомство с залом

Для начала: Хафнер вообще не пришла. Вместо неё появился её муж и соавтор Джон Маркофф. Я никогда прежде не бывал на собраниях BCS и рассчитывал, что члены общества окажутся достаточно подкованы в вопросах компьютеров и компьютерной этики. Что ж, в лекционный зал набилось около восьмидесяти человек, и ВСЕ они были старше меня (кстати, мне 24). Выглядело это как сборище яппи-мусора («О, я только что купил 486... интересно, что он умеет. Наверное, вступлю в BCS!») и каких-то старых профессорских типов. Внезапно меня пробрал холод... *Тревога: ботаны!* Двое придурков за моей спиной пытались обсудить, как написать файл MS-DOS CONFIG.SYS:

> *«Боб, мой компьютер совсем заглючил. Не работает.»*
> *«Ну, может, тебе нужна одна из этих штук — SET DEVICE EQUALS что-нибудь!»*

ПРИМЕЧАНИЕ: ВСЕ цитаты НАСТОЯЩИЕ... Да, правда бывает страннее вымысла...

Маркофф на сцене

Наконец, Джон Маркофф вышел на сцену — вылитый Дастин Хоффман. Он начал с пятнадцатиминутного монолога об определениях слов «хакер», «крэкер» и «киберпанк». Вот тут у меня и началась мигрень (лёгкая пульсация в левом виске). Он рассказал о происхождении термина «киберпанк» и сделал КУЧУ отсылок к *БИЛЛУ* Гибсону. Видимо, хотел покрасоваться и дать всем понять о своих «личных» отношениях с Гибсоном. Затем он В ДЕТАЛЯХ поведал о том, как ЛИЧНО ВЫЧИСЛИЛшел того, кто запустил интернет-червя. «Я сказал им: "сделайте finger RTM"... и выскочило имя Robert T. Morris.» Ну прямо-таки СЕРЬЁЗНОЕ техническое волшебство. Маркофф хлопал себя по плечу ещё минут десять. Он явно гордился своим общением с Клиффом Столлом (упомянул THE CUCKOO'S EGG раз пять). Самолюбование, самолюбование, самолюбование. Он, казалось, был по-настоящему *горд* тем, что откопал столько всего о компьютерном подполье (хотя его книга — это ВСЕГО ЛИШЬ *ТРИ* кейса!!!).

> *«Мы хотели проникнуть в эти культуры...»*

Да, его книга по сути лишь ОПИСАНИЕ ТОГО, ЧТО ПРОИЗОШЛО (причём даже не всегда достоверное)... НЕ О КУЛЬТУРЕ... НЕ О ТОМ, что на самом деле двигало этими людьми... НЕ О ТОМ, что ДЕЙСТВИТЕЛЬНО ПРИВЛЕКАЕТ людей в компьютерное подполье. Он был просто *репортёром*, охотящимся за сенсацией. Не более.

Вопросы и ответы

После рассказа о книге он открыл дискуссию. ПЕРВЫЙ вопрос задал какой-то болван из BCS:

> *«Вы что-нибудь знаете о вирусе в ROM принтеров, использовавшихся в иракских компьютерных системах?»*

Меня замутило. Маркофф минут десять говорил об этом, а члены BCS вставляли свои реплики. АРРРГХ. Следующий вопрос тоже был хорош:

> *«А что насчёт тех компьютеров, которые недавно прошли тест Тьюринга... они его сдали? Не могли бы вы объяснить, что такое тест Тьюринга?»*

Выходит, члены BCS и правда не были в курсе происходящего. Может, никто из них не читал книгу. Может, никто из них никогда не читал Phrack или 2600. Может, все они просто сидят с головой в... одном месте?

Мои вопросы

Наконец, я пошёл в атаку. Я спросил его:

> *«Что вы думаете о наказаниях, назначенных осуждённым "киберпанкам"? Кажутся ли они вам справедливыми? Что вы скажете об изъятии оборудования без предъявления обвинений — например, в ходе Операции Sundevil?»*

Маркофф: «Я думаю, правительство просто запугивает людей. Жаль, что оборудование изымают. Это неконституционно.»

Вот и всё, что он сказал. Никаких комментариев о складывающемся в сетях ПОЛИЦЕЙСКОМ ГОСУДАРСТВЕ. Ничего о том, что делается для *защиты* свободы слова пользователей компьютеров. Мой следующий вопрос:

> *«Что, по-вашему, действительно движет "киберпанками"... насколько серьёзным "преступлением" является хакерство?»*

Маркофф: «Это просто малолетняя преступность. По большей части это не имеет никакого отношения к технической грамотности. В основном это мошенники. Надеюсь, в этом "киберпанке" есть элемент моды. Они, наверное, перерастут это.»

Да, этот парень, безусловно, держит РУКУ НА ПУЛЬСЕ подполья. Мы просто банда малолетних жуликов-мошенников. Перерастём. Ага, конечно. Чёрт, я кипел. Всё, что он говорил, было напичкано *полуправдами* и опускало ВАЖНЫЕ вещи — например, стремление исследовать сложнейшие сети и машины, — но я не собирался затевать с ним перебранку. Я успокоился и задал следующий вопрос:

> *«Что вы думаете о таких изданиях, как Phrack и 2600? Как вы относитесь к делу E911, в рамках которого пытались заткнуть Phrack?»*

Маркофф: «Я не принимаю их отговорку про "исследования". Я не хочу, чтобы кто-то проверял замки на МОЁМкомпьютере. Это просто малолетняя преступность.»

Как прозорливо. Мой вопрос о деле E911 он полностью проигнорировал. Вот тебе и понимание подполья. Ага, мы все читаем Phrack и 2600 ТОЛЬКО ДЛЯ ТОГО, чтобы что-нибудь ПОЛОМАТЬ.

***ЕДИНСТВЕННАЯ интересная вещь, которую он упомянул: БОЛЬШИНСТВО связанных с хакерством преступлений — это ДЕЛА РУК ИНСАЙДЕРОВ. Доверенных сотрудников, работающих ИЗНУТРИ. Ну что ж, это было ЕДИНСТВЕННОЕ, с чем я был полностью согласен. По крайней мере, Маркофф не пытался устроить «охоту на киберпанков»... в отличие от НЕКОТОРЫХ (Джеральдо, Дон Ингрэм и т. п.).

Дно бочки

Дальше стало по-настоящему смешно. Остальных членов BCS, похоже, совершенно не интересовали темы хакерства/фрикерства/гражданских свобод/хакерской этики и прочего. ОДИН тип спросил:

> *«Пиратство — это серьёзная проблема в США?»*

Другой спросил:

> *«Пиратские BBS ещё существуют?»*

Некий *проницательный* член BCS заявил:

> *«Да, но это опасно. Адвокаты звонят и проверяют, нет ли у вас пиратского ПО. Можно попасть в тюрьму!»*

Маркофф: «Да, пиратство по-прежнему процветает. Цифр я вам привести не могу , но знаю, что таких случаев много.»

Член BCS отвечает:

> *«То есть я могу просто позвонить куда-то и получить PageMaker бесплатно?»*

На этом месте меня вырвало... по крайней мере, в уме. Было задано ещё немало дурацких вопросов, но я вас больше мучить не буду («Что насчёт слияния IBM и Apple?»... и тому подобное). Мне удалось задать ПОСЛЕДНИЙ вопрос:

> *«Что вы думаете о "реформированных киберпанках"... например, о консалтинговой компании в сфере безопасности Comsec, созданной бывшими членами LOD?»*

Маркофф: «Я думаю, любая компания, нанимающая их, должна понимать, с кем имеет дело. Я скептически настроен. *Я бы* их не нанял.»

Стоит сказать, что в этот момент БОЛЬШИНСТВО ботанов из BCS громко засмеялись — противными, занудными смешками. Мне стоило немалых усилий не встать и не набить им морды. Не дискуссия, а одно название. Вообще, на протяжении БОЛЬШЕЙ ЧАСТИ встречи люди смеялись без видимой причины. Наверное, знали что-то, чего не знал я?

Итог

В конечном счёте встреча подтвердила мои подозрения: Маркофф — просто репортёр, делающий деньги. Наживается на полуправдах. Совершенно не интересуется точкой зрения «киберпанка». Не интересуется ЭТИКОЙ и НРАВСТВЕННЫМИ ПОСЛЕДСТВИЯМИ преследований хакеров. Он просто сообщает «новости». По крайней мере, он не пытался раздуть «охоту на ведьм»... но и понимания подполья и того, что оно «на самом деле» означает, не прибавляет: хакерство — это НЕ болезнь... это не то, из чего «вырастают»... это свобода слова... свобода исследовать (в известных пределах... хех) и ЖАЖДА исследований. ГОРАЗДО больше, чем малолетняя преступность. Надеюсь, когда-нибудь кто-нибудь напишет книгу именно с этой точки зрения.

И ещё я составил себе представление о сообществе BCS. Беспросветная темнота. Нужно ли говорить больше?

Надеюсь, этот файл вам понравился. Следите за дальнейшими «Специальными

репортажами».

```
:   -=Restricted -=Data -=Transmissions    :
:                                          :
: "Truth is cheap, but information costs." :
```

Phrack World News

Выпуск XXXVII / Часть первая из четырёх

Составители: Dispater & Spirit Walker

Федеральный арест «хакерского» оборудования

16 декабря 1991 г.

Авторы: Barbara E. McMullen & John F. McMullen (Newsbytes)

«Нью-йоркских хакеров MOD накрыли с обыском!»

НЬЮ-ЙОРК — По сведениям Newsbytes, совместная группа Секретной службы США и Федерального бюро расследований (ФБР) исполнила ордера на обыск по местам проживания так называемых «хакеров» в различных точках страны и изъяла компьютерное оборудование.

По данным Newsbytes, ордера были исполнены в пятницу, 6 декабря, в ряде мест, включая Нью-Йорк, штат Пенсильвания и штат Вашингтон. По сведениям осведомлённых источников, ордера были выданы в ходе расследований нарушений Раздела 18 федерального законодательства — статей 1029 (мошенничество с использованием средств доступа), 1030 (Закон о компьютерном мошенничестве и злоупотреблениях), 1343 (мошенничество с использованием каналов связи) и 2511 (прослушивание телефонных переговоров).

Сотрудники правоохранительных органов, с которыми связалась Newsbytes, подтвердив факт исполнения ордеров, отказались комментировать то, что было названо «продолжающимся расследованием». Один из источников сообщил Newsbytes, что аффидавиты, на основании которых были выданы ордера на обыск, засекречены ввиду незавершённости расследования.

Он добавил: «Очевидно, что в аффидавитах содержалось достаточно оснований, чтобы убедить судей в наличии вероятной причины полагать, что при проведении обысков будут обнаружены доказательства преступления».

Источник также сообщил, что ожидает заявления от совместной группы Секретной службы и ФБР «примерно после нового года».

Двое студентов Корнеллского университета арестованы за распространение компьютерного вируса

27 февраля 1992 г.

Автор: Lee A. Daniels (New York Times News Service)
Особая благодарность: Risks Digest

Двое студентов-бакалавров Корнеллского университета были арестованы в понедельник вечером и обвинены в разработке и распространении компьютерного вируса, нарушившего работу компьютеров вплоть до Калифорнии и Японии, сообщили официальные представители университета. М. Стюарт Линн, вице-президент по информационным технологиям университета в Итаке (штат Нью-Йорк), назвал студентов: Дэвид Блюменталь и Марк Пилигрим. Линн сообщил, что

оба — Блюменталь, учащийся по инженерной программе, и Пилигрим с факультета искусств и наук — являются 19-летними второкурсниками. Их арестовали вечером 24 февраля сотрудники полиции Корнелла и Итаки. По словам Линна, студенты предстали перед городским судом Итаки по обвинению в компьютерном вмешательстве второй степени — уголовном проступке — и были отправлены в окружную тюрьму. Линн сообщил, что власти считают именно этих двоих ответственными за компьютерный вирус, внедрённый в три игры для Macintosh 14 февраля.

Он назвал игры: Obnoxious Tetris, Tetricycle и Ten Tile Puzzle. Вирус, по всей видимости, впервые появился в открытом компьютерном архиве Стэнфордского университета и распространился оттуда среди пользователей, загружавших эти игры на свои компьютеры.

Линн сообщил, что сотрудники Корнелла и других организаций обнаружили вирус на прошлой неделе и оперативно разработали то, что он назвал «дезинфицирующим» программным обеспечением для его уничтожения. По его словам, на прошлой неделе сотрудники отследили вирус до Корнелла, однако он не стал уточнять, каким именно образом и что навело следствие на двух студентов. Линн отметил, что ещё не знает, какой ущерб нанёс вирус. «В Корнелле мы категорически осуждаем подобное поведение», — заявил он.

Примечание: Ссылки на инцидент с вирусом Роберта Морриса-мл. в Корнелле удалены.
Агентство Associated Press сообщило, что оба обвиняемых содержатся в тюрьме округа Томпкинс под залог в 10 000 долларов.

Хакер признал взлом систем NASA

26 ноября 1991 г.

Автор: John C. Ensslin (Rocky Mountain News, стр. 6)
См. также: Phrack 34, файл 11
Особая благодарность: The Public

Самоучка-хакер со средним образованием в понедельник признал, что взломал защищённую компьютерную систему NASA — причём быстрее, чем команда Denver Broncos успевает сыграть футбольный матч.

Ричард Г. Уитман-мл., 24 года, сообщил федеральному окружному судье Денвера Шерману Файнсильверу, что ему потребовалось около «полутора-двух часов» работы на персональном компьютере через телефонную линию из его квартиры, чтобы получить доступ к закрытым файлам космического агентства.

Уитман в понедельник признал себя виновным по одному уголовному обвинению в изменении информации — пароля — в федеральном компьютере. В рамках соглашения о признании вины федеральные прокуроры сняли шесть аналогичных обвинений из обвинительных заключений, вынесенных в сентябре.

Выпускник средней школы Northglenn сообщил судье, что формального образования в области компьютеров он не получал. Большинство знаний о компьютерах он почерпнул из книг. И большинство этих книг, по его словам, сейчас находятся на федеральном складе — изъяты после того, как агенты ФБР обыскали его квартиру в Вестминстере в прошлом году.

«Вы думаете, вы смогли бы обучить этих двух адвокатов компьютерным делам?» — спросил Файнсильвер, имея в виду государственного защитника Уитмана и прокурора. «Вероятно», — ответил Уитман.

Уитман не только взломал 118 систем NASA, но и просматривал файлы и электронную почту других пользователей, сообщил помощник прокурора США Грегори К. Граф.

По словам Графа, следователям NASA потребовалось почти 300 часов, чтобы выследить Уитмана, и ещё 100 часов на переписывание программного обеспечения.

Уитману грозит до пяти лет лишения свободы и штраф в размере 250 000 долларов. Однако Граф отметил, что при вынесении приговора 13 января правительство будет добиваться значительно более мягкого наказания.

Обе стороны пришли к соглашению о возмещении 1 100 долларов за звонки за счёт взломанной системы. Однако они расходятся во мнениях относительно того, должен ли Уитман нести ответственность за стоимость нового программного обеспечения.

Хакер признал себя виновным

5 декабря 1991 г.

Особая благодарность: Iron Eagle

«24-летний хакер из Денвера, признавший взлом защищённой компьютерной системы NASA, признал себя виновным по уголовному обвинению в изменении информации.

В рамках соглашения о признании вины в понедельник федеральные прокуроры сняли шесть аналогичных обвинений против Ричарда Г. Уитмана-мл., которому грозило до пяти лет лишения свободы и штраф в 250 000 долларов. По заявлению властей, при вынесении приговора 13 января правительство будет добиваться значительно более мягкого наказания.

Обе стороны пришли к соглашению о возмещении 1 100 долларов за звонки за счёт компьютерной системы, однако расходятся во мнениях относительно того, должен ли Уитман нести ответственность за стоимость нового программного обеспечения.

Уитман сообщил федеральному окружному судье Шерману Файнсильверу, что ему потребовалось около двух часов работы на домашнем персональном компьютере, чтобы получить доступ к закрытым файлам космического агентства. По словам прокуроров, следователям NASA понадобилось почти 300 часов, чтобы выследить Уитмана, и ещё 100 часов на переписывание программного обеспечения для предотвращения повторения инцидента».

В последнем программном обеспечении Novell обнаружен скрытый вирус

20 декабря 1991 г.

Автор: John Markoff (New York Times)

Крупнейший поставщик сетевого офисного программного обеспечения для персональных компьютеров разослал письма примерно 3 800 клиентам с предупреждением о том, что непреднамеренно допустил заражение вирусом копий дискеты, отправленной в начале месяца.

В письме, направленном в среду клиентам Novell Inc. — издателя программного обеспечения из Прово (штат Юта) — сообщалось, что дискета, разосланная 11 декабря, была случайно заражена вирусом, известным специалистам как «Stoned III».

Официальный представитель компании сообщил накануне, что Novell получила ряд сообщений от клиентов о проникновении вируса в их системы, хотя случаев повреждения данных зафиксировано не было.

Однако калифорнийский эксперт по компьютерным вирусам заявил, что потенциал для нанесения ущерба весьма значителен, а вирус на дискете Novell нередко выводил из строя заражённые компьютеры.

Огромные потенциальные убытки

«Если это распространится по организации и поразит 1 500–2 000 машин, вы получите миллионы долларов расходов на устранение последствий», — заявил Джон Макафи, президент McAfee & Associates, консалтинговой антивирусной компании из Санта-Клары (Калифорния). «Неважно, что заражены лишь несколько машин, — сказал он. — Нельзя это определить наверняка. Придётся остановить всю сеть, а потенциальные убытки колоссальны». По словам г-на Макафи, он получил несколько десятков звонков от пользователей Novell, часть которых была возмущена.

Инцидент с Novell — второй подобный случай в этом месяце. 6 декабря компания Konami Inc., производитель программных игр из Буффало-Гроув (штат Иллинойс), написала клиентам, что дискеты с игрой Spacewrecked также оказались заражены более ранней версией вируса Stoned. В письме компания сообщила, что идентифицировала вирус до того, как большой объём дискет был отгружен дилерам.

Источник вируса неизвестен

Представители Novell сообщили, что после получения звонков в начале недели им удалось отследить источник заражения до определённого этапа производственного процесса. Однако они не смогли установить, каким образом вирус изначально поразил их программное обеспечение.

Клиенты Novell — одни из крупнейших корпораций страны. Программное обеспечение, называемое Netware, управляет офисными сетями — от двух-трёх машин до тысячи систем.

«Вирусы — это вызов для рынка», — заявил Джон Эдвардс, директор по маркетингу систем Netware в Novell. «Но мы будем сохранять бдительность». По его словам, вирус поразил дискету со справочной энциклопедией, которую компания рассылала своим клиентам.

Серверам ущерб не нанесён

Компьютерные вирусы — это небольшие программы, которые передаются от компьютера к компьютеру, тайно внедряясь в файлы данных, копируемые затем на дискетах или по компьютерной сети. Программы могут быть написаны для выполнения вредоносных задач после заражения нового компьютера или лишь копировать себя с машины на машину.

В письме клиентам компания сообщила, что вирус Stoned III не распространяется по компьютерным сетям на файловые серверы, составляющие основу сетей. Файловые серверы — это специальные компьютеры с большими дисками, хранящие и распределяющие данные по сети настольных компьютеров.

Вирус Stoned III действует, внедряясь в специальную область дискеты, а затем копируя себя в память компьютера для заражения других дискет.

Однако г-н Макафи сообщил, что программа также копирует себя на жёсткий диск компьютера, где может иногда вывести систему из строя. В этом случае возможна потеря данных, если вирус записывает информацию поверх области, где хранится специальный каталог.

По словам г-на Макафи, о вирусе Stoned III впервые сообщили в Европе всего три месяца назад. Новый вирус относится к классу программ, известных как «стелс»-вирусы, — они маскируют своё местоположение и с трудом поддаются идентификации. Г-н Макафи предположил, что именно поэтому программе удалось избежать обнаружения компанией.

Меры по обнаружению

По словам г-на Эдвардса, Novell работает над внедрением новых технологий в своё программное обеспечение, призванных затруднить проникновение вирусов. Недавно компания лицензировала специальное программное обеспечение на основе цифровой подписи, затрудняющее незаметное распространение вирусов. Novell планирует включить эту новую технологию в следующий крупный релиз своего программного обеспечения, запланированный на конец 1992 года.

В прошлом суды, как правило, не привлекали компании к ответственности за ущерб в случаях, когда виновником является третья сторона, пояснила Сьюзен Никум, адвокат из Пало-Альто (Калифорния), специализирующаяся на компьютерных вопросах. «Если компания проявила должную осторожность, привлекать её к ответственности было бы несправедливо», — заявила она. «Но в конечном счёте это может оказаться вопросом для суда присяжных».

Working Assets Long Distance!

Январь 1992 г.

Взято из рекламы в журнале Mother Jones

(На фото, отсутствующем в оригинале, — студент колледжа, показывающий «средний палец», с подписью: «Двадцать лет спустя мы дали людям лучший способ применить этот палец».)

Текст рекламного объявления:

Сидячие забастовки. Марши протеста. Цветочная революция. Времена изменились, но потребность в участии рядовых граждан никуда не делась.

Представляем «Working Assets Long Distance» — ЕДИНСТВЕННУЮ телефонную компанию, столь же приверженную социальным и политическим переменам, как и вы. Каждый раз, когда вы пользуетесь пальцем для звонка на дальнее расстояние, один процент счёта поступает в некоммерческие правозащитные организации — без каких-либо затрат для вас. Это такие действенные организации, как AMNESTY INTERNATIONAL, GREENPEACE, PLANNED PARENTHOOD FEDERATION OF AMERICA, AMERICAN CIVIL LIBERTIES UNION и многие другие.

Мы больше, чем телефонная компания, жертвующая деньги на благие дела. Наша цель — дать услышать ваш личный голос. Именно поэтому мы предлагаем *БЕСПЛАТНЫЕ ЗВОНКИ* руководителям корпораций и политикам. А также грамотно составленные письма по цене, значительно ниже стоимости телеграммы. Так что вы можете потребовать прекратить вырубку древних лесов или дать сенаторам знать своё мнение по важным вопросам, например о праве на репродуктивный выбор. Всё так просто. Ваш телефон становится инструментом демократии, и вы ничего не теряете. Понимаете, Working Assets предоставляет те же услуги, что и крупные операторы дальней связи. Удобный набор «1» для дальних звонков, круглосуточная работа и качество звука волоконно-оптических линий. И всё это по тарифам ниже базовых тарифов AT&T. А подключение не может быть проще.

Просто позвоните нам по номеру 1-800-788-8588, доб. 114, или заполните купон сегодня. Мы подключим вас немедленно, без каких-либо вторжений или неудобств. Чтобы вы могли помогать изменять мир, не шевеля и пальцем. Ну ладно, может, одним пальцем.

Компьютерный вирус в войне в Персидском заливе

12 января 1991 г.

Взято из The Boston Globe (стр. 12)
Особая благодарность: Tone Surfer

За несколько недель до начала войны в Персидском заливе американские агенты разведки внедрили компьютерный вирус в сеть иракских компьютеров, связанных с системой противовоздушной обороны страны, — сообщает новостной журнал. По данным U.S. News and World Report, вирус был разработан сверхсекретным Агентством национальной безопасности в Форт-Миде (штат Мэриленд) и предназначался для вывода из строя мэйнфрейм-компьютера.

В репортаже со ссылкой на двух неназванных высокопоставленных американских чиновников говорилось, что вирус, по всей видимости, сработал, однако подробностей не приводилось. Также отмечалось, что операция, возможно, не имела практического значения: подавляющее воздушное превосходство союзников в любом случае обеспечило бы тот же результат — вывод из строя радаров и ракет системы противовоздушной обороны. Секретная операция началась, когда американские разведчики установили, что компьютерный принтер французского производства должен был быть переправлен контрабандой из Аммана (Иордания) на военный объект в Багдаде.

Агенты в Аммане заменили в принтере компьютерный чип другим микрочипом, содержащим вирус в своих электронных схемах. Атакуя иракский компьютер через принтер, вирус смог избежать обнаружения стандартными средствами электронной защиты, говорится в репортаже. «Попав в систему, — объяснили американские чиновники, — вирус действовал так: каждый раз, когда иракский техник открывал "окно" на экране своего компьютера для доступа к информации, содержимое экрана просто исчезало», — сообщало U.S. News.

Этот материал входит в книгу, написанную по итогам 12-месячного расследования журналистов U.S. News: «Triumph without Victory: The Unreported History of the Persian Gulf War» («Триумф без победы: нерассказанная история войны в Персидском заливе»), которая должна была выйти в следующем месяце.

Обвинительные заключения против «информационных брокеров»

Январь 1992 г.

Взято из The Privacy Journal

Нечестивый союз между «информационными брокерами» и государственными чиновниками, торгующими персональными данными, был разоблачён в ходе вынесения обвинительных заключений большого жюри в отношении 18 человек в 14 штатах.

Прокурор США Майкл Чертофф в Ньюарке (штат Нью-Джерси) и его коллега в Тампе (Флорида) обвинили восьмерых «информационных брокеров» (известных также как «информационные посредники» или «суперагентства») во взяточничестве в отношении двух сотрудников Администрации социального обеспечения с целью получения конфиденциальных сведений о

доходах и персональных данных, хранящихся в федеральных компьютерных базах данных. Брокеры, занимающие нишу между крупными бюро кредитных историй и отслеживающие местонахождение лиц, продавали эту информацию своим клиентам — розничным торговцам, адвокатам, детективам, страховым компаниям и другим.

Нед Флемминг, президент Super Bureau Inc. из Монтерея (Калифорния), был обвинён по 32 статьям за склонение надзорного сотрудника Администрации социального обеспечения в Нью-Джерси по имени Джозеф Линч (который не был привлечён к ответственности) к предоставлению конфиденциальных персональных данных за вознаграждение. Его дочь Сьюзен также была привлечена к ответственности, как и Виктор Фот, оператор Locate Unlimited в Меса (Аризона); Джордж Т. Теодор, владелец Tracers Worldwide Services в Корпус-Кристи (Техас); Ричард Стоун, владелец Interstate Information Services в Порт-Джефферсон (Нью-Йорк); и Майкл Хоус, бывший владелец International Criminal Investigative Agency (ICIA) в Порт-Анджелесе (Вашингтон) — все за участие в том же сговоре. Ещё один брокер — Джозеф Норман Диллон Росс, ведущий деятельность под собственным именем в Паума-Вэлли (Калифорния), — также принимал персональные данные, по данным Чертоффа, однако обвинения ему предъявлены не были. Ричард Стоун дополнительно был обвинён в подкупе клерка Администрации социального обеспечения в Мелроуз-Парке (Иллинойс). Также к ответственности были привлечены Аллен Швайцер и его жена Петра, управляющие Security Group в Самнере (Вашингтон).

Государственные служащие также похищали персональные данные из Национального информационного центра по уголовным делам (NCIC) ФБР, хранящего данные об арестах и без вести пропавших лицах.

Флемминг сообщил Privacy Journal, что никогда не встречался с Линчем. Стоун отказался комментировать. Tracers Worldwide, ICIA и Locate Unlimited не числятся в телефонных справочниках, хотя все три компании обязаны по Закону о добросовестных кредитных отчётах (Fair Credit Reporting Act) предоставлять субъектам своих дел доступ к соответствующей информации.

18-месячное расследование, завершившееся 18 декабря обвинительными заключениями и арестами, является лишь первым этапом, заявил помощник прокурора США Хосе Сьерра. «Мы не думаем, что этим всё заканчивается».

На протяжении последних трёх лет крупнейшие тройка бюро кредитных историй продолжали регулярно продавать кредитную информацию информационным брокерам — даже после жалоб на то, что некоторые из них нарушили Закон о добросовестных кредитных отчётах, раскрыв кредитную информацию в недопустимых целях. Президент Trans Union Альберт Флиткрафт заявил в Конгрессе в 1989 году, что крупному бюро кредитных историй невозможно защитить потребительскую информацию, проданную брокерам. Джон Бейкер, старший вице-президент Equifax, тогда же сообщил, что большая тройка «объединит лучшие умы», чтобы выяснить, можно ли разработать защитные меры. К 1991 году Оскар Маркис, вице-президент Trans Union, просил Конгресс предложить решения, тогда как Бейкер представил новые руководящие принципы Equifax и контрольный список для ведения бизнеса с брокерами. Ни одна из большой тройки не была готова прекратить работу с мутными торговцами переработанными кредитными отчётами — и похищенной информацией из баз данных Администрации социального обеспечения и ФБР.

А тем временем в Налоговой службе...

Спустя две недели после разоблачения информационных брокеров прокурор США Майкл Чертофф в Нью-Джерси предъявил обвинение вышедшему на пенсию начальнику отдела уголовных расследований Налоговой службы (IRS) в продаже персональных данных калифорнийскому частному детективному агентству на последней рабочей неделе в 1988 году.

Согласно обвинительному заключению, за вознаграждение в 300 долларов руководитель IRS Роберт Дж. Рош обязался раздобыть непубличные записи актов гражданского состояния из органов регистрации. Используя ложные предлоги, он поручил одному из своих подчинённых получить эту информацию в рабочее время. Помощнику удалось раздобыть записи в одном случае лишь после того, как он оформил вызов от IRS, а в другом — после того, как предъявил письмо на бланке IRS с утверждением, что информация необходима для «официальных следственных действий». По данным прокурора США, Рош принял оплату от калифорнийского детективного агентства Saranow, Wells & Emirhanian, входящего в более крупную сеть под названием Financial Investigative Services Group.

The Privacy Journal — независежное ежемесячное издание о вопросах приватности в компьютерную эпоху. Адрес редакции:

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

Нарушения в базах данных АСО и ФБР подтолкнули к оценке систем безопасности

13 января 1992 г.

Автор: Kevin M. Baerson (Federal Computer Week, стр. 1, 41)

Недавно вынесенные обвинительные заключения в отношении инсайдеров, покупавших и продававших конфиденциальную информацию из компьютеров ФБР и Администрации социального обеспечения (АСО), побудили официальных лиц ведомств оценить уровень защищённости государственных баз данных.

«Я расцениваю это скорее как позитивное, нежели негативное событие», — заявил Дэвид Немечек, начальник отдела Национального информационного центра по уголовным делам (NCIC) ФБР, содержащего данные о тысячах лиц, подозреваемых или осуждённых за преступления. «Рад ли я тому, что это произошло? Нет. Но это позволило нам обнаружить происходящее и посылает сигнал: кто попытается — попадётся».

Однако Ренни Ди Пентима, помощник комиссара АСО по вопросам проектирования и развития систем, не счёл обвинительные заключения позитивным событием.

«Это не победа, — заявил Ди Пентима. — Даже если мы их поймаем — это всё равно поражение. Победа для меня — это когда мне вообще не поступает сообщений о том, что кто-то злоупотребил своим положением».

«Разоблачение информационных брокеров» стало результатом 18-месячного расследования инспекционного управления Министерства здравоохранения и социальных служб в Атланте. Официальные лица назвали это крупнейшим в истории делом, связанным с хищением федеральных компьютерных данных. По их словам, возможны новые обвинительные заключения.

Специальные агенты ФБР присоединились к расследованию, и в конечном счёте удалось задержать 18 человек из 10 штатов, включая одного бывшего и двух действующих сотрудников АСО. Среди обвиняемых также оказались офицер полиции Чикаго, сотрудник департамента шерифа округа Фултон в Джорджии и несколько частных детективов.

Согласно обвинительным заключениям, следователи платили за конфиденциальные данные — в том числе записи о судимостях и сведения о заработках, — которые изымались из баз данных лицами, злоупотреблявшими своим правом доступа.

«ФБР не может контролировать каждого жителя Соединённых Штатов», — заявил Немечек. «У нас есть разнообразные средства защиты для предотвращения подобного. Мы ведём журналы использования систем с указанием пользователей и целей обращений, проводим учебные программы по безопасности и регулярные проверки запросов».

«Однако лица, допустившие нарушения, имели законный доступ к системе, и есть лишь один способ справиться с этим: активное уголовное преследование виновных. И ФБР активно занимается этими людьми».

Проблема Ди Пентимы столь же деликатна. Его ведомство ежедневно проводит 15 миллионов электронных транзакций — 500 в секунду, — и отслеживать правомерность действий сотрудников — задача колоссальная.

В настоящее время каждому сотруднику, работающему с сетью, присваивается пароль и личный идентификационный номер (PIN), которые регулярно меняются. В зависимости от характера работы сотрудника PIN предоставляет ему доступ к определённым видам информации.

Если сотрудник пытается войти в меню системы, к которому у него нет права доступа, или более одного раза допускает ошибку при вводе PIN, он блокируется в системе. После этого восстановить доступ может только специалист по безопасности из одного из 10 региональных отделений ACO.

Начальник отдела ACO вместе с шестью аналитиками, работающими в головном центре обработки данных ведомства под Балтимором, также регулярно выявляют аномалии транзакций — например, сотрудников, выполнивших необычно большое количество операций с определённым счётом.

ФБР также располагает рядом мер предосторожности. Сотрудники ФБР проводят выборочные проверки поисковых запросов, а, по словам Немечека, масштабные проверки использования системы на уровне штатов и местных органов власти проводятся дважды в год. Более того, при необходимости ФБР легко может отследить запрос доступа вплоть до конкретного терминала и пользователя, от которого он поступил.

Ди Пентима сообщил, что после вынесения обвинительных заключений рассматривает новые меры для ужесточения контроля над нарушителями.

Немечек отметил, что по мере продолжения модернизации базы данных NCIC центр может автоматизировать проверку деятельности государственных и местных органов власти для выявления закономерностей и тенденций использования — по образцу ACO.

Однако, несмотря на усилия по ужесточению сетевой безопасности, оба понимают: в случаях, когда федеральные и муниципальные служащие злоупотребляют законным доступом, технологии и регламенты способны лишь ограниченно влиять на человеческую природу.

Повреждения в Свободном университете

24 февраля 1992 г.

Автор: The Dude (из Голландии)

Расследование, проведённое полицией Амстердама совместно с антимошеннической группой CRI (аналог ФБР) и кафедрой географических наук Свободного университета, привело к аресту двух хакеров. Двоим удалось взломать компьютерную систему кафедры и нанести ущерб на сумму

свыше 100 000 нидерландских гульденов.

На пресс-конференции, состоявшейся в прошлую пятницу, следственные группы объявили, что дуэт — 25-летний инженер-программист Р.Й.Н. из Нюнена [хакерский псевдоним Fidelio] и 21-летний студент-программист Х.Х.Х.В. из Рурмонда [хакерский псевдоним Wave] — стали первыми «хакерами», арестованными в Нидерландах. В ряде других стран подобное уже случалось.

Задержанные хакеры дали полные признательные показания. С ноября 1991 года они проникали в компьютер университета от 30 до 40 раз. Система была известна под именем «bronto». Используя её, хакеры получали доступ к другим системам, перемещаясь по системам в США, Скандинавии, Испании и Италии.

По словам руководителя группы по борьбе с компьютерными преступлениями полиции Амстердама Д. Комена, двое взломали коды системы ВУ, чтобы в неё проникнуть. Им удалось заполучить так называемые «пароли» официально зарегистрированных пользователей, что позволило им пользоваться системой бесплатно. Им также удалось получить «максимальные права» в компьютерной системе «bronto».

В общей сложности были обысканы четыре дома; несколько персональных компьютеров, распечатки и большое количество дискет были изъяты. Дуэт был передан в прокуратуру и заключён под стражу. Поскольку «хакерство» в Нидерландах не является уголовно наказуемым деянием, подозреваемым официально предъявлены обвинения в фальсификации документов, уничтожении имущества и мошенничестве.

В этом году правительство, по словам П. Слорта из CRI, рассчитывает принять законодательство, криминализирующее хакерство.

Дуэт хакеров заявил, что занялся незаконной деятельностью из фанатичного «хобби». «Это кайф — посмотреть, как далеко ты можешь зайти», — говорит г-н Слорт из CRI. Оба заявили, что не знали, что их цифровые путешествия нанесли огромный ущерб. Полиция также не считает их настоящими преступниками: пара не зарабатывала деньги на своей деятельности.

Компьютерный инженер приговорён к смертной казни

9 февраля 1992 г.

Особая благодарность: Ninja Master

Ричард Фарли держался хладнокровно до конца: перед уходом из зала суда, где ему вынесли смертный приговор за убийство семи человек в припадке ярости из-за неразделённой любви, он сделал глоток воды и одёрнул пиджак.

«Я не из тех, кто склонен к демонстративности или слезам», — заявил Фарли в пятницу перед тем, как принести извинения за убийства. «Я действительно сожалею о жертвах... Я не идеальный человек. Я добр. Я зол».

Фарли был осуждён в октябре за убийства, совершённые в 1988 году в компании ESL Inc. — оборонном подрядчике из Саннивейла. 1 ноября присяжные рекомендовали высшую меру наказания для компьютерного инженера, который, по версии обвинения, спланировал расправу, чтобы привлечь внимание бывшей коллеги, отвергшей его.

Судья Верховного суда Джозеф Биафоре-мл. назвал Фарли жестоким убийцей, проявившим «полное пренебрежение к человеческой жизни».

«Обвиняемый... убивал с намерением доказать объекту своей неразделённой любви, что он больше не слабак», — заявил Биафоре.

В ходе процесса обвинение подробно описало 3,5-летнее навязчивое преследование Лоры Блэк Фарли. Он отправлял ей более 100 писем, преследовал её днём и ночью, оставлял подарки на её рабочем столе и рылся в конфиденциальных личных делах сотрудников, выискивая подробности её жизни.

Несмотря на её неоднократные отказы, Фарли не отступал и был уволен в 1987 году за преследование. Год спустя он вернулся в ESL.

Блэк, 30 лет, была ранена в плечо во время расправы, однако выжила и дала показания против Фарли. По её словам, примерно за неделю до убийств она получила судебный запрет, ограждавший её от него.

Фарли, 43 года, признал факт убийств, однако заявил о невиновности: по его словам, он никогда не планировал убийство, а лишь хотел привлечь внимание Блэк или покончить с собой у неё на глазах в ответ на отказ.

Адвокат Фарли Грегори Параску доказывал, что суждение его подзащитного было помрачено навязчивой идеей и что до расправы он не проявлял склонности к насилию и вряд ли снова пойдёт на убийство.

Однако помощник окружного прокурора Чарльз Константинидес заявил, что Фарли годами готовился к убийству: практиковался в стрельбе и закупал оружие, включая огнестрельное и 98 фунтов боеприпасов, использованных в ESL.

Судья отклонил ходатайство защиты о замене приговора пожизненным лишением свободы и отказал в новом судебном разбирательстве. В соответствии с законодательством Калифорнии смертный приговор Фарли будет автоматически направлен на пересмотр в Верховный суд штата.

Среди присутствовавших в зале суда были родственники некоторых жертв, четверо из которых обратились к судье.

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                           PWN
PWN               Phrack World News           PWN
PWN                                           PWN
PWN       Issue XXXVII / Part Two of Four     PWN
PWN                                           PWN
PWN     Compiled by Dispater & Spirit Walker  PWN
PWN                                           PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Dispater & Spirit Walker

Операция «Sun-Devil» настигает первого подозреваемого — 17 февраля 1992 г.

Майкл Александер (ComputerWorld, стр. 15)

«Обвиняемый признал вину во владении кодами доступа; ему грозит десять лет заключения»

Министерство юстиции США сообщило на прошлой неделе об успешном завершении первого судебного преследования в рамках расследования «Операция Sun-Devil».

Роберт Чандлер [известный также как The Whiz Kid, бывший оператор доски объявлений Whiz House в зоне NPA 619], 21 год, признал себя виновным в федеральном суде Сан-Диего по одному уголовному обвинению — в хранении пятнадцати и более кодов доступа, которые могут использоваться для незаконных звонков по бесплатным телефонным линиям, — сообщил Скотт Чарни, руководитель отдела компьютерных преступлений Министерства юстиции в Вашингтоне. Кроме того, Чандлер признал факт использования этих кодов.

Приговор Чандлеру будет вынесен 11 мая. Максимальная мера наказания по закону составляет десять лет лишения свободы, однако федеральные прокуроры, по всей видимости, порекомендуют условный срок — при условии, что это допускается руководящими принципами назначения наказаний и позицией судьи по данному делу, уточнил Чарни.

Помимо этого, с Чандлера может быть взыскана компенсация — пока не определённая по размеру — за телефонные переговоры, совершённые с использованием кодов доступа.

7 и 8 мая 1990 года Секретная служба США и местные правоохранительные органы исполнили более двадцати ордеров на обыск [по некоторым данным — двадцать семь] в четырнадцати городах в рамках общенациональной операции против компьютерных преступлений под названием «Operation Sun-Devil». Федеральные силовики заявили, что рейды были направлены на ликвидацию организованных группировок, занимавшихся телефонным мошенничеством и мошенничеством с кредитными картами.

В ходе облавы было изъято около сорока двух компьютеров и двадцати трёх тысяч дисков, однако вплоть до прошлой недели расследование не привело ни к одному обвинительному заключению или приговору.

Министерство юстиции подвергается жёсткой критике со стороны Computer Professionals for Social Responsibility (CPSR), Electronic Frontier Foundation (EFF) и других правозащитных организаций за то, как ведётся дело «Sun-Devil». CPSR обвиняет федеральных силовиков в грубом нарушении

прав, гарантированных Первой и Четвёртой поправками к Конституции, в отношении лиц, ставших объектами этих рейдов.

Конец быстрых времён для Spicoli

Автор: Night Ranger

19 ноября 1991 года Spicoli был разбужен в своей квартире шерифами округа Пима (Аризона) и сотрудниками других ведомств. Ему предъявили ордер на обыск, выданный по подозрению в «компьютерном мошенничестве и/или краже», и попросили выйти на улицу. Затем они приступили к демонтажу его компьютерной системы, на которой работала доска объявлений под названием «Fast Times». Это не была хакерская или фрикерская BBS, и в ней не содержалось никаких материалов, которые можно было бы расценить именно так. Главной причиной существования борды было то, что он писал её сам.

Власти изъяли множество предметов, не связанных с его компьютером, включая видеомагнитофон. Никаких обвинений ему предъявлено не было, и его уведомили, что он «свободен». Этот инцидент очень напоминает то, что произошло с хакером Mind Rape: в конце прошлого года его дом был обыскан, масса вещей изъята — но обвинения так и не последовали.

Spicoli попытался нанять частного адвоката, однако выяснилось, что это ему не по средствам. С тех пор он решил воспользоваться услугами государственного защитника.

Спустя несколько недель выяснилось, что его дело связано с неназванной, но предположительно крупной суммой похищенных денег, и ему были предъявлены обвинения по нескольким тяжким статьям. Также стало известно, что власти следили за ним на протяжении как минимум трёх месяцев. Всем, кто имел с ним контакты в период с августа по ноябрь, следует проявлять осторожность. Его компьютер теперь находится в руках государства.

Это второй крупный арест в Аризоне за вторую половину 1991 года. Учитывая присутствие в штате таких людей, как Гейл Тэккери, и антихакерских компаний вроде Long Distance For Less и U.S. West, это определённо не лучшее место для какой-либо хакерской деятельности.

U2 потрясли New England Bell — 24 февраля 1992 г.

Стив Морс (The Boston Globe, стр. 15)

Ирландские рокеры U2 заставили местных телефонных операторов работать в авральном режиме. В беспрецедентном шаге, призванном пресечь деятельность спекулянтов, продажа билетов на концерт U2 17 марта в Boston Garden велась исключительно по телефону с оплатой картой — и этим утром телефонной компании пришлось несладко.

«Это был полный коллапс. Иначе не скажешь. Они накрыли нас с головой», — сообщила Джоанн Уоддел, менеджер New England Telephone. «Мы ожидали большого числа звонков... но это было невероятно. Наши операторы щёлкали не переставая».

Шоу в Garden было распродано за четыре с половиной часа, сообщил Даг Борг из Tea Party Concerts, добавив, что это заняло столько времени из-за ограничения в два билета на человека — ещё одна мера против перекупщиков.

«Спрос был ошеломляющим. Я слышал, что за первый час поступило полмиллиона звонков», — сказал Ларри Моултер, президент Boston Garden. Телефонная компания сообщила, что точные данные ещё не готовы, однако сведения Моултера согласуются с недавними показателями продаж U2 в Атланте, где было зафиксировано более миллиона звонков, многие из которых поступали от нетерпеливых фанатов с автодозвоном.

«У меня нет точных цифр. Но тысячи — это точно, многие тысячи», — сказал Питер Кронин, представитель New England Telephone. Он признал, что были незначительные задержки с получением тонального сигнала, однако назвал ситуацию «не критической». «Если люди не вешали трубку, они получали тональный сигнал через несколько секунд», — добавил он.

Для продажи билетов на концерт в Garden использовалась сотня линий. Операторы проверяли совпадения имён, номеров кредитных карт и адресов (для соблюдения лимита в два билета на человека) и выявили «некоторые» попытки использовать номер карты более одного раза.

Федеральные агенты совершают налёт на WCFL; станция заглушена и снята с эфира — 28 января 1992 г.

Патрик Таунсон (Telecom Digest)

В необычном для Федеральной комиссии по связи шаге радиостанция в юго-западном пригороде Чикаго была снята с эфира по требованию FCC, которая обвиняет её в незаконной деятельности.

WCFL-FM (104,7 МГц), станция, лицензированная в Моррисе (Иллинойс) и не имеющая никакого отношения к одноимённой чикагской станции, работавшей несколько лет назад, была заглушена сотрудниками FCC, прибывшими на место в сопровождении представителей Маршальской службы США в пятницу, 24 января.

По жалобам других чикагских вещателей инспекционная группа FCC 16 января установила, что WCFL транслирует сигнал на мощности, более чем вдвое превышающей разрешённые 11 000 Вт, и использует ненаправленную антенну вместо направленной, предусмотренной лицензией.

Последствием нарушений стало распространение более мощного сигнала в сторону Чикаго и других районов, что «увеличивает вероятность помех для других станций», — сообщил Дэн Эмрик, руководитель отдела расследований чикагского офиса FCC.

FCC уже привлекала станцию к ответственности за аналогичные нарушения в 1990 году и оштрафовала владельцев на 3000 долларов. По словам Эмрика, никаких записей об уплате штрафа не сохранилось.

Тим Спайрс является генеральным директором WCFL и должностным лицом материнской компании «MM Group», базирующейся в Огайо. Ни Спайрс, ни другие руководители «MM Group» никак не отреагировали на действия FCC, которые вынудили станцию прекратить вещание в 13:00 в прошлую пятницу.

Эмрик сообщил, что федеральные сотрудники вошли на станцию незадолго до 13:00 и вручили надлежащие юридические документы дежурным сотрудникам. Затем представители FCC захватили студию вещания и передающее оборудование. После обязательного прощального сообщения и позывного в эфире питание передатчика было отключено. Сотрудникам было приказано покинуть помещение, которое было опечатано маршалом США.

Эмрик добавил, что станции не позволят возобновить вещание до тех пор, пока она не урегулирует свои отношения с FCC и не завершит монтаж направленной антенны. После этого станции разрешат работать «на испытательном сроке» — до окончания технических проверок со стороны

комиссии, причём испытательный срок продолжится ещё в течение неопределённого времени.

Вчера «MM Group» наконец выпустила пресс-релиз, в котором, в частности, говорилось, что WCFL «...прекратила вещание добровольно — для установки новой антенны, приведения передатчика в соответствие с нормами FCC и улучшения качества обслуживания своей аудитории».

Новые сотовые телефоны порождают общенациональную дискуссию о национальной безопасности — 6 февраля 1992 г.

Джон Маркофф (New York Times, стр. D1)

Сторонники права на неприкосновенность частной жизни бросают вызов наиболее засекреченному разведывательному ведомству страны в вопросе о том, какой уровень конфиденциальности будет обеспечен при общении посредством нового поколения сотовых телефонов и беспроводных компьютеров.

Этот вопрос возник на заседаниях малоизвестного комитета экспертов в области телекоммуникаций, который должен определить, какие виды защиты от прослушивания будут заложены в новые модели сотовых телефонов. Сторонники защиты частной жизни настаивают на внедрении более мощных алгоритмов шифрования и дешифрования, чтобы предотвратить прослушивание — столь лёгкое и столь распространённое в нынешнем поколении сотовых аппаратов.

Однако правозащитники утверждают, что отраслевой комитет уже принял решение не внедрять максимальный уровень защиты под давлением Агентства национальной безопасности (АНБ), чья разведывательная деятельность включает прослушивание телефонных переговоров в иностранных государствах и перехват данных, передаваемых компьютерами. По мнению сторонников защиты частной жизни, АНБ противодействует внедрению труднодешифруемых алгоритмов, поскольку соответствующее оборудование может использоваться за рубежом.

«АНБ пытается ослабить технологии обеспечения конфиденциальности», — заявил Марк Ротенберг, вашингтонский директор Computer Professionals for Social Responsibility. «На кону — не что иное, как будущее нашей частной жизни в мире коммуникаций».

Группа по установлению стандартов состоит из производителей оборудования для сотовой связи и поставщиков услуг.

Агентство национальной безопасности является ведомством Министерства обороны, отвечающим за электронную разведку по всему миру в интересах многих правительственных структур. Представители агентства, участвовавшие в заседаниях в качестве наблюдателей, заявили, что их единственный интерес в данном вопросе — обеспечение совместимости собственных защищённых телефонов правительства с новыми сотовыми аппаратами. По их словам, сотрудники АНБ получили прямое указание не участвовать в разработке стандартов; ряд инженеров, присутствовавших на заседаниях, действительно сообщил, что не ощущал никакого внешнего давления.

Однако другие инженеры, участвовавшие в процессе стандартизации, заявили, что присутствие агентства ощутимо довлело над более ранними техническими заседаниями на протяжении последних двух лет. «Я разговаривал с людьми, и они говорили: "АНБ не понравится то или это"», — сообщил один из членов комитета, пожелавший остаться анонимным.

Длинная рука АНБ

Эта дискуссия важна, по мнению защитников приватности, не только применительно к сотовым телефонам, но и ко многим другим возникающим технологиям, использующим радиосигналы — которые перехватить легче, чем информацию, передаваемую по обычным телефонным линиям. В их число входят беспроводные «персональные коммуникаторы» для передачи и приёма данных, а также портативные «ноутбуки».

Но этот спор наглядно показывает: даже по мере угасания холодной войны АНБ по-прежнему оказывает влияние на многие американские высокотехнологичные отрасли. Руководители ряда таких компаний утверждают, что агентство мешает их усилиям по завоеванию зарубежных рынков, вынуждая производить для иностранных покупателей продукты, отличающиеся от тех, что продаются внутри страны.

Это влияние агентство реализует через оценку заявок компаний на экспорт высокотехнологичной продукции. Критики утверждают, что в этой роли АНБ противодействует экспорту оборудования с передовыми системами шифрования, становящимися всё более необходимыми для современного бизнеса.

Покупатели найдут товар и в другом месте

Критики агентства говорят, что контролировать распространение технологий шифрования практически невозможно: потребители, которых отпугнут от покупки в США, просто пойдут за рубеж или украдут технологию.

«Идея о том, что можно контролировать эту технологию, смехотворна», — заявил Уильям Х. Нейком, вице-президент по правовым и корпоративным вопросам Microsoft Corporation.

Критики также указывают на абсурдность ситуации, при которой системы шифрования, используемые в широко распространённых программных продуктах, подвергаются государственному контролю наравне с оружием. «Идея о том, что наши продукты следует классифицировать как боеприпасы и обращаться с ними соответствующим образом, лишена всякого смысла», — сказал Нейком.

Правозащитники также оспаривают намерение комитета не публиковать алгоритм, лежащий в основе технологии шифрования. Традиционно криптографы считали, что лучший способ убедиться в работоспособности алгоритма — это опубликовать его для общедоступного тестирования.

Комитет заявил, что не раскроет формулу, поскольку не хочет давать преступникам возможность взломать код. Однако публикация формулы опасна лишь в том случае, если эта формула слабая, — утверждает Джон Гилмор, разработчик программного обеспечения из Силиконовой долины и защитник приватности. Если же формула сильная, её публикация и возможность для всех желающих попытаться её взломать лишь докажут её надёжность.

Тем не менее ряд инженеров, изучавших код, считают его несложным для взлома. Некоторые члены комитета признали, что понимали: АНБ никогда не позволит принять по-настоящему невзламываемый стандарт приватности.

«Циники за барной стойкой скажут вам, что от АНБ в принципе не получить ничего, что они не могли бы легко взломать», — сказал Питер Нёрс, председатель подкомитета по аутентификации и конфиденциальности стандартного комитета и инженер Hughes Network Systems.

Отрицание роли АНБ

Тем не менее ряд инженеров, работавших над техническим стандартом, настаивают на том, что агентство не оказывало никакого открытого влияния на его разработку. «Стандарт был основан на

технических выводах лучших экспертов Северной Америки», — сказал Джон Маринью, председатель стандартного комитета и руководитель AT&T. По его словам, комитет обращался к АНБ лишь за рекомендациями по соблюдению американского законодательства.

Он также сообщил, что новый стандарт обеспечит значительно более высокий уровень защиты частной жизни по сравнению с существующей системой сотовой связи. Сегодня, несмотря на то что прослушивание сотовых разговоров незаконно, многие люди модифицируют коммерческие радиосканеры для приёма частот, на которых передаются сотовые звонки.

Прослушивание ФБР оспаривается — 17 февраля 1992 г.

По материалам The Washington Post

ВАШИНГТОН. Сотовые телефоны и другие самые современные телекоммуникационные технологии серьёзно осложняют способность ФБР прослушивать телефонные переговоры подозреваемых в уголовных преступлениях, признают правоохранители. ФБР запрашивает 26,6 миллиона долларов на следующий год для обновления своих методов прослушивания. Обычно немногословные представители ФБР становятся ещё более молчаливыми, когда речь заходит об «источниках и методах» оперативной работы. Тем не менее изучение бюджетного запроса бюро на 1993 год даёт редкую возможность заглянуть в исследования ФБР в области электронной слежки и понять, какие тревоги вызывают у него новые технологии.

«Правоохранительные органы с запозданием реагируют на переход телекоммуникационной отрасли к новым технологиям», — говорится в бюджетном предложении ФБР, направленном в Конгресс. «Если электронное наблюдение должно оставаться инструментом правоохранительной деятельности, необходимо разработать поддерживающее его аппаратное и программное обеспечение».

К новым технологиям относятся цифровые сигналы и сотовые телефоны. Одновременно возросла передача компьютерных данных по телефону — данных, которые можно зашифровать с помощью общедоступных программ, отмечают отраслевые эксперты и государственные чиновники.

По данным администрации, пятилетняя исследовательская программа ФБР по созданию оборудования, совместимого с цифровыми телефонными системами, обойдётся в 82 миллиона долларов.

Усилия ФБР являются лишь частью более широкой исследовательской программы, финансируемой также из секретного разведывательного бюджета Пентагона, сообщили официальные лица на условиях анонимности.

Электронная слежка — включая телефонные прослушки и микрофоны, спрятанные в местах, которые посещают подозреваемые, — является ключевым инструментом расследования деятельности наркоторговцев, а также финансовых преступлений и организованной преступности.

Переговоры, записанные с помощью микрофонов, установленных ФБР в нью-йоркских заведениях клана Гамбино, составляют ключевой элемент обвинения в деле предполагаемого босса мафии Джона Готти, который сейчас судят за организацию убийства своего предшественника Пола Кастеллано.

Прослушка телефонов консультантов оборонной промышленности дала ключевые улики в ходе длительного расследования Министерства юстиции о мошенничестве при закупках для Пентагона — «Операция Ill Wind». Однако с появлением цифровых телефонных сигналов стало крайне сложно выделить отдельный разговор из тысяч, одновременно передаваемых вперемешку с компьютерными данными и изображениями, говорят представители отрасли.

«В старые времена нужно было всего лишь подсоединить пару зажимных клемм и наушник к нужному терминалу — и можно было слушать разговор», — рассказал Джеймс Сильвестр, сотрудник Bell Atlantic Network Services Inc. Но цифровая передача сигнала делает эту задачу значительно сложнее: разговоры разбиваются на бессвязный поток цифр и восстанавливаются лишь на другом конце линии.

Джон Д. Подеста, бывший советник подкомитета по праву и технологиям сенатского Комитета по судебной системе, считает, что ФБР и другие правоохранительные органы попросту стали жертвами технологической революции. На протяжении более пятидесяти лет базовые телефонные технологии оставались неизменными.

Nynex выходит в онлайн со справочниками — 20 февраля 1992 г.

Адам М. Гаффин (adamg@world.std.com) (Middlesex News, Фрамингем, Массачусетс)

Теперь можно листать «Жёлтые страницы» в электронном виде.

Вчера Nynex объявила о запуске онлайновых «Жёлтых страниц», доступных любому, у кого есть компьютер и модем — таким образом компания стала первой региональной телефонной компанией системы Bell, предложившей электронную базу данных «Жёлтых страниц». Судебное решение 1984 года, разделившее AT&T, запрещало подобные инициативы, однако в прошлом году это положение было отменено.

Сервис, по крайней мере на первых порах, будет предлагать только справочные записи, а не рекламу, — из почти трёхсот директорий Nynex, которая обслуживает большую часть Нью-Йорка и Новой Англии, за исключением Коннектикута.

Пользователи также смогут просматривать новости UPI и финансовую информацию, сообщил Курт Роесснер, президент Nynex Information Technologies — дочерней компании, которая будет управлять сервисом. В перспективе компания рассчитывает начать предлагать пользователям рекламу в формате «Жёлтых страниц», добавил Роесснер.

Для доступа к информации через сеть Minitel — французскую систему, пока не получившую широкого распространения в США, — пользователям потребуется специальное программное обеспечение. Nynex предоставит его бесплатно для MS-DOS, Macintosh, Apple II и Commodore, сообщил Роесснер.

По словам Роесснера, Nynex в конечном счёте надеется предложить этот сервис на других, более популярных компьютерных сетях. Minitel был выбран потому, что Nynex предоставляет свои «Жёлтые страницы» французским абонентам уже почти два года.

Nynex будет взимать 61 цент в минуту — 36,60 доллара в час, — как и французские пользователи. Роесснер, впрочем, признал, что это может оказаться больше, чем готовы платить американцы, и заявил, что компания рассмотрит возможность снижения тарифа.

CompuServe, крупнейшая в стране ориентированная на потребителей компьютерная сеть, берёт 12,80 доллара в час — но снижает этот тариф всего до 50 центов в час для тех, кто пользуется каталогом бесплатных номеров AT&T по всей стране.

Проект Nynex — очередной шаг в ряду инициатив крупных компаний по продаже информации потребителям через компьютер. Некоторые из них, например проект Knight-Ridder в середине 1980-х, потерпели сокрушительное фиаско. В прошлом году сама Nynex закрыла собственный информационный «шлюз», потеряв несколько миллионов долларов. CompuServe и ряд других онлайн-сервисов, по имеющимся данным, приносят существенную прибыль.

Информационные услуги телефонных компаний всегда вызывали споры. Противники, в том числе организации, представляющие издателей газет, утверждают, что несправедливо позволять компании, владеющей средствами распространения, ещё и самой оказывать услуги — распространённое сравнение: управление автострадой совмещается с владением транспортной компанией.

Роесснер, однако, выразил надежду на то, что телефонная компания сможет сотрудничать с другими потенциальными «поставщиками информации», а не конкурировать с ними. По его словам, он уже провёл переговоры с руководителями ряда газет, которые, по всей видимости, более готовы к совместным проектам с телефонной компанией, чем можно было бы предположить, судя по позициям их национальных организаций.

Гражданское жюри выносит решение против AT&T; по делу о нарушении патента — 9 февраля 1992 г.

Пол Декклман (United Press International/UPI)

НЬЮ-ЙОРК. Суд присяжных признал компанию American Telephone & Telegraph Company виновной в нарушении чужого патента на оборудование телефонной коммутации и присудил истцу 34,6 миллиона долларов, сообщил один из адвокатов.

AT&T настаивает на безосновательности иска и заявила, что обжалует это решение.

Шестеро присяжных федерального окружного суда в Мидленде (Техас) вынесли свой вердикт по завершении шести дней слушаний по иску, поданному против телекоммуникационного гиганта компанией Collins Licensing L.P. из Далласа.

Адвокат истца Джозеф Грир из чикагской фирмы Rolf Stadheim Ltd. допустил, что итоговая сумма может существенно вырасти с учётом процентов, начисленных с 1985 года. Представитель AT&T отверг такую возможность.

Решение жюри рассматривает судья федерального окружного суда Луций Бантон.

Грир утверждал, что цифровое центральное офисное коммутационное устройство AT&T 5ESS нарушает федеральный патент 1976 года на «коммутатор типа «время–пространство–время» (TST)», выданный на имя покойного Артура А. Коллинза.

Коллинз был основателем Collins Radio Co., ныне входящей в состав Rockwell International Inc. из Эль-Сегундо (Калифорния).

«Артур Коллинз был первопроходцем в области цифровых телекоммуникаций. Вердикт присяжных признаёт значительные исследовательские и опытно-конструкторские вложения мистера Коллинза и его важный технический вклад в развитие цифровой телефонии», — заявил Грир.

Подразделение AT&T Network Systems разработало это устройство в начале 1980-х годов для центрального офисного телефонного коммутационного оборудования, направляющего звонки на нужные АТС и номера.

Иск, поданный в декабре 1990 года, первоначально включал Southwestern Bell из Далласа в качестве соответчика. Однако эта часть дела была прекращена после того, как региональная телефонная компания заявила, что не нарушала патент, поскольку не производила спорное коммутационное оборудование, а лишь покупала его у AT&T.

AT&T, тем не менее, настаивает на недействительности патента Коллинза.

Пресс-секретарь Кёрт Уилсон сообщил, что Федеральное патентное ведомство в настоящее время рассматривает данный патент в рамках отдельного производства по запросу как AT&T, так и Collins Licensing. «Мы полагаем, что патент будет аннулирован и нам не придётся ничего платить», — сказал он.

Конкретных сроков для ожидаемого решения Патентного ведомства нет.

Уилсон также добавил, что даже если правительство признает патент действительным, AT&T не считает, что её оборудование использовало изобретение Коллинза, — и потому полагает, что патент не был нарушен.

«Жюри вынесло решение в нашу пользу по семи из восьми первоначальных пунктов иска», — сказал Уилсон, — «а по оставшемуся присудило им 34 миллиона долларов — в семьдесят раз меньше, чем они изначально требовали».

«Мы считаем этот иск полностью лишённым оснований, — заявил представитель компании. — Патент недействителен — и мы рассчитываем, что патентное ведомство с нами согласится».

Принят «Билль о правах» пользователя — 23 января 1992 г.

ТАМПА, ФЛОРИДА. Северо-американский форум по директориям (NADF) представил «Билль о правах пользователя», призванный решить вопросы безопасности и конфиденциальности, связанные с записями и листингами в предлагаемом кооперативном общедоступном справочном сервисе. Члены NADF также одобрили продолжение работ по экспериментальному пилотному проекту публичного каталога на своём восьмом ежеквартальном заседании.

«Билль о правах пользователя» отстаивает интересы индивидуального пользователя или его представителя и является ответом на проблемы, поступившие в NADF.

Завершилась разработка окончательных планов пилотного проекта по директории X.500, запуск которого запланирован на первый квартал текущего года. Пилот будет использован NADF для проверки своих технических соглашений по предоставлению общедоступного справочного сервиса в Северной Америке. Соглашения зафиксированы в постоянных документах и включают перечень предоставляемых услуг, схему каталога и требования к обмену информацией для унификации директории. Пилот также проверит работу X.500 в масштабном многовендорном окружении.

В пилоте участвуют все члены NADF: AT&T, Bell Atlantic, BellSouth Advanced Networks, Bellcore (представляет US West), BT North America, GE Information Services, IBM, Infonet, MCI Communications Corp., Pacific Bell, Performance Systems International, US Postal Service и Ziff Communications Co. На этом заседании к NADF присоединились Canada Post Corporation и DirectoryNet, Inc.

NADF был основан в 1990 году с целью объединения ведущих провайдеров обмена сообщениями в США и Канаде для создания общедоступного справочного сервиса на основе X.500 — рекомендации CCITT для глобального справочного сервиса. Форум проводит ежеквартальные встречи в формате совместной работы над операционными, коммерческими и техническими вопросами внедрения общесеверо-американского каталога с целью ускорить переход отрасли к глобальному каталогу X.500.

Заседание этого квартала было организовано IBM Information Network — сетью IBM с добавленной стоимостью, предоставляющей услуги в области сетей, обмена сообщениями, производительности и консалтинга.

Билль о правах пользователя (для записей и листингов в публичном каталоге)

Миссия Северо-американского форума по директориям — создание взаимосвязанных электронных каталогов, наделяющих пользователей беспрецедентным доступом к публичной информации. В целях решения важных вопросов безопасности и конфиденциальности Северо-американский форум по директориям представляет следующий «Билль о правах пользователя» для записей в публичном каталоге. Как пользователь, вы имеете право:

I. Не быть включённым в листинг.
II. На уведомление вас или вашего представителя о создании вашей записи.
III. Ознакомиться со своей записью.
IV. Исправить недостоверную информацию в своей записи.
V. Удалить конкретную информацию из своей записи.
VI. Рассчитывать на то, что ваши данные в публичном каталоге будут соответствовать законодательству США или Канады, регулирующему вопросы конфиденциальности и доступа к информации.
VII. Ожидать своевременного осуществления всех вышеперечисленных прав.

Область применения — Билль о правах пользователя

Северо-американский форум по директориям объединяет провайдеров, планирующих предложить кооперативный справочный сервис в Северной Америке. Это достигается путём объединения электронных каталогов с использованием комплекса международно разработанных стандартов, известных как серия CCITT X.500.

В данном контексте «Каталог» означает совокупность электронных директорий, администрируемых как провайдерами, так и частными операторами. Когда запись, содержащая информацию о пользователе, включается в Каталог, к ней возможен доступ, если только он не ограничен средствами защиты и обеспечения конфиденциальности.

Часть Каталога — Публичный каталог — содержит информацию, предназначенную для открытого распространения. Другие части Каталога, напротив, могут содержать сведения, не предназначенные для публичного доступа. Пользователь или его представитель может выбрать включение информации в публичный каталог, частную директорию или их сочетание. Например, пользователь может публично указать номер телефона или адрес электронной почты, а другие сведения отнести к конкретному частному использованию.

Билль о правах пользователя относится к Публичному каталогу.

Источник: NADF, январь 1992 г.

Phrack World News

Выпуск XXXVII / Часть третья из четырёх

Составили: Dispater & Spirit Walker

ЖАДНОСТЬ RBOC НАПРАВЛЕНА НА УНИЧТОЖЕНИЕ НАШИХ ДОСОК ОБЪЯВЛЕНИЙ!

Пользователи компьютеров видят угрозу в тарифах

5 ноября 1991 г.

Автор: Martin Rosenberg (Kansas City Star)

> *«Планы Southwestern Bell предвещают перемены — таковы их опасения»*

Ряд операторов компьютерных досок объявлений в штате Миссури заявляет, что им, возможно, придётся закрыть свои всё более популярные компьютерные сети, если Southwestern Bell Telephone Company добьётся повышения тарифов.

Southwestern Bell утверждает, что лишь пытается справедливо оценить свои услуги, переводя операторов досок объявлений с жилых тарифов на коммерческие. Компания добивается одобрения этих изменений у регуляторов штата Миссури.

Отраслевые эксперты считают, что эта ситуация может стать первым залпом в масштабной кампании телефонных компаний, направленной на изменение порядка оплаты электронных коммуникаций потребителями и бизнесом.

Эксперты говорят, что рядовые клиенты могут в один прекрасный день платить за пользование персональными компьютерами и модемами больше, чем за голосовую связь. А предприятиям, возможно, придётся платить больше за использование факсов.

Southwestern Bell отрицает, что пытается изменить какие-либо тарифы, кроме тех, что касаются небольшого числа клиентов, использующих передачу данных и подлежащих переводу на единый коммерческий тариф, более высокий, чем жилой.

Доски объявлений, которые нередко запускают прямо из дома, позволяют пользователям обмениваться сообщениями, советами и программами. Многие из них бесплатны, и операторы зачастую не получают никакого дохода. За последние несколько лет по всему штату их появились сотни.

Предложение Southwestern Bell направлено только против тех, кто организовал доску объявлений на своём персональном компьютере. Пользователей, которые лишь обращаются к доске объявлений по телефонной линии, оно не затрагивает.

Это предложение появилось в то время, когда планы телефонных компаний по оказанию информационных услуг вышли на первый план.

Верховный суд США уже открыл дорогу семи региональным телефонным компаниям, включая Southwestern Bell, к предоставлению информационных услуг. Эти услуги со временем смогут

конкурировать с электронными досками объявлений, газетами и операторами баз данных, такими как CompuServe Inc. и Prodigy Services Co. (CompuServe принадлежит H&R Block Inc. из Канзас-Сити).

По данным отраслевых источников, доходы от информационных услуг, предоставляемых по телефону в США, в прошлом году составили около 750 миллионов долларов и, по прогнозам, вырастут до 2 миллиардов долларов в 1992 году.

Предложение Southwestern Bell, в случае одобрения, должно вступить в силу в середине ноября.

По словам Уильяма Бейли, районного менеджера компании по тарифному регулированию в Миссури (Сент-Луис), операторы досок объявлений работают как предприятия.

«Некоторые клиенты на жилых линиях более правомерно должны находиться на коммерческих линиях», — сказал Бейли.

Бейли сообщил, что изменения затронут и нынешних коммерческих клиентов. Им разрешат перейти на единый коммерческий тариф (33,55 доллара в месяц в метро Канзас-Сити) и избежать более высокого тарифа «услуги информационного терминала» (в настоящее время 43,60 доллара в месяц).

Southwestern Bell предпринимала аналогичную попытку перевести доски объявлений на коммерческие тарифы в Техасе. Впоследствии компания решила разрешить бесплатным доскам объявлений, использующим не более трёх линий, сохранить жилые тарифы.

По словам Бейли, это было «колоссальной ошибкой». Телефонные компании не могут контролировать, взимает ли доска объявлений деньги с пользователей, добавил он.

Многие операторы досок объявлений в Канзас-Сити возмущены предложением Southwestern Bell.

«Если они начнут брать коммерческие тарифы, часть досок объявлений закроется», — заявил Lanny Conn, оператор бесплатной доски объявлений SOLO-Quest.

Bill Hirt, оператор доски объявлений Amiga Central для пользователей компьютеров Amiga, сказал, что закроет её, если с него возьмут коммерческий тариф. Его доска объявлений тоже бесплатна.

По его словам, сейчас к его доске объявлений обращаются около 200 пользователей персональных компьютеров — некоторые из Австралии и Швеции.

Conn и Hirt выступают в роли пресс-секретарей Ассоциации сисопов Большого Канзас-Сити (Greater Kansas City SysOps Association), объединяющей около 22 досок объявлений. (SysOps означает «системные операторы».) По оценке Hirt, в городе около 100 досок объявлений; большинство созданы как хобби.

Адвокат Robin Martinez, представляющий интересы ассоциации, заявил, что предложение Southwestern Bell ударит по первопроходцам информационной эпохи.

«Те, кто ведёт доски объявлений, и те, кто ими пользуется, — это передовой отряд информационной эпохи», — сказал он.

По его словам, Southwestern Bell хочет проредить ряды провайдеров досок объявлений, чтобы у её собственных услуг было меньше конкурентов.

«В определённой мере они пытаются захватить контроль над информационными услугами», — заявил Martinez.

Бейли отрицал связь между предложениями своей компании и её собственными планами в области информационных услуг.

«Мне никто сверху не указывает, что делать», — сказал он. — «Я на самом деле не знаю, что моя компания намерена делать в части информационных услуг».

Однако Уильям Дегнан, консультант по телекоммуникациям из Остина (Техас), заявил: «Большинство этих ребят (из досок объявлений) занижают цены на услуги, которые Southwestern Bell хотела бы предоставлять в более широком масштабе».

Дегнан консультировал группу техасских операторов досок объявлений, выступавших против попыток Southwestern Bell брать с них коммерческие тарифы.

«Я думаю, Southwestern Bell обеспокоена тем, что не сможет продать то, что другие раздают бесплатно», — сказал Дегнан.

Марта Хогерти, общественный советник по защите прав потребителей в Миссури, изучив заявку Southwestern Bell, сказала: «Похоже, что любой, у кого есть модем, должен будет платить по коммерческому тарифу».

Большинство региональных компаний Bell сейчас разрабатывают стратегии предоставления информационных услуг.

Говард Андерсон, президент Yankee Group of Boston, сказал, что телефонные компании вскоре могут попытаться ввести для клиентов повременной тариф на передачу данных. При такой системе ежемесячные расходы на передачу данных будут расти пропорционально времени подключения в течение месяца — как счётчик такси.

Переход на повременную оплату был бы разумен и позволил бы телефонным компаниям увеличить доходы по мере роста нагрузки и расходов, считает он.

Андерсон отметил, что средний жилой клиент пользуется телефоном 21 минуту в день, тогда как клиент с персональным компьютером и модемом занимает телефонную линию в среднем 62 минуты в день.

Андерсон предположил, что телефонные компании могут предложить клиентам высокоскоростную передачу данных по тарифу, превышающему стоимость голосовой связи. Использование сверх фиксированного числа часов будет увеличивать ежемесячный телефонный счёт.

Чтобы стимулировать переход на новую линию, телефонные компании могут намеренно ухудшить качество стандартных линий, чтобы они не могли чисто передавать электронные данные, сказал Андерсон.

Бейли с этим не согласен: по его словам, у Southwestern Bell нет планов по введению повременной тарификации для голосовой или передачи данных.

И, добавил он: «Мне не известно ни о каких планах по ухудшению качества нашего сервиса с целью перевода клиентов с одной услуги на другую».

Тариф SW Bell назван угрозой для компьютерных досок объявлений

18 ноября 1991 г.

Автор: Robert Sanford (St. Louis Post-Dispatch)

Предложение Southwestern Bell Telephone Co. пересмотреть тариф на пользование телефоном вызвало протесты владельцев персональных компьютеров, использующих телефонные линии для работы служб досок объявлений для других владельцев компьютеров.

Операторы досок объявлений утверждают, что их члены в подавляющем большинстве управляют досками объявлений как хобби, а не как бизнесом. И они настаивают на том, что изменение, предложенное Bell, является частью усилий телефонной компании заставить их платить по коммерческим тарифам за телефонную линию, а не по жилым.

Доски объявлений — это компьютеры с модемами, к которым могут подключаться другие компьютеры с модемами. «Доски объявлений» содержат информацию, которую можно передавать на другие компьютеры, — информацию любого рода, от кулинарных рецептов до игр, советов по автомобилям и программирования.

Пользователи досок объявлений, занимающихся этим как хобби, имеют общие интересы, пояснил Jim Harre, координатор сети досок объявлений Network 100. «Можно сказать, что пользователи досок объявлений чем-то похожи на радиолюбителей. Это люди, использующие компьютеры для общения. Они выполняют функцию, схожую с доской объявлений в супермаркете. Они распространяют информацию.

Операторы видят в предложении Bell угрозу для всех досок объявлений. Рост расходов просто вынудит некоторые любительские доски прекратить существование».

По словам Боба Шмедака, системного оператора (или «сисопа», как они себя называют), список нескольких сетей в районе Сент-Луиса насчитывает около 250 досок объявлений. По оценкам, столько же их может быть в районе Канзас-Сити. Таким образом, по всему штату их несколько сотен. В мире насчитывается 16 000 досок объявлений.

Хотя тарифное предложение вывело на первый план в дискуссиях среди сисопов Миссури вопрос о жилых и коммерческих тарифах, само предложение не предполагает никакого изменения жилых тарифов. Предложение подразумевает, что некоторым пользователям иного вида услуги под названием «Услуга информационного терминала» (Information Terminal Service) следует разрешить перейти на единый коммерческий тариф.

В общем, тариф ITS составляет 43,65 доллара, единый коммерческий тариф — 33,55 доллара, а жилой — 11,35 доллара.

По словам Уильяма Бейли, районного менеджера Southwestern Bell по тарифному управлению в Миссури, в действующих тарифах телефонной компании есть определение, согласно которому линия, используемая «скорее в деловых, нежели в жилых целях», должна оплачиваться по коммерческому тарифу.

«Деловой характер» может считаться установленным, если линия рекламируется каким-либо образом, пояснил он.

Однако сисопы говорят, что рост популярности досок объявлений объясняется тем, что владельцы компьютеров подключали модемы к домашним персональным компьютерам и начинали общаться с другими по компьютеру, пользуясь жилой линией. Они всегда считали доски объявлений хобби. Хотя за доступ к некоторым доскам объявлений может взиматься плата, никто на них не зарабатывает, заявили они.

Бейли сообщил, что телефонная компания не знает, сколько сисопов пользуется жилыми линиями, и у компании нет официального плана по выяснению того, как используются линии.

Бейли присутствовал на встрече в Канзас-Сити, в которой также участвовал Джон Ван Эшен, помощник управляющего по телекоммуникациям Комиссии по общественному обслуживанию Миссури, и около 150 сисопов.

Встречу впоследствии охарактеризовали как временами «напряжённую», а её итогом стало то, что сисопы и телефонная компания остались при своих мнениях. Пользователи настаивали на том, что доски объявлений являются общественной службой, распространяющей информацию, и что рост тарифов может вынудить некоторые из них закрыться.

«Пользователи хотят, чтобы с них брали по жилому тарифу», — сказал Ван Эшен. — «Путь к этому — подать официальную жалобу на Bell. Это может привести к письменным показаниям и слушанию».

По его словам, сейчас на рассмотрении находится жалоба с обвинением в том, что Bell хотела перевести тариф пользователей с жилого на коммерческий, а на встрече речь шла о каких-то судебных действиях.

Ван Эшен сообщил, что PSC продолжает изучать вопрос и пока не выработала никакой рекомендации. Дата вступления в силу любого решения — 15 декабря.

Некоторые сисопы, в том числе Харре, высказывают предположение, что телефонная компания может быть заинтересована в сокращении числа досок объявлений, поскольку сама планирует войти в бизнес информационных услуг и может рассматривать доски объявлений как потенциальных конкурентов. Верховный суд недавно поддержал решение, разрешившее компаниям Baby Bell войти в сферу информационных услуг.

Бейли заявил, что не знает, что компания планирует делать в сфере информационных услуг.

Телефонные компании прицеливаются на повышение тарифов для BBS

18 ноября 1991 г.

Автор: Steve Higgins (PC Week, стр. 173)

Возможно, BBS на минимальном бюджете уйдут в прошлое, если крупные телефонные компании добьются своего.

Региональные операционные компании — такие как U.S. West Inc., Southwestern Bell Corp. и Southern Bell Telephone & Telegraph Co. — маневрируют с целью повышения расходов для более чем 40 000 операторов dial-in досок объявлений в Соединённых Штатах, по утверждению самих операторов.

Службы досок объявлений (BBS), предлагающие всё — от технической поддержки до дискуссий об экзотических птицах, — могут быть сильно подорваны или полностью уничтожены возросшими затратами на подключение и ежемесячными платежами за линию, которые в ряде случаев удвоятся.

«Если телефонные компании повысят эксплуатационные расходы, нам придётся перекладывать их на пользователей», — сказал Кевин Беренс, оператор Aquilla BBS, дистрибьютора шэрвэра в Авроре, Иллинойс.

Хотя попытки поднять ставки до сих пор отражались мощной оппозицией пользователей BBS, предложение Southwestern Bell, способное облегчить компании преследование операторов BBS, платящих по низким жилым тарифам, рассматривается в этом месяце.

«У нас есть тариф для коммерческих клиентов. Операторы служб досок объявлений должны платить по этому тарифу», — заявил Дэвид Мартин, пресс-секретарь Southwestern Bell в Сент-Луисе. — «У нас пока нет организованной программы по переводу провайдеров досок объявлений на этот тариф».

Зона деятельности компании охватывает пять штатов на Среднем Западе и на юге США, однако предложение вступило бы в силу только в Миссури. В случае одобрения регуляторами Миссури оно может более чем вдвое увеличить ежемесячный тариф для операторов систем досок объявлений.

Коммерческие тарифы на линии передачи данных в среднем составляют от 18 до 45 долларов в месяц по стране, тогда как жилые тарифы — от 7 до 20 долларов в месяц.

Кроме того, решение федерального судьи в октябре, освобождающее телефонные компании и позволяющее им вести собственные службы досок объявлений, может сделать повышение

тарифов ещё более соблазнительным. По мнению аналитиков, из-за этого федерального решения интерес телефонных компаний к повышению расходов для операторов BBS выходит за рамки простого извлечения дополнительных доходов.

«Телефонные компании хотят создать электронные "Жёлтые страницы"... [что] само по себе [не является] плохой идеей», — сказал Джек Рикард, редактор Boardwatch, ежемесячного журнала для пользователей BBS, издаваемого в Лейквуде, Колорадо. — «Но судя по всему, в головах у них — задавить всё остальное».

КОНКУРЕНТОВ ХВАТАЕТ

Если телефонные компании запустят собственные онлайн-сервисы, им придётся столкнуться с колоссальной установленной базой конкурентов. Помимо гаражных BBS-операций, по данным отраслевого информационного бюллетеня Soft*letter из Уотертауна, штат Массачусетс, почти 40 из 100 крупнейших компаний по производству PC-программного обеспечения используют низкую стоимость и широкий охват досок объявлений для обеспечения поддержки клиентов.

«Мы только сейчас начинаем видеть, как бизнес использует службы досок объявлений», — сказал Джим Харрер, президент и генеральный директор Mustang Software Inc., поставщика коммуникационного программного обеспечения и оператора служб досок объявлений из Бейкерсфилда, Калифорния. — «Для них это было бы ударом, если бы [тарифы] встали на пути».

Если ситуация сложится именно так, некоторые системные операторы, по мнению наблюдателей, могут попытаться обойти новый тариф, маскируя свои операции под личные телефонные линии. По имеющимся сведениям, некоторые операторы уже прибегают к такой тактике.

«Я слышал об одном парне, который пытался убедить телефонную компанию, что у него пятеро детей», которым нужны отдельные телефонные линии, рассказал Харрер из Mustang Software.

Рост расходов может также затронуть крупных операторов досок объявлений — таких как Prodigy Services Co. и CompuServe Inc., — особенно в сочетании с появлением досок объявлений, поддерживаемых телефонными компаниями.

«Их это из бизнеса не выбьет», — сказал Рикард из Boardwatch, — «но [Prodigy и CompuServe] тоже пострадают».

Политика выжженной земли Southwestern Bell в отношении досок объявлений

Декабрь 1991 г.

Взято из журнала BOARDWATCH Magazine

На протяжении всей дискуссии о том, позволить ли региональным телефонным компаниям Bell (RBOC) войти в информационный бизнес, противники предупреждали, что RBOC воспользуются своим монопольным положением для нечестного устранения конкуренции. И на протяжении всей этой дискуссии RBOC благочестиво отрицали, что когда-либо пойдут на антиконкурентные действия. Судья Грин в чётких и недвусмысленных выражениях предупреждал, что история компаний говорит об обратном, и на протяжении семи лет после разукрупнения раз за разом отказывал им в праве конкурировать в сфере информационных услуг.

Потратив миллионы из средств плательщиков тарифов на лоббирование и апелляции во всех ветвях власти, RBOC в конечном счёте нашли апелляционный суд, который предписал судье Грину пересмотреть свою позицию.

Вынужденный снять запрет на информационный контент, Грин приостановил вступление своего решения в силу, ожидая апелляций со стороны оппозиции. Однако 7 октября апелляционный суд отменил и эту приостановку, открыв компаниям Bell свободу в одночасье запустить собственные онлайн-сервисы.

Чернила на документе ещё не успели высохнуть, когда последовал первый удар. Southwestern Bell Telephone, имевшая за плечами историю преследования BBS с середины 80-х, вырвалась вперёд первой. В октябре она подала заявку на пересмотр тарифа, требуя, чтобы ВСЕ электронные доски объявлений, будь то коммерческие или любительские, были классифицированы как услуги информационных терминалов — причём не только обязаны платить по более высоким коммерческим тарифам, но и лишены права пользоваться существующими тарифами на коммерческую измеряемую услугу для снижения своих телефонных счетов. Тариф был подан 7 октября 1991 года как предлагаемая поправка к Местному тарифу на обмен в Миссури, P.S.C. Mo. No. 24 и P.S.C. Mo. No. 35, Общий тариф на обмен, раздел 17, Правила и нормы, применяемые ко всем договорам с клиентами.

В настоящее время базовый тариф за линию для предприятий в районе Канзас-Сити составляет 33,55 доллара в месяц — примерно вдвое больше жилого тарифа. А тариф информационного терминала и того выше — 43,60 доллара в месяц. Хотя модификация тарифа специально направлена против операторов BBS, формулировки тарифа, по всей видимости, охватывают всех, кто пользуется модемом или факсом на телефонной линии.

У Southwestern Bell давняя история вражды с операциями досок объявлений. В 1988 году компания анонсировала собственный шлюзовой сервис SOURCELINE в Хьюстоне и в октябре того же года разослала сотням хьюстонских досок объявлений письма с требованием платить по коммерческим тарифам за жилые телефонные линии. Группа местных системных операторов, объединившихся под флагом COSUARD, обратилась в Комиссию по коммунальным услугам штата Техас с обвинениями в хищнических практиках, антиконкурентных действиях и дискриминации любительского BBS-сообщества.

В январе 1991 года Southwestern Bell, одновременно с провалом собственного шлюзового сервиса SOURCELINE, урегулировала спор с группой. Все BBS в районе Хьюстона, работающие не более чем на трёх линиях и не претендующие на абонентскую поддержку, классифицированы как любительские BBS и по-прежнему имеют право на жилую телефонную услугу.

Любительские доски объявлений — вот в чём суть вопроса. Большинство коммерческих и подписных систем досок объявлений уже платят коммерческие тарифы за телефон. Однако большинство выбирают тип коммерческой классификации, именуемой «полностью измеримой услугой». Практически все RBOC предлагают сниженный базовый тариф в обмен на право измерять местные звонки — как правило, по два-три цента за минуту. Поскольку большинство досок объявлений делают мало исходящих звонков — основная активность входящая — полностью измеримая услуга, даже в коммерческой классификации, обходится всего на несколько долларов дороже жилой телефонной услуги. SWB своей заявкой, в случае одобрения, в одночасье фактически удвоила бы телефонные расходы любой BBS в штате Миссури.

Системные операторы Канзас-Сити объединились, создав некоммерческую организацию Greater Kansas City Sysops Association (GKCSA), чтобы бороться с предложенными изменениями. На публичных слушаниях 14 ноября в Канзас-Сити около 150 операторов и пользователей явились на протест, и MPSC согласилась отложить введение нового тарифа до 15 декабря. SWB изначально намеревалась ввести тарифы с 15 ноября.

По словам адвоката GKCSA Робина Мартинеса, группа намерена подать юридическое ходатайство с просьбой к MPSC постановить, что всем любительским BBS, расположенным в жилых помещениях, разрешается более низкая классификация — жилой тариф. В своём ходатайстве GKCSA утверждает, что Southwestern Bell Telephone действует хищнически и антиконкурентно,

стремясь устранить любую воспринимаемую конкуренцию своим собственным планируемым информационным услугам в Миссури.

Президент GKCSA Скотт Лент предсказывает, что если Southwestern Bell добьётся своего, это положит конец бесплатным любительским BBS в штате — чего телефонная компания как раз и добивается. И он предсказывает, что если SWB победит в Миссури, другие RBOC не заставят себя долго ждать и введут собственные тарифы, чтобы устранить конкуренцию в виде бесплатных информационных услуг, которые предоставляют бесплатные BBS.

Уильям Бейли, районный менеджер компании по тарифному управлению в Миссури, не приносит никаких извинений за подход компании. На встрече в Канзас-Сити он признал, что повышение тарифа не окажет существенного влияния на доходы компании, но отрицал, что оно каким-либо образом связано с выходом компании на рынок информационных услуг, и уверил, что ему не известно, каковы планы компании в сфере информационных услуг. Он заявил, что их единственная цель — «справедливость»: пользователи модемов занимают линию дольше, чем голосовые абоненты, и должны платить больше. Он не смог прокомментировать совпадение — SWB подала заявку на тариф в течение недели после решения апелляционного суда.

Телефонная компания взвинчивает плату за компьютер, вызывая широкое возмущение

8 декабря 1991 г.

Автор: Christine Bertelson (St. Louis Post-Dispatch)

> *«Расходы для электронных досок объявлений могут утроиться»*

Для Барбары Клементс электронная доска объявлений, которую она держит на домашнем компьютере на юге округа Сент-Луис, — это гораздо больше, чем хобби. Это её единственное окно в мир.

Клементс, 43 года, страдает тяжёлой формой детского церебрального паралича, которая не позволяет ей ходить или пользоваться руками. Её невнятная речь труднопонятна для многих людей при живом общении и абсолютно неразборчива по телефону, говорит она сама.

Но, сидя за клавиатурой и пользуясь «головной указкой», Клементс может работать с модемом и компьютером, общаясь с растущей сетью других компьютерных любителей.

Компьютерная сеть дала ей свободу и общественную жизнь, которыми она не готова жертвовать.

«Шесть лет назад, до того как я обзавелась модемом, я была законченным затворником», — сказала Клементс в интервью у неё дома.

«Моя частная система доски объявлений — это строго для социальной жизни, ради моего душевного равновесия. На любой доске объявлений я равноправный человек, потому что люди не видят моей инвалидности и не слышат моей невнятной речи. Это облегчает заведение друзей».

Клементс — одна из сотен компьютерных любителей по всему штату, на которых повлияет предложение Southwestern Bell Corp. взимать с операторов досок объявлений коммерческий, а не жилой тариф за телефонные подключения к их терминалам.

Предложение затронет не только инвалидов, таких как Клементс, воспринимающих сеть как спасательный круг.

Доски объявлений стали всё более популярны среди компьютерных любителей в широких массах населения — как способ обмениваться информацией о компьютерах и различных других

интересах.

Их пользователи — от подростков-«компьютерных хакеров» до взрослых, обменивающихся рецептами, и одиноких людей, ищущих знакомств.

За последние несколько лет по всему Миссури были добавлены сотни электронных досок объявлений. В районе Сент-Луиса их уже более 200. Предлагаемое повышение тарифа затронет только операторов досок; сотни других, кто звонит на них, под его действие не подпадут.

Компания объявила о своём плане несколько недель назад. Ожидается, что вопрос вскоре будет передан в Комиссию по общественному обслуживанию Миссури, которая регулирует коммунальные тарифы в штате.

Телефонная компания утверждает, что лишь пытается справедливо оценить свои услуги, указывая на то, что компьютерная болтовня нередко длится дольше, чем телефонные звонки. По словам пресс-секретаря компании, занятость телефонных линий увеличивает эксплуатационные расходы Bell.

Робин Мартинес, адвокат из Канзас-Сити, представляющий интересы местных компьютерных любителей, сказал, что намерен на этой неделе подать жалобу с требованием провести публичные слушания по данному вопросу.

Уильям Бейли, районный менеджер Southwestern Bell по тарифному управлению в Миссури, заявил, что компания считает электронные доски объявлений, которыми пользуются такие люди, как Клементс, предприятиями.

«Если клиент ведёт себя как бизнес — размещает рекламу и т.п. — мы можем взимать коммерческий тариф», — сказал Бейли. — «Мы берём коммерческие тарифы с клубов и братств. Одна из причин, по которым мы оцениваем бизнес дороже, — это поддержание жилых тарифов на низком уровне».

Электронные доски объявлений, часто работающие из домов, служат местом встречи, говорят их операторы.

Многие бесплатны, и операторы нередко не получают от них никакого дохода.

У каждой есть своё название, отражающее личность её «сисопа» или системного оператора. Клементс назвала свою — как нельзя более точно — «Barb's Outlook Window» («Обзорное окно Барб»).

Один из электронных знакомых Клементс — Джон Броули-младший из Эврики, известный в сети под ником «The Wanderer» («Странник»).

Они познакомились три месяца назад на её доске объявлений и теперь регулярно общаются по компьютеру на темы от погоды до ДЦП Клементс и до идей Броули о влиянии квантовой механики на религиозные концепции.

Броули опасается, что предложение Bell фактически лишит Клементс голоса. Но, добавил он, здесь есть и более широкий вопрос. Введение повышенных тарифов ограничит свободный поток информации, считает он.

Бейли заявил, что на кону стоит не свобода слова, а лишь определение того, что является бизнесом, а что нет.

Верховный суд США недавно открыл путь региональным телефонным компаниям, включая Southwestern Bell, к предоставлению информационных услуг, способных со временем конкурировать с электронными досками объявлений, газетами и операторами баз данных.

По данным отраслевых источников, доходы от информационных услуг, предоставляемых по телефону по всей стране, в прошлом году оценивались в 750 миллионов долларов и

прогнозируются на уровне 2 миллиардов долларов в следующем году.

Мартинес, адвокат пользователей досок объявлений из Канзас-Сити, подсчитал, что Southwestern Bell может ежегодно дополнительно получать 8 миллионов долларов, взимая обсуждаемые коммерческие тарифы. Бейли эту цифру не подтвердил.

После того как компьютерные любители подадут официальную жалобу в государственную комиссию, у Bell будет 30 дней для ответа. Если вопрос не будет урегулирован в частном порядке, комиссия может провести публичные слушания, сообщил пресс-секретарь ведомства Кевин Келли.

Тем временем Клементс сказала, что написала в компанию и готова дать показания на слушаниях.

Соглашение между телефонной компанией и сисопами BBS Миссури близко

14 февраля 1992 г.

Взято из Newsbytes

По сообщениям из Канзас-Сити, телефонная компания Southwestern Bell близка к соглашению с местными операторами компьютерных систем досок объявлений в споре о переводе BBS на коммерческие тарифы. Основой пакта, по всей видимости, станет формулировка в новом тарифном плане.

На этой неделе информационный бюллетень Communications Daily процитировал адвоката Робина Мартинеса, представляющего интересы сисопов: по его словам, предлагаемое соглашение предусматривает освобождение BBS от коммерческих тарифов при соблюдении определённых условий.

Одно из условий — доски объявлений должны находиться в жилых помещениях. Освобождённые BBS также не должны взимать плату за доступ, не должны размещать рекламу и иметь менее пяти телефонных линий.

По словам Мартинеса, последним камнем преткновения в соглашении остаётся выработка приемлемого определения понятия «BBS» для текста тарифа.

Заключительные замечания

В ситуации с Миссури / Southwestern Bell ещё предстоит урегулировать ряд проблем, а тем временем аналогичные проблемы возникают с компанией C&P (Bell Atlantic) Telephone в Вирджинии и US West Telephone в Орегоне.

Наши электронные права и свободы, которыми мы пользовались столь многие годы, оказались под угрозой из-за жадности региональных телефонных компаний Bell.

Поддержите наш Конгресс, поддержав законопроекты S 2112 и HR 3515!

Подробности — в Phrack 38.

Phrack World News

Автор: Составлено Dispater & Spirit Walker

Выпуск XXXVII / Часть четвёртая из четырёх

Компьютерный шпионаж: может ли Интернет нас скомпрометировать?

Декабрь 1991 г. Извлечено из Security Awareness Bulletin

Распространение компьютерных сетей, объединяющих учёных и их исследовательские учреждения, существенно усложняет любые попытки выявить советский научный шпионаж. К примеру, зарубежные поездки могут утратить прежнее значение по мере того, как компьютеры становятся всё более непосредственно взаимосвязанными, позволяя учёным из любой точки мира общаться друг с другом — а в ряде случаев и получать доступ к информации в базах данных западных академических и оборонных учреждений.

Эта возможность существует уже некоторое время, однако в 1989 году СССР сделал важный шаг к расширению охвата и доступности связи, подав заявку (совместно с Польшей, Чехословакией, Венгрией и Болгарией) на подключение к Европейской академической исследовательской сети (EARN). Одобрение заявки в апреле 1990 года открыло советским и восточноевропейским пользователям доступ, далеко выходящий за рамки простого соединения с компьютерами по всей Западной Европе. Через EARN Советский Союз получал бы подключение к Internet — американской сети, обслуживающей оборонные, исследовательские и академические организации по всему миру.

В тенденции к компьютерной взаимосвязанности заложен целый ряд угроз. Наиболее очевидна возросшая лёгкость, с которой советский агент может обсуждать профессиональные вопросы с западными специалистами, работающими над аналогичными проектами. Пользователь также может разослать общий запрос на информацию по любой теме, и далеко не всегда будет очевидно, что запрашивающий работает на СССР. Кроме того, Академия наук СССР способна использовать компьютерную сеть для рассылки общих приглашений на конференции — в надежде, что ответы позволят выявить незадействованные исследовательские учреждения или отдельных учёных, которых впоследствии можно будет разрабатывать в целях получения конкретной информации.

Доступ к данным, хранящимся в компьютерах, подключённых к сети, как правило, контролируется таким образом, что конкретные файлы могут читать лишь авторизованные пользователи. Тем не менее Советы уже продемонстрировали, что изобретательный «хакер», подключившись к компьютерам с секретными данными, способен обходить средства контроля доступа, чтобы прочитать эту информацию. В деле «Ганноверского хакера», например, советские спецслужбы использовали западногерманских компьютерных экспертов для доступа к засекреченным американским базам данных, получив как программное обеспечение, так и сведения оборонного характера.

Война с войной номеров

27 ноября 1991 г. Автор: Эдмунд Л. Эндрюс (New York Times). Особая благодарность: Dark Overlord

ВАШИНГТОН — На волне всеобщего раздражения телефонными продажами Конгресс одобрил и направил президенту Бушу законопроект, запрещающий использование автоматических устройств дозвона, воспроизводящих заранее записанные сообщения в жилых домах. Законопроект также предусматривает возможность для потребителей блокировать звонки от живых продавцов, внеся свои имена в список «не звонить».

Законопроект, принятый путём голосования голосом как в Палате представителей, так и в Сенате, получил поддержку как демократов, так и республиканцев, некоторые из которых рассказали о собственных неприятностях с нежелательными коммерческими звонками.

Хотя Белый дом выразил озабоченность тем, что расценивает как излишнее регулирование, президент не угрожал наложить вето на законопроект.

Законопроект, объединяющий положения нескольких отдельных мер, ранее принятых обеими палатами Конгресса, запрещает использование автодозвонщиков для звонков большинству частных абонентов. Немногочисленные исключения составляют случаи, когда человек явно выразил согласие принимать такие звонки, либо когда автодозвонщик применяется для оповещения людей об экстренной ситуации.

При использовании автодозвонщиков для обзвона предприятий им будет запрещено набирать более двух номеров одной организации.

Многие штаты уже приняли законы, ограничивающие использование автодозвонщиков; около дюжины штатов запрещают их полностью, ещё около двух дюжин ограничивают их применение различными способами.

Законы штатов, однако, не препятствуют компании использовать автодозвонщик в нерегулируемом штате для звонков в дома, находящиеся в штате с ограничениями.

В попытке обуздать телемаркетинг с участием живых торговых представителей законопроект обязывал бы Федеральную комиссию по связи либо контролировать создание общенационального списка «не звонить», либо издать правила, обязывающие компании вести собственные списки.

Законопроект позволял бы людям, внёсшим свои имена в такой список, подавать иски в мировые суды против компаний, продолжающих звонить. Иски могли предусматривать взыскание до 500 долларов за каждый нежелательный звонок, но не более трёх звонков от одной компании.

Наконец, законопроект запрещал бы незапрошенные «факс-спам» сообщения — рекламу, передаваемую на факсимильные аппараты.

«Это победа для осаждённых потребителей, которые в этом законе получили декларацию независимости от мусорных факсов и мусорных звонков», — заявил конгрессмен Эдвард Дж. Марки, демократ от Массачусетса, главный спонсор законопроекта в Палате представителей.

Компании, производящие или использующие автодозвонщики, угрюмо предрекали, что законопроект разорит их и сильнее всего ударит по мелким рекламодателям.

«Думаю, это нас добьёт», — сказал Марк Андерсон, владелец Leshoppe Corp. из Нового Орлеана, использующей около 160 машин для клиентов, продающих всё — от средств для загара до медицинского страхования. — «Люди не понимают, что электронным маркетингом пользуется немало семейных предприятий, и весьма успешно».

Рэй Колкер, президент Kolker Systems — крупнейшего производителя автодозвонщиков, — разделил эту точку зрения. «Принятие этого законопроекта свидетельствует о том, что Конгресс не так уж печётся об экономике, как им кажется, — сказал он. — Это уничтожит многомиллиардный бизнес».

Телемаркетинг резко вырос в последние годы — по мере падения стоимости международной телефонной связи и по мере того, как потребителей стали заваливать горами каталогов, которые

они не читают, и конвертами, которые они не вскрывают.

По оценкам Конгресса, объём товаров и услуг, проданных через все формы телефонного маркетинга, вырос примерно с 72 миллиардов долларов в 1982 году до 435 миллиардов в 1990 году. В целом, по различным оценкам, в той или иной сфере телефонного маркетинга занято около 300 000 человек.

Автодозвонщики, каждый из которых способен совершать около 1500 звонков в день, стали одной из наиболее эффективных, но и наиболее нелюбимых форм телемаркетинга. По некоторым оценкам, одновременно эксплуатируется 20 000 автодозвонщиков, способных совершать более 20 миллионов звонков в сутки.

На слушаниях по этому вопросу в начале года сенатор Дэниел К. Иноуэ, демократ от Гавайев, с раздражением отметил, что его вызвали к телефону лишь для того, чтобы он услышал записанное рекламное сообщение о выигрыше поездки на Гавайи.

Законодательство не встретило противодействия со стороны всех компаний, занятых телефонными продажами. Многие маркетинговые эксперты давно осуждали использование автодозвонщиков как инструмента продаж, утверждая, что они контрпродуктивны, поскольку вызывают больше раздражения, чем коммерческого интереса.

Ассоциация прямого маркетинга — отраслевое объединение — выразила осторожную поддержку законодательству и уже ведёт собственный добровольный список «не звонить».

Помимо простого раздражения людей дома, автодозвонщики, как известно, забивают телефонные пейджинговые сети и коммутаторы больниц и университетов, а также звонят на сотовые телефоны.

Тем не менее остаётся неясным, насколько эффективными окажутся списки «не звонить» на практике, поскольку два варианта, доступных FCC, существенно различаются.

Национальный список под управлением правительства эффективно защищал бы потребителей от всех нежелательных коммерческих звонков. Однако требование к каждой компании вести собственный список было бы значительно более ограниченным: людям, возможно, пришлось бы звонить в каждую компанию, чтобы попасть в её индивидуальный список.

Сотрудники Конгресса отметили, что законопроект, принятый в среду, настоятельно подразумевал, что FCC должна создать собственный список, поскольку содержит два страницы подробностей о том, как именно следует формировать такой список.

Иностранные гости узнают, что Америка — земля свободы

2 декабря 1991 г. Извлечено из Orlando Sentinel

«С Рождеством от BellSouth!»

Из-за компьютерного сбоя телефонной системы десятки иностранных путешественников в одном из отелей в центре Орландо получили ранние рождественские подарки в субботу и воскресенье.

Всё началось, когда постоялец гостиницы Plantation Manor — международного молодёжного отеля напротив озера Эола — обнаружил, что таксофоны позволяют бесплатно звонить по межгороду практически в любую точку мира.

По мере распространения слухов четыре общественных телефона, обычно пустовавших в гостинице, работали без остановки вплоть до воскресного полудня, когда Southern Bell обнаружила проблему и направила техников отключить международную связь.

Роджер Суэйн, администратор Plantation Manor, сказал, что обнаружение произошло случайно.

«Один из наших гостей сказал, что попытался позвонить в Хьюстон, Техас, со второго этажа, — рассказал Суэйн. — Оператор сообщил ему, что монеты не нужны, поскольку телефон не числится как общественный. Он разговаривал 40 минут, и с него ничего не взяли».

Представитель AT&T, обслуживающей дальнюю связь на некоторых телефонах Southern Bell, сообщил, что проблема, по всей видимости, связана с компьютером Southern Bell.

«Наше оборудование работает исправно, — сказал Рэнди Бэррidж, представитель AT&T. — Если это проблема Southern Bell, им и нести расходы».

Возможно, Southern Bell всё же частично возместила убытки: местные звонки по-прежнему стоили 25 центов.

«Для них это — капля в море», — сказал один английский путешественник о телефонной компании, только что оплатившей его звонок домой по воскресному тарифу — 21,74 доллара за каждые полчаса.

8-й Конгресс Chaos Computer Club

27–29 декабря 1991 г. Автор: Клаус Брунштейн. Особая благодарность: Terra of CCC

По случаю 10-летия своего основания Chaos Computer Club (CCC) организовал 8-й Конгресс в Гамбурге. Более чем 400 участникам (рекордное число за всю историю, причём доля студентов неуклонно росла, тогда как подростков становилось меньше) была предложена богатая программа по темам, связанным с ПК и сетями; при этом сессий, посвящённых критическим темам — фрикингу, хакерству или созданию вредоносных программ, — стало заметно меньше, чем прежде. Изменения в европейской хакерской сцене стали очевидны: на бывшую мекку хакеров приехало лишь немногочисленное представительство из Нидерландов (в частности, Hack-Tic) и Италии.

Соответственно, материалы конгресса задокументированы исключительно на немецком языке. По мере того как основатели CCC накапливают возраст и опыт, переосмысление роли CCC и растущее разнообразие мнений свидетельствуют о том, что «подростковый» CCC, возможно, больше не будет производить столь же громких событий, как прежде.

Доминирующей темой нынешнего года стали презентации коммуникационных технологий для ПК, Atari, Amiga и Unix, разработка локальной сети, а также описание региональных и международных сетей с обзорными докладами. В сравнении с этим, документы CCC '90 более детально освещали архитектуры, тогда как сессии и демонстрации CCC '91 (в «Hacker Center» и других залах) были в большей степени ориентированы на практическую навигацию в таких сетях.

Тема фрикинга была освещена нидерландской группой HACK-TIC, обновившей свою презентацию CCC '90 о том, как «минимизировать расходы на телефонные переговоры» с помощью синих и красных боксов, а также рассказавшей о доступном программном обеспечении и последних событиях. Обсуждались подробные сведения о методах фрикинга в конкретных странах и об уязвимостях в ряде телекоммуникационных систем. Дополнительная информация (на нидерландском) была доступна, включая схемы электронных цепей, в нескольких номерах голландского журнала «HACKTIC: Tijdschrift voor Techno-Anarchisten» («Новости для техно-анархистов»).

Замечание № 1: Недавние события (например, «взломы во время Войны в Персидском заливе») и материалы, представленные на Chaos Congress '91, свидетельствуют о том, что Нидерланды становятся новым европейским центром злоумышленных атак на системы и сети.

Среди прочей потенциально опасной информации HACKTIC №14/15 публикует код компьютерных вирусов (BAT-вирус, работающий некорректно).

Замечание № 2: Несмотря на то что лишь немногие нидерландские университеты ведут исследования и преподавание в области безопасности, Делфтский университет хотя бы предлагает вводные курсы по защите данных.

В отличие от прошлых лет, семинар по компьютерным вирусам (который провёл Мортон Суиммер из Центра тестирования вирусов Гамбургского университета) был намеренно посвящён распространению неразрушительной информации (без каких-либо презентаций по программированию вирусов). Обзор правовых аспектов ненадлежащего качества программного обеспечения (включая вирусы и ошибки в программах) представил адвокат барон фон Гравенройт.

Некоторое общественное внимание привлёк тот факт, что телефонная система «city-call» передаёт информацию по радиоканалу фактически в формате ASCII. Демонстрация доказала, что такие передаваемые тексты легко перехватываются, анализируются и даже могут быть изменены на обычном ПК. CCC публично предупредил, что «профили» таких сообщений (и их адресатов) легко поддаются сбору, и призвал Telecom информировать пользователей об этой незащищённости; однако немецкий Telecom не последовал этому совету.

Наряду с обсуждением развивающихся голосовых почтовых ящиков, интерес вызвала сессия, представившая систему анализа смарт-карт на базе C64. Двое студентов создали несложный механизм анализа (на основе систематического ввода-вывода) протокола немецкой телефонной карты при взаимодействии с уличным телефоном-автоматом; они описали в определённых подробностях (включая электронно-микроскопическую фотографию) архитектуру и системное поведение, в том числе 100 байт коммуникационных данных, хранящихся в центральном компьютере немецкого Telecom. На вопрос о правовых последствиях их работы они заявили, что просто хотели понять эту технологию и не подозревали о каких-либо правовых ограничениях. Они не анализировали возможности пополнения телефонного счёта (что в принципе возможно в силу архитектуры) и не изучали архитектуры или процедуры других смарт-карт (банковских и пр.).

Следуя уставу CCC (которому уже 10 лет), значительное место заняли дискуссии по социальным темам. Мастер-класс «Женское обращение с компьютером» намеренно был закрыт для мужчин (участвовало около 25 женщин), чтобы избежать прошлогоднего опыта мужского доминирования в аналогичных дискуссиях. Отдельная сессия (преимущественно для студентов-информатиков) была посвящена «Информатике и этике»: на ней рассматривалось международное состояние дискуссии и обсуждалась ценность профессиональных стандартов применительно к немецким реалиям.

Дискуссия о «техно-терроризме» стала своеобразным симптомом нынешнего состояния CCC. Хотя внешние участники (фон Гравенройт, Брунштейн) были приглашены по этой теме, внутренние разногласия в CCC свели панельную дискуссию к техническому заголовку «вопросы определений». Одна часть хотела открыто обсудить возможности, примеры и опасности техно-терроризма; другие (ветеран CCC Вау Холланд) желали в целом дать «терроризму» некое академическое определение, а часть участников попыталась представить «государственные репрессии» как разновидность терроризма. В ходе спорной дискуссии было приведено несколько примеров техно-терроризма: червь WANK, разработка вирусных техник в целях экономической конкуренции и ведения войны.

Очередной сбой линий 800 AT&T;

16 декабря 1991 г. Автор: Дана Бланкенхорн (Newsbytes)

БАСКИНГ-РИДЖ, НЬЮ-ДЖЕРСИ — AT&T пережила очередной досадный сбой своих бесплатных линий «800» в выходные дни — прямо в разгар рождественского сезона каталожных покупок.

Эндрю Майерс, представитель AT&T, сообщил, что проблема возникла в 19:20 13 декабря, когда технические специалисты загружали новое программное обеспечение в компьютеры в Алабаме, Джорджии и Нью-Йорке. Программное обеспечение идентифицирует и перенаправляет звонки по номерам 800, пояснил он. По данным компании, пострадали в общей сложности 1,8 миллиона звонков, поступивших из ряда восточных штатов США.

Обслуживание было восстановлено примерно через час, когда технические специалисты «откатили» исправление и вернулись к использованию старого программного обеспечения. Сейчас программисты работают над ним, стараясь устранить ошибки до повторной загрузки. «Нам, разумеется, не нравится, когда не проходит ни один звонок, но я бы не назвал это серьёзной проблемой», — сказал Майерс. О проблеме сообщили Федеральной комиссии по связи в выходные, а прессе — на следующий день.

Последняя проблема продолжает тревожную тенденцию сбоев в обслуживании AT&T на северо-востоке страны. Что ещё хуже — все неполадки имели разные причины: предыдущие сбои были вызваны перебоями в электропитании, проблемами с программным обеспечением коммутаторов и разрывами кабелей.

Конгресс США открывает BBS для информаторов

16 декабря 1991 г. Автор: Дана Бланкенхорн (Newsbytes)

ВАШИНГТОН, О.К. — Конгрессмен США Боб Уайз и его подкомитет по правительственным операциям Палаты представителей по вопросам государственной информации, правосудия и сельского хозяйства открыли службу электронных досок объявлений (BBS) для государственных информаторов.

Сам Уайз является системным оператором (sysop) новой доски. Newsbytes вышла на связь с системой и обнаружила, что она принимает параметры соединения 8 бит, без чётности, 1 стоп-бит (известное в отрасли как 8-N-1), а также совместима со стандартным модемом Hayes на скорости 2400 бит/с.

Информаторы — это сотрудники, сообщающие следователям о правонарушениях в своих компаниях или ведомствах, иными словами, «вскрывающие» нарушения. Уайз сообщил, что на BBS будут приниматься псевдонимы — большинство частных систем требуют настоящих имён, чтобы исключить проникновение компьютерных взломщиков или иных нарушителей. По словам Уайза, пароли будут защищать сообщения от прочтения другими пользователями, а комитет будет ежедневно проверять доску и отвечать звонящим по существу их обращений. Система работает под управлением программы RBBS — «freeware»-пакета, распространяемого бесплатно.

Исполнительная ветвь власти США использует систему инспекторов для контроля за своими ведомствами; большинство из них располагают телефонными горячими линиями для информаторов и принимают корреспонденцию. Однако инспекторы ожидают, что информаторы будут собирать доказательства на работе, что само по себе может навлечь на них неприятности. Кроме того, попытки инспектора связаться с информатором могут раскрыть его личность нарушителям. В теории звонки от сотрудников Конгресса будут восприниматься злоумышленниками как обычные назойливые звонки по надзорным вопросам.

Контакт для прессы: конгрессмен Боб Уайз, тел. 202-224-3121, BBS: 202-225-5527

NIST продлевает срок рассмотрения стандарта цифровой подписи

16 декабря 1991 г. Автор: Джон Маккормик (Newsbytes)

ВАШИНГТОН, О.К. — NIST, Национальный институт стандартов и технологий (бывшее Бюро стандартов), предпринял необычный шаг, продлив период рассмотрения спорного стандарта цифровой подписи, предложенного агентством в конце августа.

Стандартный 90-дневный период общественного обсуждения уже бы истёк, однако NIST продлил этот срок до конца февраля — по мнению ряда наблюдателей, потому что агентство желает ужесточить стандарт.

Представители NIST отрицают необходимость модификации предложенного стандарта ради повышения уровня безопасности, однако Джеймс Бидзос, чья компания RSA Data Security предлагает конкурирующий стандарт, утверждает, что алгоритм Эль-Гамаля в редакции NIST слишком слаб и продвигается правительством, поскольку Агентство национальной безопасности считает, что при необходимости легко сможет его взломать.

Новый стандарт не является методом шифрования самих сообщений — это обеспечивается действующим стандартом DES (стандарт шифрования данных). Речь идёт о DSS — стандарте цифровой подписи, то есть методе верификации «подписи» отправителя сообщения: иными словами, подтверждения того, что сообщение — которое может быть приказом о переводе денег или иным важным документом — действительно исходит от лица, уполномоченного отдавать такие распоряжения.

Как сообщала Newsbytes ещё в июле, АНБ и NIST были обязаны разработать систему безопасности около четырёх лет назад. Анонсированный недавно алгоритм Эль-Гамаля изначально должен был быть представлен ещё прошлой осенью; за это время схема шифрования RSA приобрела широкую популярность.

Тогда заместитель директора NIST Раймонд Дж. Каммер сообщил Подкомитету по технологиям и конкурентоспособности Комитета по науке, космосу и технологиям Палаты представителей, что схема шифрования Эль-Гамаля, запатентованная федеральным правительством, была выбрана потому, что позволит федеральным ведомствам экономить средства по сравнению с частной схемой шифрования и верификации подписей RSA.

Примечательно, что единственной компанией, в настоящее время предлагающей на рынке систему ЦП на основе Эль-Гамаля, является Information Security Corp. (1141 Lake Cook Rd., Ste. D, Deerfield, IL 60015) — компания, выигравшая затяжную судебную тяжбу с RSA за право продавать федеральному правительству программное обеспечение для шифрования на основе RSA. Это стало возможным, поскольку RSA был разработан в Массачусетском технологическом институте математиками, работавшими по федеральным грантам.

Программа ISC Secret Agent стоимостью 249,95 долларов, использующая алгоритм Эль-Гамаля, была представлена на прошлогодней выставке Federal Office Systems Expo в Вашингтоне. Эль-Гамаль — это система с открытым ключом, которую можно применять точно так же, как систему RSA, однако отличающаяся от неё существенными теоретическими особенностями.

Генеральный директор и президент ISC Томас Дж. Венн сообщил Newsbytes, что система Эль-Гамаля весьма надёжна, однако алгоритм Эль-Гамаля существенно отличается от алгоритма RSA: его стойкость обусловлена сложностью вычисления дискретных логарифмов в конечном поле, а не принципиально иным методом RSA — разложением произведений двух простых чисел на множители.

RSA дала отпор, объявив о денежном призе для всех, кто сможет взломать схему RSA. Желающим попробовать следует отправить конверт с обратным адресом и маркой по адресу: RSA Data Security, Inc., 10 Twin Dolphin Dr., Redwood City, CA 94065, — для получения списка RSA и условий. Те, у кого есть доступ к электронной почте Internet, могут отправить запрос по адресу challenge-info@rsa.com.

PWN Quicknotes

1. Компьютерные доски объявлений теперь не только для занудных киберпанков — по крайней мере, не в Сан-Франциско. Предприниматель Уэйн Грегори создал SF Net — вполне общительную компьютерную сеть, связывающую посетителей самых модных кафе города. От Лоуэр-Хайта до района к югу от Маркет-стрит хай-тек-тусовщики общаются за капуччино. Всё, что нужно, — купить билет в кафе, ввести номер в стационарный компьютер и начать техно-чат за 1 доллар в 15 минут. Следующий пилотный проект Грегори — Сиэтл, штат Вашингтон. (*Newsweek*, 2 декабря 1991 г.)

---

2. Согласно номеру San Jose Mercury News от 29 ноября 1991 года, система экстренного вызова 911 округа Сан-Матео, Калифорния, была парализована из-за розыгрыша — причём не хакером и не фрикером.

Диджей на радиостанции KSOL решил крутить недавнюю запись MC Hammer снова и снова и снова — в качестве шутки. Слушатели забеспокоились, не случилось ли что с персоналом станции, и начали звонить по номеру 911 (и на дежурный номер полиции). Несколько сотен звонков за сорок пять минут — час оказалось достаточно, чтобы перегрузить систему. В газете не сообщалось о погибших или пострадавших от перегруженной системы.

Диджей не хотел останавливать запись (ссылаясь на права Первой поправки), однако всё же вставил объявление с просьбой не звонить в полицию.

---

3. Жан Поль Барретт, заключённый тюрьмы округа Пима в Тусоне, Аризона, отбывавший 33-летний срок за подлог и мошенничество, был освобождён 13 декабря 1991 года после получения поддельного факса с приказом о его освобождении. По всей видимости, копия подлинного приказа об освобождении была изменена с проставлением ЕГО имени. Судя по всему, никто не заметил, что в факсимильном документе отсутствовал исходящий номер телефона и не было «официального» титульного листа. «Ошибка» была обнаружена, когда Барретт не явился на судебное заседание.

Тюрьма ежедневно освобождает около 60 человек, и факсы стали стандартной процедурой. Сержант шерифа Рик Кастигар заявил, что «процедуры меняются, чтобы подобная ошибка не повторилась». (*San Francisco Chronicle*, 18 декабря 1991 г., стр. A3)

---

4. AT&T повысит тарифы на прямые международные звонки 2 января 1992 года. Повышение, затрагивающее будничные и вечерние звонки, добавит примерно 8 центов к среднему ежемесячному счёту за межгородскую связь в 17 долларов и около 60 миллионов долларов к годовой выручке AT&T. (*USA Today*, 23 декабря 1991 г., стр. B1)

---

5. Следующее сообщение взято из квартального бюллетеня акционеров AT&T и публикуется не в коммерческих целях, а в расчёте на возможный интерес читателей.

Красочный постер форматом 22×28 дюймов, прослеживающий развитие телефона от первой модели Белла до новейших высокотехнологичных аппаратов, можно приобрести за 12 долларов. Для заказа отправьте чек по адресу: Poster, AT&T Archives, WV A102, 5 Reinman Road, Warren, NJ 07059-0647. Тел.: 908-756-1590.

(Особая благодарность: The Tone Surfer)

---

6. По имеющимся сведениям, обычный синий бокс на бесплатных номерах в Норвегии теперь МЁРТВ. По некоторым данным, поступившим в Phrack, бесплатные номера были переключены на обычную телефонную сеть в США, которую уже не удаётся фрикать тем же способом. *(Особая благодарность: Nosferatu)*

---

7. Если вы пытались дозвониться до Blitzkreig BBS и не могли соединиться — Predat0r переносит свою доску в подвал. Он сказал, что доска возобновит работу с 1 февраля. Также сообщается, что мастер-копия TAP №106 готова, однако он отстаёт на год с обновлением списка рассылки. По его словам, делать копии — не проблема, но из-за потока новых подписчиков ему придётся привлечь местных помощников для обновления базы данных. Он также подтвердил, что если кто-то заплатил за десять номеров — тот получит десять номеров. *(Особая благодарность: Roy the Tarantula)*

---

8. Вышла новая научно-фантастическая книга «Fallen Angels» («Падшие ангелы») Ларри Нивена. Её основная идея такова: правительство США захватили религиозные фанатики и воинствующие экологи. Вскоре Соединённые Штаты превращаются в антитехнологическое полицейское государство. Два астронавта сбиты над США и вынуждены скрываться. Они бегут от различных правительственных ведомств, в том числе от (напоминающего Секретную службу) Агентства по охране окружающей среды. Буйная фантазия Нивена обеспечивает изрядную долю юмора — а также немало вещей, которые совсем не смешны, поскольку они попадают чуть слишком близко к реальности.

В книге также упоминаются Legion of Doom и рейды против Steve Jackson Games. В разделе «Благодарности» в конце книги автор пишет: «Что касается общества, изображённого здесь, — разумеется, многое в нём является сатирическим. Увы, многие эпизоды — например, дело Стива Джексона, когда бизнес был обыскан агентами Секретной службы, предъявившими ордер без подписи, — вполне реальны. Реальны и многие антитехнологические аргументы, приведённые в книге. В студенческой среде действительно существует антиинтеллектуальное движение, осуждающее "материалистическую науку" в пользу чего-то значительно более "холодного и безжалостного". Так что будьте осторожны». *(Особая благодарность: The Mad Alchemist)*

---

9. Bell Atlantic стреляет себе в ногу (5 февраля 1992 г.) — Newsbytes сообщает, что Bell Atlantic признала финансирование лоббистской группы «Small Businesses for Advertising Choice» («Малый бизнес за свободу рекламы») для противодействия законопроекту HR 3515, регулирующему выход RBOC на рынок информационных услуг. Спонсор законопроекта, демократ от Теннесси Джим Купер, назвал это «неуклюжей кампанией Astroturf» — то есть имитацией народной инициативы.

Республиканский соавтор законопроекта Дэн Шэффер стал объектом аналогичной кампании со стороны US West: сотрудников телефонной компании поощряли в рабочее время звонить своим представителям и выражать протест против законопроекта.

Законопроект имеет номер HR 3515. Чтобы получить копию, позвоните в Документационный отдел Палаты по номеру (202) 225-3456 и запросите её. Это бесплатно (точнее, вы за это уже заплатили

налогами).

---

10. Компьютерные хакеры получили доступ к частным кредитным досье (Columbus Dispatch, 24 февраля 1992 г.) — ДЕЙТОН. Компьютерные хакеры получили конфиденциальные кредитные отчёты потребителей Среднего Запада от кредитного бюро в Атланте. Базирующаяся в Атланте компания Equifax сообщила, что группа из 30 хакеров в Дейтоне, штат Огайо, похитила номера кредитных карт и истории платежей потребителей, воспользовавшись паролем одного из клиентов Equifax.

Рональд Дж. Хорст, консультант по безопасности компании, сообщил, что взлом, по всей видимости, начался в январе. Полиция не установила, был ли пароль похищен или сотрудник компании-клиента вступил в сговор с хакерами. По словам Хорста, хакеры, судя по всему, делали это ради развлечения. Обвинения пока не предъявлены. Equifax уведомит клиентов, чьи кредитные отчёты были получены.

---

11. Отпечатки пальцев и объединённые базы данных (краткое изложение статьи Стивена Шварца, *San Francisco Chronicle*, 22 февраля 1992 г., стр. A16) — Отпечаток пальца, обнаруженный при нераскрытом убийстве 1984 года 84-летней женщины, все эти годы хранился в базе данных полиции Сан-Франциско. Недавно база данных отпечатков пальцев Сан-Франциско была объединена с аналогичной базой округа Аламеда. Старый отпечаток совпал с новым, снятым в связи с делом о мелкой краже, — и спустя восемь лет полиции удалось раскрыть старое дело (кража со взломом, поджог, убийство). Двум девушкам, замешанным в преступлении, на тот момент было 12 и 15 лет. *(Особая благодарность: Питер Дж. Нойманн из RISKS)*